U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Accessible Version

December 20, 2022

The Honorable Gerald E. Connolly
Chairman
Subcommittee on Government Operations
Committee on Oversight and Reform
House of Representatives

The Honorable Thomas R. Carper
United States Senate

The Honorable Rob Portman
United States Senate

Information Management: Agencies Need to Streamline Electronic Services

With certain enumerated exceptions, the Privacy Act of 1974 prohibits disclosure of records to any person or agency, unless disclosure is pursuant to the prior written request by, or with the prior written consent of, the individual to whom the record pertains.[1] Accordingly, agencies have developed various procedures and forms by which individuals may establish their identity and request access to or provide written consent for the disclosure of their records.
To simplify and modernize this process, the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act) required the Office of Management and Budget (OMB) to issue applicable guidance. This guidance was to: (1) require agencies to accept electronic identity proofing and authentication; (2) create a template for electronic consent and access forms and requires each agency to post the template on the agency website; and (3) require each agency to accept electronic consent and access forms from individuals that have been properly identity proofed and authenticated.[2]

You asked us to review the implementation of the CASES Act at OMB and federal agencies. Our objective was to determine the extent to which OMB and selected agencies addressed the requirements in the CASES Act.

To conduct this work, we identified 119 agencies that reported Freedom of Information Act (FOIA) requests on the federal government's central website for FOIA in fiscal year 2020.[3] From

[1]With certain enumerated exceptions, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant written request by, or with the prior written consent of, the individual to whom the record pertains…" 5 U.S.C. §552a(b)

[2]Creating Advanced Streamlined Electronic Services for Constituents Act of 2019, Pub. L. No. 116-50, 133 Stat. 1073-74 (Aug. 22, 2019).

[3]The Freedom of Information Act (FOIA) provides the public the right to request access to records from any federal agency with certain enumerated exemptions. We obtained this information from https://www.foia.gov/about.html on Feb. 15, 2022.

those agencies, we chose 17 agencies that received 5,000 or more FOIA requests.[4] The 17 agencies selected were the Departments of Agriculture (USDA), Defense (DOD), Health and Human Services (HHS), Homeland Security (DHS), the Interior (DOI), Justice (DOJ), Labor, State, Transportation, the Treasury, and Veterans Affairs (VA); and the Environmental Protection Agency (EPA), Equal Employment Opportunity Commission (EEOC), National Archives and Records Administration (NARA), Office of Personnel Management (OPM), Securities and Exchange Commission (SEC), and the Social Security Administration (SSA).

To address this objective, we reviewed the CASES Act to identify the requirements directed to OMB and federal agencies. We also analyzed OMB's guidance on *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act* (OMB M-21-04) to determine whether the guidance included all of the elements required by the CASES Act.[5] In addition, we reviewed documentation from the selected agencies, including policies and procedures, plans for addressing the CASES Act requirements, and drafts of access and consent forms to determine whether it met the act's requirements. We conducted interviews with agency officials who were responsible for privacy and FOIA activities at the 17 selected agencies. We also interviewed OMB officials to identify the actions taken to implement the CASES Act requirements as identified in OMB M-21-04 by the November 2021 deadline. Further, we interviewed General Services Administration (GSA) officials to gain a better understanding of the issues and challenges that agencies are facing in meeting the CASES Act requirement related to remote identity proofing and authentication.

We conducted this performance audit from November 2021 to October 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

OMB Issued the Required Guidance, but Most of the Selected Agencies Have Not Yet Implemented It

As required by the CASES Act, in November 2020, OMB issued guidance to agencies that included all the required elements referenced by the CASES Act requirements. The guidance outlined agencies' responsibilities for accepting access and consent forms provided in a digital format from individuals who are properly identity proofed and authenticated. Specifically, by November 2021, agencies were to

- accept remote identity proofing and authentication for the purposes of allowing individuals to request access to their records or to provide written consent authorizing disclosure of their records under the Privacy Act;
- digitally accept the access and consent forms from any individual that was properly identity-proofed and authenticated; and

[4]In consultation with our research methodologist, we determined that agencies receiving 5,000 or more FOIA requests was a reasonable threshold for selecting which agencies to evaluate. Each of the 17 selected agencies handled a large volume of the requests and, as a whole, the 17 agencies covered 95 percent of the federal government wide FOIA request volume. The selection of 17 agencies cannot be used to make generalizable statements about the full population of agencies.

