LOGIN.GOV DOESN'T MEET THE STANDARD

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS
AND THE FEDERAL WORKFORCE

OF THE

COMMITTEE ON OVERSIGHT
AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 29, 2023

Serial No. 118–17

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
51–722 PDF WASHINGTON : 2023

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
KELLY ARMSTRONG, North Dakota
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
SHONTEL BROWN, Ohio
JIMMY GOMEZ, California
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
BECCA BALINT, Vermont
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
BILL WOMACK, Senior Advisor
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Senior Policy Analyst
MALLORY COGAR, Deputy Director of Operations and Chief Clerk
CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON GOVERNMENT OPERATIONS AND THE FEDERAL WORKFORCE

PETE SESSIONS, Texas, Chairman

GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
ANDY BIGGS, Arizona
BYRON DONALDS, Florida
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
CHUCK EDWARDS, North Carolina
ERIC BURLISON, Missouri

KWEISI MFUME, Maryland *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
MAXWELL FROST, Florida
GREG CASAR, Texas
GERALD E. CONNOLLY, Virginia
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
BECCA BALINT, Vermont
SUMMER LEE, Pennsylvania
JASMINE CROCKETT, Texas

C O N T E N T S

WITNESSES

Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

Documents are available at: docs.house.gov.

LOGIN.GOV DOESN'T MEET THE STANDARD

Wednesday, March 29, 2023

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON GOVERNMENT OPERATIONS AND THE FEDERAL WORKFORCE
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:45 p.m., in room 2247, Rayburn House Office Building, Hon. Pete Sessions (Chairman of the Subcommittee) presiding.

Present: Representatives Sessions, Higgins, Biggs, Timmons, Burchett, Burlison, Mfume, Norton, Frost, and Lee.

Mr. SESSIONS. The Subcommittee on Government Operations and Federal Workforce will come to order.

Without objection, Chair may declare a recess at any time.

And I recognize myself for the purpose of an opening statement.

Good afternoon. Welcome to this hearing. Today we are going to focus our attention on *Login.gov*. *Login.gov* is intended to allow citizens to access Federal services and even some state services across different agencies using the same username and password. For agencies, *Login.gov* provides identity verifications services which will help applicants who say they are who they are.

Given what we have learned in recent hearings around waste, fraud, and abuse in COVID-related programs, the types of services *Login.gov* provides could be an important tool in combating fraud, especially fraud resulting from identity theft. The problem is that, as documented in a report issued by the General Services Administrator inspector general earlier this month, *Login.gov* did not actually provide the services it claimed to provide. As the IG report documents, employees and leaders in *Login.gov* and the technology transformation services, the branch within GSA which *Login.gov* falls, knew that they did not provide these services. So, not only did *Login.gov* mislead its customers, it charged them for services it did not provide. Deception is a bad thing.

So, it lied when seeking authorization for cloud-based services through the Federal RAMP program, and it lied when it applied for and received a $187 million grant from the Technology Modernization Fund. NIST standard requires agencies, including *Login.gov*, to use biometric comparisons to achieve a certain level of security, but *Login.gov* never performed biometric comparisons and it still does not today. These can be powerful tools to fight fraud, and presumptively NIST required them for that reason, so their lack of

representation is a significantly important gap in security and saving fraud in and with government money.

To its credit, GSA has accepted what happen at *Login.gov*. They actually asked for the audit. This would be considered favorable, but important questions need to be answered. And not only has the GSA received this report, but so did Congress on a bipartisan basis. Why did this happen, how did it happen, what was the impact, and what is being done to fix this problem is a fair part and should be a fair part of this hearing today by the Subcommittee.

As for the impact, for the most part, we do not yet know. It was beyond the scope of the IG report to determine what damage the former fraud resulted, but this Subcommittee needs to get those answers. That said, the reputational damage to *Login.gov*, TTS, and GSA are significant, but today we can be on the road together to find these answers, to find the direction we are going to go, and hold not only *Login.gov* to its points that it makes, but also the reciprocal money that would be expended by Members of Congress.

As one Federal official recently put it, what else about GSA services have they been less transparent about? Why did this happen? It boils down to the fact that *Login.gov* employees and leaders felt they did not have to follow the rules is what some would be led to believe. Express concerns about one type of biometric comparison, facial recognition, and the impact it could have had on certain demographic groups is one of the questions, but there are other ways to perform biometric comparisons. Most importantly, you cannot simply express concerns about a requirement and then choose not to address the issue, and you certainly cannot lie about things that your product does and not fix.

So, how did all this happen? According to IG report and previous IG reports, it reflects the culture within TTS and especially one of its components, 18F, which built *Login.gov*. TTS and 18F purport to be a startup mentality to government, but since its creation, this is equal to running amok. Previous IG reports have documented how 18F made a practice of ignoring procedures; policy, including hiring policies, policies about paying employees and to include information security policies; and rules. The previous TTS director, a significant figure in this current scandal, also absolved TTS of the burden of bringing in revenue from the project it works on.

The TTS mindset was, albeit, due to a lack of oversight from GSA leadership, that meant, we believe, that GSA leadership, so to speak, turned a blind eye, to their managerial responsibilities. We need to ask these questions. GSA needs to look inward and determine what they have done and what needs to be done better. I would like to say, it is easy simply to tell the truth today, but I think that what we are trying to get is, on a bipartisan basis, it is my hope, that what we are trying to get at is an opportunity to figure out what happened, fix it, and make sure it moves forward properly.

The fallout from *Login.gov* appears to only add preexisting concerns from inside Federal agencies. As one CIO put it, if you talk to any CIO, they tell you that they would not welcome having TTS inject themself into their enterprise, and yet that became a standard of operation at GSA. So, what is the value? Why would Congress continue to support it? All GSA has to say, is it is conducting

an equity study. What does that involve, and who is performing this study, and what would you expect to get from it? So, the concerns that we have are more than disagreeing with the reply. We think it is a mature opportunity to look at and ask questions.

I have concerns that the Biden Administration may be making the problem worse. *Login.gov* remains a significant part of the recently released anti-fraud plan. The IRS announced it was going to use *Login.gov* even after it was widely known it did not comply with the NIST standard. There are even concerns with pending update on the NIST standard. There are some questions about where the IRS position is actually, and I need to admit that also.

Before I refer to our Ranking Member, I would like to acknowledge the pain that is experienced by some of our Members and to recognize that. I would like to take a moment and offer my condolences to our Ranking Member, Mr. Mfume. I learned yesterday that you recently experienced the death of one of your staff members, Mrs. Diana Gibson. I understand that she was with you for 40 years, and I know you feel the loss deeply and as profound in your life. On behalf of myself and all of the Republican Members and staff of the Committee, I want to offer my condolences to you, your staff, and family and friends of Mrs. Gibson, and yet I think today we want to acknowledge her service to you and this country.

I would yield to the gentleman for any opening statement. Excuse me. The gentleman is recognized.

Mr. MFUME. Well, thank you very much, Mr. Chairman. Diana Gibson and I were friends for actually well over 40 years. I was there when she went to work for our former colleague, the late Elijah Cummings, and spent 24 years with him and after Elijah's death has been with me up into her own death. We all have staff people that we sort of take for granted that they will always be there, that they will, you know, outlive us and go on to do great things, and that is not always the case. So, I appreciate your comments, your condolence, your reference here. She gave a lot of herself and her service to this country, and it is going to be missed in a lot of different ways. So, thank you very much, sir. I appreciate that.

Today we convene, as the Chairman said, an important hearing to discuss a topic that millions of Americans who have engaged with the Federal Government's secure online sign-in service know what we are talking about. It is *Login.gov*. If you have received unemployment benefits through the Paycheck Protection Program, or if you have received a disaster loan from the Small Business Administration, or applied for a job through U.S.A. Jobs, you have used *Login.gov* to securely sign in and access the much-needed government services that would be available. And so, Americans have come to trust *Login.gov* with their sensitive information and, of course, the Federal Government relies on *Login.gov* to help root out any potential fraudsters hoping to siphon money away from the essential government programs that we support, that we stand up, and we expect to carry out their charge.

Today, unfortunately, we must reconcile certain failures that have, indeed, come to light. Just a few weeks ago, the General Services administrator and the inspector general released an alarming report that details how the GSA misled customers on

Login.gov's compliance with the identity proofing standards that the National Institute of Standards and Technology issued some time ago in 2017.