[5]Office of Management and Budget, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act,* OMB Memorandum M-21-04, (Washington, D.C.: Nov. 12, 2020).

- post the forms developed using the template provided in OMB's guidance on its website's privacy program webpage.

To assist agencies with meeting the technical requirements of the CASES Act, GSA assembled a discovery team in November 2021 to evaluate whether developing a web portal for agencies to address the act's requirements was a viable option. During the team's evaluation, they determined that: (1) individuals wanted to know the status of their records request to an agency but did not want to use another portal to submit their requests; and (2) individuals generally wanted fewer government forms. Ultimately, GSA decided not develop a government-wide solution.

As of September 2022, one of the selected agencies reported that it had fully implemented OMB's guidance. Specifically, SEC reported that it had addressed all of the requirements of the CASES Act. According to SEC Office of FOIA Services officials, the agency uses FOIAXpress and its Public Access Link (PAL) to connect Privacy Act requesters to Login.gov.[6] This solution provides multifactor authentication, such as the collection of a requestor's name, address, Social Security number, and driver's license information. Additionally, the SEC, through its website, allows for digital acceptance of access and consent forms from individuals who have been identity proofed and authenticated. Further, SEC demonstrated that PAL is available to the public and has posted access and consent forms to its privacy webpage. According to the same officials, OMB officials approved the use of Login.gov as a suitable solution to address the remote identity proofing and authentication requirement of the CASES Act.[7]

The remaining 16 agencies reported that they have not yet fully implemented the three requirements in OMB's guidance, but reported taking various actions, which are discussed below (see enclosure for additional details on the extent to which selected agencies addressed these requirements.)

Most Agencies Did Not Accept Remote Identity Proofing and Authentication

As of August 2022, 16 of the 17 selected agencies reported that they did not yet have the capability to accept remote identity proofing and authentication. Officials responsible for privacy activities acknowledged that agencies did not yet have these capabilities and that their efforts were at different stages of implementation.

- **Planning stage.** Nine agencies—DOD, DOI, DOJ, Labor, Transportation, VA and the EEOC, NARA, and the OPM—reported that they were planning to address OMB's requirements. One of these agencies, Labor, is planning to develop the remote identity proofing and authentication capability and the department intends to complete this requirement by December 2024. However, the other eight agencies had not established a time frame for when they would meet OMB's requirements.

- **Development stage.** Four agencies—USDA, HHS, DHS and the EPA—reported that they were currently developing a solution that would meet OMB's requirements and provided time frames for completion. For example, DHS reported that, in July 2022, the

[6]Login.gov is a secure sign in service administered by the General Services Administration (GSA) that provides identity proofing and authentication for individuals wanting to log into government websites.

[7]Login.gov's identity verification process does not currently conform to the Identity Assurance Level 2 requirements described in NIST Special Publication 800-63. National Institute of Standards and Technology, *Digital Identity Guidelines, Enrollment and Identity Proofing*, Special Publication 800-63A (Gaithersburg, MD: June 2017).

agency started to transition its current legacy systems to a new system that will provide the capability to accept remote identity proofing and authentication. DHS anticipates the system will be available by March 2023. In addition, USDA reported that they were planning to implement FOIAXpress configuration changes.[8] Once these changes are implemented, the agency expects to have the capability to accept remote identity proofing and authentication by the end of the second quarter of fiscal year 2023.

- **Testing stage.** Three agencies—State, Treasury, and SSA—reported that they were in the process of testing their respective solutions and provided timeframes for completion. Specifically, State reported that it is currently performing configuration testing and will then implement any necessary post-configuration changes. State estimates implementation to be completed by December 2022. In addition, as of December 2022, Treasury reported that testing has been completed. The department anticipates that implementation of identity proofing and authentication software will begin by the end of fiscal year 2023 and public access will be available after implementation is complete. Further, SSA reported that they intend to leverage their existing remote identity proofing and authentication capability to support the implementation of the CASES Act requirements in calendar year 2023.