Federal agencies must ensure that their identity proofing and authenticating services meet the NIST standards. For government services that may have to have a higher risk of fraud, agencies may then require the service provider to meet an even higher identity proofing standard. For example, they may require more than a username and a password. In these cases, they may need to prove who they are by visiting a Federal facility in person or by providing biometric data, such as a selfie, in an online environment. *Login.gov* operates a high level of identity proofing, but it was not at the IAL2 level and that standard, which requires biometric data. *Login.gov* failed to offer either an in-person or remote identity proofing option, and yet GSA started to bill its customers, comprised of roughly 22 agencies, for non-compliant services for as many as two years.

The report found that multiple key personnel informed the *Login.gov* team of its non-compliance with NIST's IAL2 standards as early as January 2020, a few months after *Login.gov* began billing its customers. That was not the last time *Login.gov* was informed of its noncompliance, and yet it continued to mislead certain customers. It happened again in 2020 when a GSA consultant informed senior *Login.gov* staff persons of its lack of an IAL2 component. But it was not until June 2021 that a senior official at GSA announced internally that GSA would cease its efforts to meet biometric requirements because of equity concerns.

So, what is important to highlight here is that *Login.gov* has never met the standard. At least we have not found any proof that it has. It did not meet the standard then and, for many of us, it has not found a way to meet that standard today. And still *Login.gov* continued to mislead customer agencies about its lack of biometric comparison capabilities until January of last year, when the Agency released its equity action plan. And then finally, at the end of our five-year timeline, GSA notified customer agencies that the services they were paying for did not comply with NIST requirements published, as I said earlier, back in 2017.

So, what the report does not show and what is just as important to this conversation are the decisive and immediate actions taken by GSA leadership when they were finally made aware of *Login.gov*'s shortfalls. In February 2022, GSA leadership removed the temporary director of *Login.gov* and instituted a temporary director. GSA then initiated a formal management inquiry to investigate misrepresentations. By March of last year, leadership referred to this matter, or referred the matter—excuse me—to the inspector general to undertake a non-partisan, impartial review of the matter. Now, I must say that it is rare for an agency to actually unilaterally request an inspector general review, and I commend the GSA for taking that important step.

GSA leadership has also created a new Technology Law Division to specialize in technology-focused legal services. This is one action that we should be looking to replicate, I think, across all Federal agencies in the future to ensure there is adequate understanding of the technology that is being deployed. I hope we can explore that

today. As the Chairman says, we are really trying to get to answers. We know what the issues are, but we really are seeking answers as we go forward.

And last, in October of last year, GSA leadership directed *Login.gov* to undertake a top-to-bottom review of the program. I look forward to hearing an update on the progress of that review, what it has come up with, and what it is pointing to as things that this body and the full Congress should be looking out for as we provide the oversight that we are attempting to do.

I want to thank all of our witnesses who are here today that the Chair, I am sure, will properly introduce. We have been on a crazy little schedule, and so we didn't start when we were supposed to start, but we are all together now, and I look forward, like so many Members of this panel, to hearing your testimony. I yield back.

Mr. SESSIONS. The gentleman yields back. Thank you very much. It is my hope that our witnesses and those who are guests to today's hearing see that the gentleman and I, and our team, and his team, and our teams intend to not only vigorously pursue the information we have, but to do so in a professional standard. And I know that you expect that of me, and thank you very much.

Mr. MFUME. Absolutely.

Mr. SESSIONS. I appreciate it. I am now pleased to introduce our witnesses for today's hearing. Our first witness is Carol Fortine Ochoa, Inspector General for the General Services Administration. Ms. Ochoa has been an inspector general for GSA since 2015. Prior to that experience, she worked for over 25 years as a Federal prosecutor and manager in the United States Department of Justice. Thank you for being here, Ms. Ochoa.

Our second witness is Sonny Hashmi, Commissioner of the GSA Federal Acquisition Service. Mr. Hashmi has also served as GSA's Chief Information Officer and Chief Technology Officer and led the Agency in IT modernization strategy. Mr. Hashmi, thank you for joining us today.

Our third witness is Mr. Jim St. Pierre, acting director of the NIST—I called it earlier "NISTA," and that is my fault; my staff very promptly said quit acting like you are from Texas—of the NIST IT Laboratory. In this role, Mr. St. Pierre oversees the development, dissemination of standards, measures, and testing for IT. Mr. St. Pierre has worked for NIST since 1994 and has an applied and academic background in electrical engineering.

I want to welcome each of these witnesses, and if I could please have you stand and raise your right hand. Pursuant to Committee Rule 9(g), the witnesses will raise their hand and they answer the following questions.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God.

[A chorus of ayes.]

Mr. SESSIONS. Thank you very much. Please let the record reflect that each of these witnesses all answered in the affirmative. And, thank you very much.

We appreciate you being here today and look forward to your testimony. Let me remind the witnesses that we have read your written statements, and they will appear in full in the hearing record.

However, we ask that your oral testimony would be to five minutes. That way, we are able to get through the questions from those who have spent a good deal of time studying on this issue, so thank you very much.

I think you know how this works. We have four minutes, and when four minutes left, the light turns yellow. When the red comes on, your five minutes has expired. I would expect that you would want me to allow you to finish your sentence, but we would like to ask that you please wrap it up pretty quickly after that.

So, Ms. Ochoa, thank you for being here, and the gentlewoman is recognized for five minutes.

STATEMENT OF CAROL FORTINE OCHOA, INSPECTOR GENERAL, OFFICE OF THE INSPECTOR GENERAL, GENERAL SERVICES ADMINISTRATION

Ms. OCHOA. Thank you, Chairman Sessions, Ranking Member Mfume, Members of the Subcommittee. I appreciate the opportunity to testify here today about our recent report.

GSA misled customers on *Login.gov*'s compliance with digital identity standards. As you noted in your opening statements, *Login.gov* is the platform which the General Services Administration offers to Federal agencies to meet Federal cybersecurity requirements for a single sign-on source for the American public to use when accessing government services.

Within the Office of Inspector General, we conduct audits, investigations, and evaluations to promote efficiency and effectiveness and to prevent and detect waste, fraud, abuse, and mismanagement in GSA programs. We began this particular evaluation when GSA informed us of possible misconduct—my staff in the office responsible for *Login.gov*. Our evaluation found that GSA did mislead its customer agencies by failing to tell them about *Login.gov*'s known non-compliance with guidelines published by the National Institute of Standards and Technology or NIST.

Notwithstanding GSA's assertions that *Login.gov* met NIST requirements for identity verification, at what is known as Identity Assurance Level 2 or IAL2, the truth is that *Login.gov* has never included the physical or biometric comparison that is required for identity proofing and authentication at that level. At multiple points, starting in 2019, *Login.gov* officials knew and should have notified customer agents that *Login.gov* did not comply with Level 2 requirements. However, GSA did not do this.

Further, the Agency continued to mislead customer agencies even after GSA suspended efforts to meet the NIST guidelines in June 2021. GSA knowingly billed multiple customer Federal agencies over $10 million for IAL2 services that did not, in fact, meet IAL2 standards. Additionally, GSA used misleading language to secure additional funds for *Login.gov* from the governmentwide Technology Modernization Fund.

Finally, we found that despite our prior OIG reports identifying GSA's inadequate management and oversight of its technology transformation services, 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 the technology transformation

services in *Login.gov*, GSA's Federal Acquisition Service shares responsibility for the misrepresentations to GSA's customers.

Our report made several recommendations to the Agency to address our findings, including that the Agency establish adequate management controls over the technology transformation services, undertake a comprehensive review of its billings to customer agencies, and establish a system to ensure compliance with relevant standards. We were pleased that GSA management referred this matter to us and that it agrees with our findings and our recommendations. The Agency has 60 days from the issuance of the report to provide us with a corrective action plan, which we will look forward to receiving and reviewing.

I, again, appreciate the invitation to appear here today and to share with you this recent work by our office. We appreciate your interest in and support for our work, and I am happy to answer your questions.

Mr. SESSIONS. Thank you very much.

[Audio issues in room.]

STATEMENT OF SONNY HASHMI, COMMISSIONER, FEDERAL ACQUISITION SERVICE, GENERAL SERVICES ADMINISTRATION

Mr. HASHMI. Good afternoon, Chairman Sessions, Ranking Member Mfume, and Members of the Committee. Thank you for the opportunity to come before you and discuss the *Login.gov* program, a part of the U.S. General Services Administration's Technology Transformation Service, or TTS, a component of the Federal Acquisition Service. My name is Sonny Hashmi. I am the Commissioner for the Federal Acquisition Service, and I am honored to testify before you, alongside my colleagues from NIST, National Institute of Standards and Technology; and the Inspector General—I do apologize—the Inspector General of the General Services Administration.

First, let me state very plainly, the misrepresentations made by the Login team in this matter were absolutely unacceptable. This was a serious issue which GSA identified and has been working very collaboratively with the IG to address since we learned of the problem in early 2022. Today, I want to update the Committee on our actions to date. Before I do that, let me say a word about what *Login.gov* is and why it is important.

The public deserves a secure, identity-proofing solution that ensures access, protects privacy, and prevents fraud. Identity verification is a requirement for people to access services at all levels of government. Historically, when someone sought to renew a passport or to apply for veterans' benefits, they did so in person by presenting a government-issued ID. Increasingly, people need to access and obtain these services virtually, so we need a similar mechanism to verify these identities.

Login.gov is an authentication and identity verification solution that helps the American people securely and readily access the government services they need while protecting their privacy and preventing fraud. Having a public solution for identity verification is critical for a number of reasons. First, we can prevent fraud by driving a single and secure service that provides robust security

controls. Second, we can protect people's information, and third, we can make accessing government services simpler and more secure for the public and ensure we serve all Americans.

As GSA moves forward to implement the IG's recommendations, I want to make sure the Committee is aware of the actions we have taken since learning of this issue. We notified GSA's Inspector General immediately upon learning of this issue in early 2022. We notified customers and agency partners, including the TMF board, about the misrepresentations, and modified interagency agreements to accurately reflect the services provided. We replaced leadership of the program and launched an employee disciplinary inquiry. And all those who we are aware of, who knowingly misrepresented features of *Login.gov*, are no longer employed by the GSA.

We launched a top-to-bottom internal management review of the program's compliance roadmap, customer communications, internal controls environment, financial operations, human resources, and contracts. And we strengthened accountability and oversight practices, including the creation of a new Technology Law Division in GSA's Office of the General Counsel and a new executive steering committee, comprised of technology leaders at OMB. These actions have strengthened the management of *Login.gov* program.

While there were serious management challenges at *Login.gov* and TTS, I want to make it clear that *Login.gov* itself is a strong service. *Login.gov* has a robust suite of security features to prevent fraud, like mandatory multi-factor authentication, phone and address verification, and we continue to add more features targeting bad actors, bots, and other threat vectors. *Login.gov* also has a strong encryption model to protect the privacy of the citizens who use it, ensuring that users, not corporations, control access to their own information. And *Login.gov* is FedRAMP authorized, meaning that extensive controls are in place and independently audited to ensure the system is secure from cybersecurity threats.

Moreover, GSA continues to enhance the *Login.gov* service for better delivery for the needs of our customers. Since its referral to the inspector general, GSA has expanded options for secured identity verification. GSA is now piloting a service, in partnership with the U.S. Postal Service, to allow certain users to complete their identity verification in person at one of over 18,000 locations across the country. And GSA has scaled up *Login.gov*'s contact center to provide 24/7 customer support so that constituents can get help with their identity verification process at all hours.

Overall, *Login.gov* is a strong product that provides robust identity verification services across government. We have taken many actions to improve the management of *Login.gov* and TTS, and will take further steps to ensure that we remain accountable and transparent. We are committed to maintaining the trust for our customers, stakeholders, and the public as we deliver a secured entity verification solution.

Finally, I want to, once again, thank the IG for our office's evaluation and their view of the matter. I am happy to answer any questions the Committee might have. Thank you.

Mr. SESSIONS. Sure. Thank you very much. That was a mature response to the important issues that need to begin resolution. I appreciate your attitude. Mr. St. Pierre?

STATEMENT OF JIM ST. PIERRE, ACTING DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mr. ST. PIERRE. Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, I am Jim St. Pierre, the Acting Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology, known as NIST. It is an honor to testify today on behalf of NIST and how we develop guidance, and about our digital identity guidelines, Special Publication 800–63.

The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST's role in cybersecurity is to provide standards, guidance, tools, data references, and testing methods to protect information systems against threats to confidentiality, integrity, and access availability of information services.

The Cyber Security Enhancement Act of 2014 authorized NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. Under the Federal Information Security Modernization Act, NIST develops security standards and guidelines for non-national security Federal agency systems, which may be made mandatory for Federal agencies, as is the case for NIST Special Publication 800–63 digital identity guidelines. NIST does not, however, oversee the adoption or implementation of information security standards and guidelines by Federal agencies or ensure agency compliance where they are adopted.

In developing its guidelines, NIST prides itself on the strong partnerships we have developed and relies upon transparent and collaborative processes that enlists broad expertise from government, industry, academia, and nonprofit entities to develop and improve our cybersecurity resources.

As part of our research, NIST maintains and regularly updates its digital identity guidelines, Special Publication 800–63. The current version of this guidance, which is Revision 3, was published in June 2017, and details the process for organizations' management of digital identity risk and use of digital identity products and services. These guidelines provide requirements for Federal agencies implementing digital identity services. They can also be voluntarily adopted by non-Federal organizations. The guidelines cover identity proofing and authentication for individual users, such as employees, contractors, or private individuals, interacting with government information technology systems over open networks.

The guidelines detail a risk management process that seeks to achieve both interoperability and flexibility. SP 800–63 provides a common language and taxonomy to allow organizations to identify risks and select one of three defined groups of baseline controls depending on their assessment of their risk profile. Organizations that implement the guidance are allowed to select and implement compensating controls, provided they document their decision and offer justification based on risk. In practice, this allows organizations implementing these digital identity guidelines to review spe-

cific controls, such as biometric comparison or evidence requirements, and choose to document and implement comparable alternative controls. This allows organizations to maintain broad interoperability while allowing for modifications to meet organizational and mission-specific needs.

A draft of Revision 4 of SP 800–63 is currently out for public comment through April 14, 2023. This is following a robust engagement process to gain feedback from public and private sector organizations on how to improve the draft guidance and achieve a more secure identity ecosystem.

NIST is proud of its role in establishing and improving cybersecurity solutions, standards, guidelines, and other resources, and of the longstanding and robust collaboration we have established with our Federal Government partners, private sector collaborators, and international colleagues. Thank you for the opportunity to discuss NIST activities related to digital identity guidelines. I will be pleased to answer any questions you may have.

Mr. SESSIONS. Mr. St. Pierre, thank you very much. The distinguished gentleman from Louisiana is recognized for five minutes.

Mr. HIGGINS. I thank the Chairman. My, my, my. I am going to attempt to ask some questions that might have meaning to the American people because this is a complex topic that we are discussing today.

Madam Inspector General, I am going to be asking you these questions. My understanding here is, just sort of to sum it up, is that what we are looking at essentially is theft by fraud, by misrepresentation, by a government agency through government entities with money flowing back into the government agencies regarding *Login.gov*, a service provided across the government to verify the identity of applicants to determine that they are who they claim to be, and that the levels of security required in these applications call for a very strict standard of verification, and that standard was presented as being met, and yet it was not met. And there was payment made for years for services rendered at a particular level, and it has come to our attention that that level of service had never been rendered. So, this is a complex series of events.

Madam Inspector General, I will just ask you, and I will give you sufficient time to reply. Who is being held accountable? Is anyone getting fired or going to jail? Who is suspended? Where is the money, and how much money was fraudulently billed by misrepresentation through the *Login.gov* network? If you understand my questions, who is being held accountable, has anybody been fired, is anybody going to jail, how much money was fraudulently billed through misrepresentation of capabilities, and where is that money? Madam Chair, I yield for you to answer. I am sorry, Madam Inspector General.

Ms. OCHOA. Thank you. I think the short answer to the question on accountability is that the GSA OIG does not have the authority to hold accountable agency employees for misconduct. That authority rests with the agency, so I would defer to——

Mr. HIGGINS. So, your chain of command through the Federal Government, which ultimately would reside with the President of the United States and his Secretary-level advisors to make deci-

sions regarding who gets fired here, and who is held accountable, or who is prosecuted, *et cetera*?

Ms. OCHOA. As to the question of prosecution, we did not find evidence of criminal false statements in this matter, so we made no referrals for criminal prosecution. As to administrative misconduct, we referred the results of our evaluation to the Agency. Agency leadership is responsible for holding accountable those employees, and we have been told that the Agency has disciplinary proceedings underway.

Mr. HIGGINS. Have you witnessed any of those disciplinary proceedings, like notices coming, advisements to you by emails or anything else, or any documentation of accountability that you have observed, good lady? And I ask this respectfully. It is a legitimate question.