Most Agencies Do Not Digitally Accept Access and Consent Forms

As of August 2022, 16 agencies reported that they have not yet implemented the capability to digitally accept access and consent forms from individuals that were properly identity proofed and authenticated. Officials responsible for privacy activities acknowledged that they are either still drafting digital access and consent forms or have not yet started drafting the forms.

- **Agencies drafting digital access and consent forms.** Nine agencies—USDA, HHS, DOI, State, Treasury, EPA, EEOC, OPM, and SSA—reported that they are drafting access and consent forms that will meet the act's requirements. For example, EPA officials responsible for privacy reported that the agency is developing a plan to update its access and consent forms using OMB's M-21-04 templates, and the plan is expected to be completed by April 2023. In addition, State reported developing access and consent forms that are posted to its FOIA and Privacy Act websites, but they will not be fully digitized until the end of 2022. USDA and SSA also provided time frames for when the requirements would be completed, but the five remaining agencies (HHS, DOI, Treasury, EEOC, and OPM) did not.

- **Agencies that have not yet started drafting forms.** Seven agencies—DOD, DHS, DOJ, Labor, Transportation, VA, and NARA—reported that they have not yet drafted access and consent forms, but they intend to develop them based on the language provided in OMB guidance. For example, DHS has not yet posted access and consent forms to its webpage but anticipates meeting this requirement with the implementation of its new system by March 2023. In addition, Labor reported that it has not yet posted access and consent forms using the OMB M-21-04 guidance to its website but expects to meet this requirement by December 2024. However, the five remaining agencies

[8]The purpose of FOIAXpress is to enable agencies to more efficiently receive, track, and respond to records requests and appeals made under the Freedom of Information Act and the Privacy Act.

(DOD, DOJ, Transportation, VA, and NARA) did not provide time frames for when this requirement would be completed.

Most Agencies Did Not Post Access and Consent Forms on Privacy Program Website

As of August 2022, 16 agencies reported that they have not yet posted access and consent forms on their privacy program's website. Officials responsible for privacy activities stated that they are moving toward addressing this requirement. For example, USDA reported that it is developing forms to post on its privacy program webpage and expects to meet OMB requirements by the end of the second quarter of fiscal year 2023. Further, State posted its paper-based access and consent forms on its FOIA and Privacy Act websites; however, the agency expects to have fully digitized its form by the end of 2022. While five agencies (USDA, DHS, Labor, State, and EPA) provided time frames for when they will meet this requirement, the other 11 agencies (DOD, DOJ, HHS, DOI, Transportation, Treasury, VA, EEOC, NARA, OPM, SSA) did not.

Agencies Identified Two Main Reasons for the Delay in Meeting OMB Requirements

The 16 agencies not yet meeting OMB requirements identified either technical delays and challenges or competing agency priorities as the main reason for their delay in meeting OMB requirements. Specifically:

- **Technical delays and challenges.** Twelve agencies (USDA, DOD, DOJ, HHS, DHS, DOI, State, VA, EPA, EEOC, NARA, and SSA) reported that they encountered technical delays and challenges. For example, DOJ reported that it faced challenges identifying a technical solution that could be implemented across the agency's decentralized request processing landscape while not causing confusion to requesters. In addition, the primary reasons that HHS reported for not implementing OMB guidance by the deadline were delays in updating its existing system and the need for a solution that uses Identity Assurance Level 2.[9] Further, EEOC and NARA reported that their technical delays resulted from waiting for GSA to develop a government-wide CASES Act solution. As agencies move forward in implementing OMB guidance, it will be important for them to evaluate ways to overcome technical hurdles.
- **Competing agency priorities.** Four agencies (Labor, Transportation, Treasury, and OPM) reported that they had implementation delays primarily due to competing agency priorities. For example, Labor reported that its resources to address OMB M-21-04 were occupied with other activities, such as addressing the SolarWinds software hack, supporting the IT needs of the American Rescue Plan Act, creating solutions to collect and track employee COVID-19 vaccine status, and complying with requirements of Executive Order 14028 on Improving the Nation's Cybersecurity.[10] In addition,

[9]Identity Assurance Levels (IALs) are a key component of the National Institute of Standards and Technology (NIST) Digital Identity Guidelines, NIST 800-63A. IAL 2 requires identity proofing, which can be completed remotely or in person. The person requesting access must provide evidence that they are the owner of the identity they are claiming. National Institute of Standards and Technology, *Digital Identity Guidelines, Enrollment and Identity Proofing*, Special Publication 800-63A (Gaithersburg, MD: June 2017).