Ms. OCHOA. I appreciate the question. We have not received such notices from the Agency that I am aware of.

Mr. HIGGINS. Did either of you gentlemen—are you aware of official accountability action that has been taken here?

Mr. HASHMI. Yes, Congressman. Thank you for that question. My name is Sonny. I am responsible for the program that this report identifies. As I mentioned in my opening statement, immediately upon finding out about this issue earlier last year, we initiated an internal inquiry for employee discipline based on information that we had, and we have continued to provide that information to the individuals who are looking at disciplinary actions. In fact, to date, as of today, none of the employees who were identified to have misled their customers knowingly are employed by the GSA. So, while due process continues, we have made sure that those employees no longer are employed by our Agency.

Mr. HIGGINS. Thank you. Mr. Chairman, my time has expired, but we never quite got to the money. Where is the money and how much? So perhaps another Member during questioning could get to that. Thank you, Mr. Chairman, I yield.

Mr. SESSIONS. The gentleman yields back his time. The gentleman from Maryland, Mr. Mfume, is recognized for five minutes. Sir?

Mr. MFUME. Thank you very much, Mr. Chairman. Madam Inspector General, I want to commend you on the work that you did in compiling this report. I noticed that there are a number of redactions. Is that, in each instance, to protect the name of an individual?

Ms. OCHOA. Yes, it is.

Mr. MFUME. And were there other instances of redaction that did not fall into that category but were done for another reason?

Ms. OCHOA. No. No, these were names of individuals.

Mr. MFUME. OK. This is a very damning report. I mean, we have all kind of said that. You have pretty much said it also as the inspector general here. It is a very damning report against GSA, the one agency that we trust to do the sort of oversight of other agencies, and of the government, and of the government's money, so it is very disconcerting. The GSA clearly has tarnished its own name here, and the question becomes, how do they get out of this hole? Now, I said earlier that I wanted to commend them for unilaterally requesting the inspector general to get involved, but that was years

down the road. And I don't know if there was anything in your report that would suggest why it took so long for the GSA to recognize that it had a problem.

Mr. SESSIONS. Excuse me. Would the gentlewoman answer the question despite it being in the report? If the gentlewoman would answer the gentleman's question. It is appreciated.

Ms. OCHOA. I think I was being told that my microphone was off. Sorry about that.

Mr. SESSIONS. That is OK.

Ms. OCHOA. Yes, we did address that in the report. We have had several prior reports at the Inspector General's Office pointing out the lack of management oversight and controls over that particular technology unit. And for whatever reason, that culture of noncompliance was allowed to persist, and we make mention of that in the report. I think that is the best answer that——

Mr. MFUME. Yes, it must have been a real deep sort of culture to exist and then resist the sort of scrutiny that everyday people would have who are part of the Agency. I just find that to be amazing that they lacked adequate controls. I want to talk about the Federal Acquisition Service also in just a moment, but the deliberate misrepresentation to government agencies that they were being billed as they should be when they were not getting the services that they, in fact, paid for.

But let us talk about the Acquisition Service for just a minute. I am still trying to get my hand around this. This is a very, very serious issue here. What happened in that service, that division, or, better still, what did not happen that allowed this to continue to go on and on and on? Could you speak to that for just a moment?

Mr. HASHMI. Congressman, thank you for that question, and forgive me for clarifying. I believe you are talking about the Technology Transformation Service, that division.

Mr. MFUME. Mm-hmm.

Mr. HASHMI. Yes, thank you for that question. Listen, I can't speak to events from 2, 3, 4 years ago. Certainly, the IG reports speak for themselves. What I can speak to and which I want to reemphasize is that these misrepresentations, in my experience, and I have been a public servant for many, many years, represent the absolute unacceptable approach for government to conduct business. And that is exactly why in 2022, when I first became aware of the issues, I made sure that internally and with the IG, we have full transparency.

My first action, immediately upon learning it, was reach out to our customers to ensure that they know the full truth so that we are not continuing this cycle of misrepresentation that, for whatever reason, has existed for many years. That notification then led to several communications that we continue to do to this date. The next opportunity for me was to make sure that people are held accountable, and we want to make sure that we see the full truth, we identify all the details, and we take management employee disciplinary actions immediately. Last, it is clear that internal controls need to be in place, and clearly, they were not sufficient to prevent this sort of thing happening.

Mr. MFUME. OK.

Mr. HASHMI. And so, my third action—sorry, sir.

Mr. MFUME. No, no, no. My time is just about up, but just one quick question, if I might, Mr. Chairman. We rely on *Login.gov* to help us to root out potential fraudsters. There are a lot of bad guys out there, and for this to have gone on this long, we don't know if they were siphoning off money from essential government programs. And has anybody in any way worked with the Justice Department to make them aware of the fact that there could be possible criminal activity here or was possible criminal activity that denied everyday taxpayers the right to believe that their money was being used as it should?

Mr. HASHMI. If I may, sir. Just in full disclosure, this particular issue that we have worked with the IG on does not represent a cybersecurity breach or somebody's information being exfiltrated. While these misrepresentations are absolutely unacceptable, we have no evidence based on all the assessments over the last year that this has led to any particular cases of——

Mr. MFUME. Of fraud. We don't know because we are not looking, apparently. I don't think we can make the assumption that nothing bad happened when for five years this misrepresentation occurred, and there are a lot of programs within the government that go every day to help people that are affected by this kind of a breach. I don't want to prolong it. I will leave it there. Mr. Chairman, thank you. I yield back.

Mr. SESSIONS. Thank you very much. The distinguished gentleman from Arizona, Mr. Biggs, is recognized for five minutes.

Mr. BIGGS. Thank you, Mr. Chairman. You know, Mr. Hashmi, I am baffled. You have now said this was unacceptable five times. This is more than unacceptable. This is, in my opinion—is criminal. I looked up the definition of "fraud," just the criminal definition of "fraud." Make sure I am still there on that. It is a deliberate scheme to obtain financial or other gain by using false statements, misrepresentations, or concealment. To me, that is the classic element of fraud. That is fraud. That is criminality. Somebody should be held accountable. And I want to ask about 18F. Tell me what 18F was, please?

Mr. HASHMI. Yes, Congressman. Thank you. 18F is a division within the Technology Transformation Service. The core issue that the 18F tries to solve for is the need to bring in modern technology talent to help agencies——

Mr. BIGGS. And where did they come from? Where did these guys and gals, this group of 18F, where did they come from to get into the TTS division and start working on this?

Mr. HASHMI. Sir, we recruit personnel within 18F from all the different sources that any agency recruits for: private sector——

Mr. BIGGS. And they were the group that were working on *Login.gov*. They are the ones that said we are going to make this comply with IAL2, right?

Mr. HASHMI. With respect, Congressman, 18F is a separate division from *Login.gov*. The two divisions are not the same.

Mr. BIGGS. But they had a contract. They were working with *Login.gov*. Isn't that true? They are a quasi-governmental institution. They are not a government entity. They are a quasi-government entity. Is that not right?

Mr. HASHMI. With respect, Congressman, they are a government entity.

Mr. BIGGS. OK. So, they are all in the government?

Mr. HASHMI. Yes, sir.

Mr. BIGGS. OK. They were the ones working on *Login.gov*, they are the ones that were trying to get contracts, *et cetera*, and they are the ones that made the claims that they were going to make this IAL2 compliant. Isn't that true?

Mr. HASHMI. Again, with respect, Congressman, they are a different division from *Login.gov*. They are not related.

Mr. BIGGS. You are telling me that they had nothing to do with getting to IAL2. Is that what you are telling me?

Mr. HASHMI. Congressman, yes, the *Login.gov* team is responsible for that compliance and misrepresentation.

Mr. BIGGS. So, 18F had nothing to do with it?

Mr. HASHMI. Sir, in this particular instance, 18F is a separate——

Mr. BIGGS. OK. So, who was it that was making the misrepresentation saying that we are IAL2 compliant? Let's see. I am looking at the timeline, November 2019. That is when GSA started billing customers for *Login.gov* IAL2 compliance.

Mr. HASHMI. As is outlined in the IG's report, yes, this misrepresentation does go back several years.

Mr. BIGGS. Who is it? I said who. I know it goes back. I have read the report. Who was it that was making the representations beginning in November 2019 when you are soliciting contracts. Not just soliciting. You are billing customers fraudulently for services that you cannot render. Who was doing that?

Mr. HASHMI. Sir, as I have mentioned in my testimony, several folks within the *Login.gov* team were identified.

Mr. BIGGS. Who?

Mr. HASHMI. Like I said, sir, several folks who are no longer with the Agency.

Mr. BIGGS. Who, and have they been referred for prosecution? Criminal fraud requires a deliberate act, and you got $10 million that came in. That was, I think, the IG's report, $10 million from clients. That seems deliberate. There was consideration exchanged, and somebody deliberately misrepresented things. And then they submitted requests for an additional $187 million. Did they receive anything prior to that from the same organizations? From the TMF, they wanted $187, Technology Modernization Fund. Did they get anything prior to 2021?

Mr. HASHMI. Not to my knowledge, Congressman, no.

Mr. BIGGS. I will ask the IG, Ms. Ochoa. Did they receive anything other than that $10 million from clients? I thought you said they received additional funds.

Ms. OCHOA. Our report speaks to the $187 million they received from Technology Modernization Fund.

Mr. BIGGS. So, when I read the report, it said that in September 2021, that is when they ultimately received $187 million because they could comply, and that is on page 18 of your report. That is because they claimed that they were in compliance with IAL2. Is that right?

Ms. OCHOA. They did, yes.

Mr. BIGGS. OK. Well, Mr. Chairman, there is so much more that I would like to ask, and I am out of time, but, I mean, I have asked who was fired. They won't tell me.

Mr. SESSIONS. Who was fired?

Mr. BIGGS. Yes, who was fired, I have asked, and they said they haven't made referrals criminally. This is a criminal fraud. I want to know where the money is, when we are going to get it back, and I want to know who is being held accountable, Mr. Chairman. I yield back.

Mr. SESSIONS. I want to thank the gentleman and all Committee Members. I believe that this entire Committee sees the purpose of this hearing. The purpose of this hearing is to begin this face-to-face investigation by the IG, by those people who, I think, have reasonably and professionally owned up to the frailties. And this is the beginning of that, and I will assure the gentleman from Arizona, and the gentleman from Louisiana, as well as others on this Committee that we will be very pleased to get these answers. We will work with the GSA to have it done in a professional way that will include Mr. Mfume and myself on that request, and I thank the gentleman for his insistence. Thank you very much. Excuse me, just a moment. Oh, you said thank you?

Mr. BIGGS. I want to say, thank you, Mr. Chairman.

Mr. SESSIONS. Oh, yes, sir. Mr. Frost, you are recognized for five minutes.

Mr. FROST. Thank you, Mr. Chairman, and thank you to our witnesses. On the website of *Login.gov*, it states that it is the public's one account for government. Agencies that use *Login.gov's* platform include SBA, Department of Defense, Veterans Affairs, Department of Agriculture. Each of these agencies has a complex mission that involves engaging sensitive information, including the personally identifiable information of American citizens, which is incredibly important and sensitive. To properly secure this information, the National Institute of Standards and Technology establishes guidelines for digital identity standards. Mr. St. Pierre, how does the NIST ensure the security and strength of this type of information and the verification standards, and why are these standards so important?

Mr. ST. PIERRE. Thank you for the question. So, we developed them in an open and transparent process with industry, other government agencies' experts, and other government agencies, and industry, and academia, and other colleagues. This guideline is to help agencies develop digital identity systems and ensure that they are secure. It is based on a risk management or risk approach, and so there are different levels of security that can be achieved. The agency would assess the risk of their system, and then based on that risk assessment, that determines what level of controls they need. The highest level of controls would be for the highest risk, and so that is the way the process works.

Mr. FROST. Got you.

Mr. ST. PIERRE.. Yes.

Mr. FROST. Yes. Thank you so much. Madam Inspector General, when Federal agencies partner with *Login.gov* or any identity proofing service, why is it critical that the agency have trust with that service provider?

Ms. OCHOA. As I understand it, the agencies choose for themselves the risk level that is necessary, depending on the services that they are offering. And so, they are then representing to their customer taxpayers that their information will be secure, so it is critical that they trust the platform that they have chosen.

Mr. FROST. Yes. And even on the website, I mean, in the mission statement, it says, "When it comes to logging into government websites, agencies trust *Login.gov* to help protect their users' information, and the public trust *Login.gov* to streamline their sign in process." *Login* knew that trust was foundational to their success, and also to the success and to the American people using the platform, which makes the breach of trust so upsetting.

Commissioner Hashmi, in the OIG report, you attribute *Login.gov*'s breach of trust to, and we kind of spoke about this earlier, the culture of oversight being burdensome. Can you explain what you meant by that and why the FAS didn't do more to address this culture when it first assumed responsibility of *Login.gov*?

Mr. HASHMI. Well, thank you for the question, Congressman. I wholeheartedly agree with you. Trust is the key currency that we must maintain when we build services for other agencies. I will say that in order to ensure that trust, it requires that we internally have adequate internal processes and internal controls in place. It is clear from the report that that was not the case here. And for many years, that lack of internal controls led people to make statements without appropriate oversight, without checking and balancing, without third parties looking at those statements and making sure that they are sufficient, accurate, and complete. So that is one of the reasons why the immediate action for us was not just to notify customers, but being as transparent as possible. And then secondly, immediately focusing on the internal controls that we need to put in place.

Mr. FROST. But why don't you all do more sooner?

Mr. HASHMI. Well, sir, I can only speak to when I became aware of the issues and the actions that I took. Of course, many people in the past have made choices that I can't speak to. But my job, as now that I am aware and, again, is to not only take the actions that we have done and scale them, but also fully implement the recommendations that the IG has made. I do believe that those recommendations, taken as a whole, will make the program stronger, and ultimately, it is up to us to earn that trust back. And with one phone call at a time, I am making sure that agencies have full transparency into what we do and how we do it, and then, ultimately, they can make informed decisions about whether Login is the right solution for them.

Mr. FROST. Thank you. I appreciate the comprehensive plan you have laid out today to remedy this very, very troubling matter. *Login.gov* serves a critical purpose for Federal agencies, as we all know, and I just want to urge you to ensure that the remedial actions discussed today are implemented quickly and completely to protect the privacy and data of our people. Thank you so much. I yield back.

Mr. HASHMI. You have my commitment, sir. Thank you.

Mr. SESSIONS. Mr. Frost, thank you very much. This is the kind of professional, I believe, response and questions that we are after,

and I want to commend the panel and our Members for their behavior in that endeavor. Thank you very much. The gentleman from South Carolina, Mr. Timmons, is recognized for five minutes.

Mr. TIMMONS. Thank you, Mr. Chairman. This has been very productive. I appreciate that we have wasted millions of dollars creating *Login.gov* and them alleging that they were providing a service that they do not, but it actually costs tens of billions of dollars, particularly as it relates to SBA's work during the pandemic. They were responsible with identifying PPP and EIDL applications.

So, we have already identified that those applications likely resulted in tens of billions, if not a hundred billion dollars, being stolen, outright theft. And if *Login.gov* had done their job, those applications would have two-factor authentication. We would be able to say this is actually who did this. It would be harder to commit that fraud, and if you did commit that fraud, you would be held accountable because we knew who you were. So, it is not just ten million dollars that we have lost. It is tens of billions of dollars because of a fraud that was allowed during the pandemic.

Inspector General Ochoa, I guess my question is, how did GSA's misrepresentation of *Login.gov*'s capabilities affect SBA's work during the pandemic, particularly as it relates to PPP and EIDL programs? And is it fair to say that *Login.gov* is a contributing factor, to the extent of the fraud that we saw and makes it harder to hold people accountable? Is that fair?

Ms. OCHOA. You are asking a very broad question about and a good question about the——

Mr. TIMMONS. If *Login.gov* had done what it said it could do, would it be harder to steal from PPP and EIDL and easier to hold people accountable that did?

Ms. OCHOA. IAL2 is meant to be a fraud detection.

Mr. TIMMONS. So, we would have a higher degree of confidence to know who took out these fraudulent loans, well, just who took out the loan. I mean, PPP and EIDL, thousands and thousands of loans were taken out by people that weren't who they said they were, so this would prevent that. If *Login.gov* had been able to do what they allege they were doing, that would not be possible.

Ms. OCHOA. I can't speak to SBA's experience with *Login.gov*. To determine the impact on any particular agency requires a robust investigation into those agency operations. This is beyond my jurisdiction.

Mr. TIMMONS. I will shorten the answer, it did. SBA relied on *Login.gov*, and they lied with what they were able to do, and it is going to cost us tens of billions of dollars if we ever get it back. Let's go to Acting Director St. Pierre. So, if *Login.gov*'s capabilities had not been misrepresented and the IAL2 standards were in place, do you think that SBA would be able to better identify the individuals that took out these pandemic relief loans and possibly make it easier to prosecute them?

Mr. ST. PIERRE.. Thank you for the question. So, NIST is neither an oversight or enforcement agency, but your question is about if IAL2 had not been implemented, is that correct?

Mr. TIMMONS. Well, if it had been effectively implemented——

Mr. ST. PIERRE.. OK.

Mr. TIMMONS [continuing]. Because SBA, they thought they did, but they don't, so we have all of these loans out there that we don't know who got them.

Mr. ST. PIERRE.. So IAL2, as you said, it ensures that you have confidence in who you are speaking to. So, without mitigating that, you would not be mitigating the level of risk that your system design had intended.

Mr. TIMMONS. You would just know who you are talking to?

Mr. ST. PIERRE.. No, I am saying, if you did not implement it, you would not have the level of mitigation that you had planned for if you did not implement IAL2.

Mr. TIMMONS. OK.

Mr. ST. PIERRE.. However, I can't speak to what level of fraud may or may not have been attributable to the system.

Mr. TIMMONS. If *Login.gov* had worked as intended, we would have a higher degree in confidence in knowing who we were communicating with through the SBA portal?

Mr. ST. PIERRE.. So, I can't make a determination on that because I don't know enough. I am not an oversight agency. We don't look at this overall system and if there are other controls that they have with other——

Mr. TIMMONS. OK. Well, the fraud that was perpetrated by *Login.gov*, as it relates to SBA, makes it harder for us to hold individuals that committed fraud accountable because we don't necessarily know who they are because *Login.gov* didn't work as it was intended. Given all of these problems with *Login.gov*, I guess my question is, there are conversations about an executive order to expand its use. I would say that that is just a terrible idea. I mean, we need to reevaluate the effectiveness of it. We need to confirm that it works. Social Security, VA, and the IRS have already went with a third party that is able to actually do what they say they can do. So, I mean, we need to evaluate all of our options to make sure that we are actually getting the service that we are paying for. I would pose that as a question, but at the end of the day, I am out of time. I am sorry.

Mr. Chairman, this is very important. We cannot keep wasting taxpayer dollars, and it is costing more than we have even talked about. Thank you for having this hearing. With that, I yield back.

Mr. SESSIONS. Thank you very much. The gentleman is correct, and Mr. Mfume and I intend to do that. You would be a part of the follow-up and the opportunity as we meet with those leaders of GSA. And thank you very much. The gentlewoman, Ms. Lee from Pennsylvania, is recognized for five minutes.

Ms. LEE. Thank you, Mr. Chairman. I would like to refocus just for a moment on what began this whole incident. At the heart of the misrepresentation by *Login.gov* was one official's attempt to protect citizens from discrimination by algorithms. So, to quote one of the messages found in the investigation, "The benefits of the liveness/selfie do not outweigh any discriminatory impact." I am not praising his actions, but while we are weeding through the facts and looking for a way forward, we must do better to bring more diverse perspectives into the mix. Facial recognition technology is becoming more accurate, but time and time again, these

systems have been found to not work for Black women, for non-binary people, and for Asian people.

Mr. Saint Pierre, what actions are being taken in the industry to improve facial recognition technology and decrease bias in the systems?

Mr. ST. PIERRE.. So, thank you for the question. So, NIST has actually looked at this issue and done a study of bias in facial recognition algorithms that was published in 2019, and that study did find that nearly all algorithms have bias for demographic differentials. However, it is important to note that those algorithms, they are the best algorithms too, have a significant difference from the lowest-performing algorithms, and it is also important to note that over that time, since then, they have improved as well. And so that is a positive to see that those algorithms are improving.

Ms. LEE. Thank you. In response to the valid criticism of the issues with *Login.gov*, GSA is planning to complete an equity study to better inform future use of biometrics. Mr. Hashmi wrote that he hopes the equity study will help GSA "understand the current technological barriers to equitable remote identity proofing services for the public." Mr. Hashmi, when did GSA launch the equity study, and what is the timeline for its completion, and will it be made public?

Mr. HASHMI. Thank you very much, Congresswoman. Just for the record, in response to this very important issue, all of the actions that I have outlined in my testimony remain strong, obviously, making sure internal controls are in place, making sure we are holding employees accountable and being transparent with our customers. In reference to the equity study, ultimately let me be very clear. Any technology that we implement that face and allow Americans to access government service has, in my view, to meet three very important criteria. It must balance the need for access for all Americans against making sure that their privacy is protected and ensuring that appropriate fraud management controls are baked in. That is our goal with *Login.gov*. We continue to make progress there.

In terms of the equity study, that is work we started a while ago, independent of this particular investigation, to ensure that we have full understanding from academia, from research organizations and the private sector on the best and brightest technologies that are available to be able to test and validate them, and to be thoughtful about how to implement those technologies. At this moment, we do consider that there are significant privacy implications as well as access implications to using certain technologies like facial recognition, as you mentioned. We want to make sure that we continue to investigate it, and we will implement those technologies when they become ready to go live.

Ms. LEE. Thank you. Our STEM industry overall is severely lacking in diversity. Black people make up just nine percent of the STEM work force and Hispanic people just eight percent. Last year, GSA released its equity action plan to advance racial equity and support underserved communities. The plans helped these goals of integrating diversity, equity, and inclusion in everything from delivering projects to designing websites. Mr. Hashmi, what

specific steps has GSA taken since announcing this plan to better include diverse people and perspectives?

Mr. HASHMI. Thank you, Congresswoman. They are a very important topic. Unfortunately, in 50 seconds, I will probably require more time to have a fuller briefing for you. We are very proud of the work that we have done over the last two years.

Mr. SESSIONS. The gentleman is recognized for four minutes.

Mr. HASHMI. Thank you, Chairman. Let me outline some of the things we have done to pursue—make progress in that front. In the Federal Acquisition Service, our primary focus and continues to be to make sure that diverse businesses become part of the Federal marketplace. We have done significant work in that front. As of today, we are proud to say that over 35 percent of the dollars that flow through the Federal Acquisition Service go to small and disadvantaged businesses, including those that are considered to be in the categories such as women-owned small businesses, hubs-owned small businesses, and veteran-owned small businesses. We also are doubling our commitment to flowing more acquisition dollars toward those businesses that are designated as a special category, disabled. So, those are just two examples.

In the area of technology transformation service, we recognize that the products we make need to serve all Americans equally. We have seen not just issues with equity around certain demographics, but we have seen that technology sometimes leave behind people in rural America who don't have access to broadband capabilities, modern devices, smartphones, and such. So, we continue to think about ways that we can bring all those Americans into the fold because in many cases, those communities are the ones that need access to government services the most.

We are proud of the work we are doing. Certainly, a lot more needs to be done yet. We will be happy to provide a fuller briefing to your staff if you are interested.

Ms. LEE. Just very quickly. Thank you, Mr. Chairman, for yielding the gentleman four minutes. I do want to ask, how successful?

Mr. SESSIONS. The gentleman is recognized for five minutes more.

Ms. LEE. Yes. OK. I just wanted to ask, to that same question, how successful you think you have been so far in implementing this plan.

Mr. HASHMI. In some cases, we are very excited about the progress. In fact, we are ahead of schedule. Our equity study and all the results are actually publicly available on our website. If you are interested, you can go to *GSA.gov*, not only take a look at our plan, but also see how we are working against that plan.

Ms. LEE. Thank you. I yield back.

Mr. SESSIONS. Thank you very much. It is important for me and, I think, Mr. Mfume, when we have these hearings to allow each of the Members the proper amount of time for them to always ask the questions, receive an answer back, and so I hope that the gentleman would recognize how important this is. Before I ask my first question, I am going to come to the gentleman—I am very happy doing this—for a second round of questions. The gentleman is recognized for five minutes.

Mr. MFUME. Thank you, Mr. Chairman. You are gracious. This is not being lost on this hearing. I do appreciate it. I do want to say two quick things. I want to associate myself with the remarks from the gentlewoman from Pennsylvania, particularly as it relates to the inherent bias, Mr. St. Pierre, and facial recognition technology, and to ask in that regard, since it has been four years since you undertook the review in 2019, could you provide this Committee with what has been accomplished or what has taken place to make that facial recognition less biased in the last four years? That would be helpful.

Mr. ST. PIERRE.. Yes, thank you for the question. So NIST's role in this is to, in that particular instance of measuring and testing those algorithms, is to do just that, is to measure the performance of the algorithms because we realize how important it is to understand how they perform and how they perform whether they include bias in their determinations, in their outcomes.

NIST is not directly involved in the development of these. These are developed by outside organizations, industry. So, we believe that our testing helps advance the technology and helps to improve it so that we can avoid and decrease the amount of bias in these algorithms, which is what we have seen over time that our tests since 2019 have shown a decrease in the amount of bias. This does depend on the data you are using and the use case, *et cetera*, but the encouraging thing is that over time, we have seen, through our testing, improvements in the technology.

Mr. MFUME. Yes, I would just like to get a summary of the assessment. Since you test, test, test, I am sure there is an assessment after each test that are pointing in one direction or another. If you could just provide a summary of that, that would be helpful. At least it would assure me that there is progress being made as a result of your testing for certain things at NIST.

Mr. MFUME. The other thing is that I cannot get away from this whole issue of taxpayer dollars and what is lost as a result of what we have seen over the last five years or so. The government is talking about cutting back on SNAP benefits for very needy and poor families. And all I can think about is how much money has been lost as a result of people siphoning off money by deliberately and, in some instances fraudulently, misrepresenting the truth. That really concerns me because we don't know what that number is, but I know where those needy people are, and I know the fight that it has taken to make sure that dollars get to them who deserve it. I am concerned about the bad guys. I keep talking about them because I think they are everywhere and, you know, the fraud that we have seen in the PPP program and EIDL, which this Committee, the full Committee has been overseeing, is alarming.

And now I have got confidence in Administrator Carnahan. I think she is doing the right thing and doing it in the right way to save taxpayer dollars. But I just cannot underscore enough the fact that I feel like a heist has taken place, and nobody knows who that masked man was that rode off into the sunset, and whoever it was rode off with a lot of money by misrepresentation and misrepresenting the truth. So, Mr. Chairman, thank you for graciously giving me some extra time. I yield back, and I thank you very much.

Mr. SESSIONS. Thank you very much. Does the gentlewoman from the District of Columbia seek time?

Ms. NORTON. I do, Mr. Chairman.

Mr. SESSIONS. The gentlewoman is recognized for five minutes.

Ms. NORTON. I thank you. I want to punctuate that GSA's misrepresentation with *Login.gov* plagued both administrations. The GSA inspector general's findings about *Login.gov* staff actions are troubling, but under this administration, GSA has been proactive about addressing these issues from the moment GSA leaders were made aware that some staff had been misrepresenting *Login.gov*'s capabilities and customers. Mr. Hashmi, please describe the steps GSA took upon discovering this problem?

Mr. HASHMI. Thank you, Congresswoman. It is an honor to meet you in person and to testify before you. I appreciate the question. As I mentioned in my opening testimony and to reiterate here, these misrepresentations represent the worst in how a government should operate. I take this very seriously. I have been a public servant for most of my professional career, and as soon as I became aware of these misrepresentations earlier last year, I took immediate action.

Here's the list of actions that I have taken, and the overall GSA management leadership team has taken. First, my immediate focus and priority was to inform our customers. We want to make sure that we are proactive, and we make sure that our customers understand exactly what the capabilities of our products are so they can make informed decisions and are not basing those decisions on misrepresentations that we have made. Not only our customers, but working with our Office of General Counsel, immediately informed the Inspector General's Office as well as other stakeholders, including the Technology Modernization Fund Board.

Second, I wanted to make sure that we get into the heart of exactly what happened, and if there are people who knowingly misrepresented this situation, are held accountable. As a result, we initiated a management inquiry and started to analyze the facts. Those facts subsequently showed that certain members of the Login team did, indeed, misrepresent intentionally, and as a result, we immediately initiated an employee disciplinary inquiry. As a result, all those who misled intentionally, that we are aware of, are no longer employed by the Agency.

Third, it is clear from the IG's report, as well as our internal management review, that internal controls have to be put in place so that this doesn't happen again. One of the key internal controls that we put in place was establishing a separate division within the Office of General Counsel that is not pressured to deliver, but only be accountable for compliance and oversight. That division is now responsible for reviewing every single document that we sign with our customers, every single communication that the program makes, and, in fact, they are providing those services not just for *Login.gov*, but all of technology transformation service.

By having this internal control and, of course, building on that, as I brought a new leadership, I immediately removed the existing *Login.gov* director, brought in new leadership. That leadership, as soon as they were brought on board, my first task for them was to conduct a full top-to-bottom review of the program to include per-

sonnel, contracts, finances, billing, and much more. And then last, I want to again reiterate my appreciation for the work that the IG has done and their recommendations because those recommendations also form a good basis for us to continue to take strong action in this case.

Ms. NORTON. Well, Mr. Hashmi, did these mitigating actions begin before the OIG published their recent report?

Mr. HASHMI. Yes, ma'am. These actions were initiated immediately upon learning about this issue earlier last year. We have been taking these actions deliberately over the last year, and we will continue to build on them as we incorporate the OIG's recommendations.

Ms. NORTON. Mr. Hashmi, at GSA, for example, we assigned the director of *Login.gov* in February 2022. Since leadership learned of the concerns with *Login.gov*, the office has undergone extensive turnover in leadership. What is GSA's plan to ensure long-term stability in this new leadership?

Mr. HASHMI. Thank you for that question, ma'am. My first and main priority is to bring a culture of accountability and transparency to this office and in everything we do. That is why as soon as the IG made the report public, I shared a copy of it with every single employee within my charge because I want to make sure that everyone who works for me understands that our responsibility goes beyond just getting the job done, but also doing it in full transparency, with accountability.

To your question, ma'am, we have seen turnover. However, I remind staff that the reason why we are here is to serve the American people. One of the things that we need to do is to continue to hire aggressively people who not just have the technology skills, but bring the right ethical and accountability framework to the role and we continue to do so.

Ms. NORTON. Thank you. I see my time has expired.

Mr. SESSIONS. Does the gentlewoman seek additional time?

Ms. NORTON. I would like additional time.

Mr. SESSIONS. The gentlewoman will be recognized for five minutes.

Ms. NORTON. Soon after Dan Lopez became the new director of *Login.gov* in September 2022, he began conducting a top-to-bottom review of the office to determine other potential improvements. Mr. Hashmi, how is GSA supporting Mr. Lopez's review?

Mr. HASHMI. Thank you for that question, ma'am. One of my first actions as soon as he came on board was to direct him to conduct this top-to-bottom review. I have also made resources available to him to conduct a full analysis of people with expertise in contracting with—on finance and budgeting, to making sure that he has resources, not just in his area of expertise, which is technology and management, but a full breadth of capabilities that he needs to evaluate this program fully.

We are working very closely with our Office of Chief Financial Officer as well as our Office of General Counsel to evaluate all aspects of that program. We will continue to provide that support, and as results become available, we take action immediately. As a result, one of the internal controls we have put in place is that all contracts that are managed by the Technology Transformation

Service have a review that my staff and the Office of the Acquisition Services, the Federal Acquisition Service conducts.

With this independent review, we want to make sure that all contract actions meet the Federal acquisition regulation and appropriate regulations, policy, and law. Similarly, we are taking similar actions to make sure that we are managing our human resources appropriately, our finances, budgets and forecasting appropriately and, again, continue to communicate transparency with our customers in collaboration with our Office of General Counsel.

So, to answer your question, ma'am, significant resources are being put into it because this is my top priority. I want to make sure that this program, which is so important for so much of the work the Americans expect from their government. The success of this program is paramount for the government to deliver digital services to their constituents. We want to make sure that this is done in transparency and full accountability because in this particular case, we feel very strongly that this program has a right philosophy to add value to the American people, and we want to make sure that we have the right accountability in place so that we can continue to do so.

Ms. NORTON. Finally, Mr. Hashmi, what steps are GSA and Mr. Lopez taking to change the *Login.gov* work culture from one that allowed this misrepresentation to one that demands transparency and integrity?

Mr. HASHMI. Thank you, again, Congresswoman. As I mentioned, some of the controls that we put in place with our Office of Chief Financial Officer, General Counsel, put required controls in the process so that misrepresentations are caught before they are made. While we are very proud that we have been able to bring in leadership with the right focus on ethics, transparency, and accountability, we cannot always rely and mistakes sometimes can get made. So, we want to make sure that the process is in place to protect those things from happening, No. 1.

No. 2, Mr. Lopez has already also been looking to make sure that the right people are brought in for the right roles. One of the challenges that he has identified, and we are happy to provide additional information to your office at your interest, is that we need more experts who are not just technologists, but experts in fraud management, and those skills are very different. And so, we are starting to build a small team of folks who have previously not only litigated, but processed fraud cases so that we can really understand how do we build the products that are actually designed to prevent those cases from happening. Those are examples of him taking initiative to identify the gaps that exist and then to continue to fill those gaps as he moves forward.

Ms. NORTON. Thank you very much. I appreciate the extra time, Mr. Chairman.

Mr. SESSIONS. I thank the gentlewoman for taking her time to be at this important Subcommittee and respect her questions. I will now yield myself such time as I consume as the last questioner, and I want to really relate this. I know it is a Mr. Hashmi show today, it has turned into that, but, really, all three of you could answer this.

Looking back at it, I wonder how prudent it is to look at on a case-by-case, which means, I think, one at a time, anybody that was currently in the system, whether they had come through the filter improperly, they might be the wrong person, or view it, or—can you talk about how you got a database. How you vet that now based upon what we know? Mr. St. Pierre?

Mr. ST. PIERRE.. Yes. Thank you for the question. In this role, our role is to develop the standards and guidance that are used to develop identity management systems. We have no oversight or enforcement role, so I really couldn't speak to how that would be addressed.

Mr. SESSIONS. Mr. Hashmi?

Mr. HASHMI. Thank you, Chairman. I wholeheartedly agree with the need to ensure that we continue to invest in fraud mitigation capabilities within the Federal Government. I want to reiterate our strong belief that *Login.gov* is a strong product and it has many fraud mitigation controls already in place. For example, one of the gentlemen had raised a question of two-factor authentication. *Login.gov* requires two-factor authentication in all cases. We also do controls such as phone and address verification, making sure that the device the user is using is actually tied to them by name. Many other controls exist.

The key failing here and the key thing that prevents us from achieving that IAL2, the primary reason is continuing to investigate whether biometric technology is the right thing to implement at this point in the government. However, let me just be very clear. I want to say it for the record. IAL2 compliance—*Login.gov* does not meet IAL2 compliance. It hasn't ever. The misrepresentations are absolutely unacceptable. We strongly believe in the product. We believe in the fraud capabilities the product already offers. For that reason, we will continue to invest in those capabilities.

I mentioned one of the things that we have implemented recently is a pilot program to allow Americans to prove their identity in person, partnering with the U.S. Postal Service, because there is nothing more secure than asserting your identity in person, so in certain circumstances that option becomes available. These are the kinds of investments we will continue to make because, ultimately, the goal should remain to create a service that creates access, protects people's privacy and has adequate and strong fraud prevention controls built in.

Mr. SESSIONS. OK. Well, that was the next question I was going to ask, but let me go back. I'm not making my point here. You have got people who are in *Login.gov*, and we believe that we oversold what you have done to make sure they are who they are, right? You told people you used these processes. Are you going back to the existing people that are in the data bases, and then when you get these techniques, running that against these people? If not, I mean, I still don't understand. I think some of the people in the data base, can't tell you how many, might not be necessarily who they are, or you may want to double check on them. I did not hear you. That was my question. Did you hear my question?

Mr. MFUME. I did.

Mr. SESSIONS. OK. What am I saying wrong to get the answer?

Mr. MFUME. I don't know, it is a matter of framing it. We all hear it differently, but I trust that Mr. Hashmi, who has become the center of this discussion, probably has a way to respond.

Mr. SESSIONS. OK. People who are in the data base today, you don't know if your eggs are fresh. You don't know if that is really who it is, because you may have had some frailties. Are you going to check those that are in there today against some system that you then develop, reassessing the customer? That is what I am asking.

Mr. HASHMI. Yes, thank you, Chairman, and I do apologize for perhaps not understanding.

Mr. SESSIONS. My fault. It is not yours.

Mr. HASHMI. Well, let me just say this, sir. All the controls that I mentioned earlier, we are checking all of the accounts against them constantly. If I may be allowed, sir, again, the key thing that we do not implement today is facial recognition. Because of that lack of, you know, that capability, we have no mechanism to test these identities with facial recognition. However, we employed third-party data sources. We worked with state DMV offices. We work with many different data sources like that to ensure exactly what you and I agree needs to be done, which is to ensure that we identify if there is any fraud that exists in the system and take care of it immediately.

All the agencies that we work with for identity verification, through our communication since last year, we have made sure that they understand exactly which accounts have come into their systems and they have independent ways to validate and mechanisms so that those individuals can be subsequently vetted again. So, all the controls that I mentioned—address verification, phone verification—we constantly employ all of them as well as third-party-based data sources that can allow us with an independent view of who is saying what they are. We do that every day, and all these identities are constantly validated through all these controls.

Mr. SESSIONS. Good. That makes sense to me. I think that answered my question. The last question I had, which I am not sure really what the answer might be. But looking across the free enterprise commercial space, is there a best practice and is that the same as the government, or do you think someone has a lens, a camera, a process that we just don't want to get at, or can't get at, or unwilling to pay it, or are we leading edge? That is, I guess, is the question?

Mr. ST. PIERRE.. So, what I would say is we work with industry, the leading experts in industry, government and other agencies, and for IAL2, there are a number of ways to meet IAL2. One is a physical comparison that can be either done in person or remote. One is a biometric and one is a compensating control that would have to be documented and justified. And also, I would say that with respect to our draft version that is out, one of the things we have explicitly called for is more information and input from the industry, the experts, if there are ways to meet the same level of security that we feel is required to protect the Americans' data, that would meet that same level of security in a non-biometric fashion. So, that is part of our call in the draft, but the draft, I

mean, the IAL2, again, does have three different ways to meet the standard.

Mr. SESSIONS. All right. I want to thank each of you for being here. I want to thank your colleagues who have joined you. I see a good bit of recognition in the employee body that is behind you that they believe that they understand what we are trying to do today, that they understand the responsibility to be truthful about what they do. And it is perhaps a lesson to all of us, but I want to thank you, so thank you to everybody. I don't know whether, sir, you would wish to have closing, thank yous and comments, but the gentleman is recognized.

Mr. MFUME. Yes. Thank you, again, Mr. Chairman. I think it has been a good hearing. I want to thank all of the witnesses. And, Mr. Hashmi, I will go out on a limb here and say that I really trust your sincerity about wanting to end this. I could hear in your heart the sort of pain that is there because this is existing, and I want to commend you on immediately taking action when you got the information. And we are looking forward to the day when fraud mitigation and IAL2 compliance and everything else is sort of secondary.

But there was one thing I did hear that I am particularly interested in, also based on one of the questions that the Chairman asked, and that is that you are not just looking at fraud mitigation, but you are looking to bring in people who have actually prosecuted fraud and who can identify it in an early stage. That is very significant. I want to commend you on it. And as I said before, I have got a great deal of trust in Ms. Carnahan and her leadership there. We just don't want to relive the nightmare all over again, I guess, that is what we are all seeing here.

And Ms. Ochoa, we, in this Committee and Subcommittee, get to deal with a lot of inspector generals, as you might understand. I am just glad to see somebody other than a man sitting in that chair and to know that there is some gender equity taking place, particularly in that profession because I oftentimes believe that in many instances, the best man for the job is a woman. So, thank you, and I am just hoping that your example is replicated. You did a great job on this. I am still a little troubled about the redactions, and that is why I asked the question about the Justice Department, but we can deal with that at another point in time.

I just want to thank all of you again and your work also, Mr. St. Pierre, at NIST, and yield back to the Chairman so that we might move forward to the next phase of this. Thank you, Mr. Chair.

Mr. SESSIONS. The gentleman yields back his time and I thank the gentleman. So, please accept the same comments from me, the thanks to each of you. The need for follow up will occur. It will be quite direct and specific. We will give the GSA Administrator that opportunity to know that ahead of time. It will be done together, and it will be done on behalf of this Subcommittee.

With that said, without objection, all Members will have five legislative days within which to submit materials and submit additional written questions for the witnesses, which will be forwarded to the witnesses for their response. It is our expectation that you will respond to those questions.

Mr. SESSIONS. Please know that we appreciate and respect what you have done today and thank you for your service to the people of the United States of America.

This ends our hearing. Without further objection, the Subcommittee stands adjourned.

[Whereupon, at 4:19 p.m., the Subcommittee was adjourned.]