[10]The SolarWinds software hack allowed unauthorized persons to breach infected federal agency information systems. The American Rescue Plan Act of 2021, Pub. L. No. 117-2, 135 Stat, 4. (March 11, 2021), is a $1.9 trillion economic stimulus bill that provides additional relief to address the continued impact of COVID-19 on the economy, public health, state and local governments, individuals, and businesses. The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021) r***equired agencies to enhance cybersecurity and software supply chain integrity.***

Transportation stated that it had a number of competing priorities, such as the SolarWinds software hack and COVID-19 activities. Further, Treasury stated that competing priorities, such as a rollout of a new FOIA/Privacy Act request case system, the COVID-19 pandemic, and vaccine mandates were the reasons for its delay in meeting the deadline. Lastly, OPM reported that the agency had to devote resources to other priorities related to COVID-19. It is important that agencies work to address OMB requirements that are now a year overdue.

As we previously mentioned, SEC has had success with its implementation of OMB guidance. SEC sharing of its experiences in developing and implementing a successful model, including how it overcame any technical and managerial challenges, could be valuable to other agencies. SEC could also share any lessons learned from its experience. The Federal Privacy Council and Chief Information Officers Council, led by OMB, are available mechanisms for such information sharing.[11] Promoting information sharing, through these councils and their subcommittees and communities of practice, could assist agencies in meeting the requirements of the CASES Act.

Until agencies fully implement OMB's requirements to modernize the processes that individuals use to establish identity and request access to or provide consent for disclosure of their records, agencies cannot ensure that they are adequately protecting records from improper disclosure.

Conclusions

Implementing the CASES Act is essential to protecting records while providing prompt assistance to the public. OMB met its CASES Act requirement of developing guidance for federal agencies that included the required elements. However, only one of the 17 selected agencies has reported fully implementing the requirements set forth by OMB; while five agencies have committed to timeframes for implementing the requirements. Until the other agencies implement the requirements or commit to doing so within a reasonable time frame, these agencies cannot ensure that they are using modern processes for individuals to establish their identity and request access to or provide consent for disclosure of their records. Sharing information on SEC's success in meeting OMB's requirements could benefit agencies' efforts.

Recommendations for Executive Action

We are making a total of 12 recommendations, including one to OMB and 11 to reviewed agencies.

The Director of the Office of Management and Budget should take steps to promote, through mechanisms such as the Federal Privacy Council and Chief Information Officers Council, sharing of information and lessons learned to help agencies implement the requirements of the CASES Act; this could include SEC sharing information on overcoming challenges and identifying lessons learned. (Recommendation 1)

[11]Executive Order 13719 directed OMB to establish the Federal Privacy Council as the principal interagency forum to improve the government privacy practices of agencies and entities acting on their behalf. The council's membership consists of senior privacy officials from across the executive branch. It also has multiple committees addressing topics such as agency implementation and privacy workforce, as well as working groups on several topics, including risk management. The White House, *Establishment of the Federal Privacy Council*, Executive Order 13719 (Washington, D.C.: Feb. 9, 2016).

The Secretary of Defense should establish a reasonable time frame for when the Department of Defense will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy program website. (Recommendation 2)

The Secretary of Health and Human Services should establish a reasonable time frame for when the Department of Health and Human Services will be able to digitally accept access and consent forms from individuals who were properly identity proofed and authenticated and post access and consent forms on the department's privacy program website. (Recommendation 3)

The Secretary of Interior should establish a reasonable time frame for when the Department of the Interior will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy program website. (Recommendation 4)

The Attorney General should establish a reasonable time frame for when the Department of Justice will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy program website. (Recommendation 5)

The Secretary of Transportation should establish a reasonable time frame for when the Department of Transportation will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy program website. (Recommendation 6)

The Secretary of Treasury should establish a reasonable time frame for when the Department of the Treasury will be able to digitally accept access and consent forms from individuals who were properly identity proofed and authenticated and post access and consent forms on the department's privacy program website. (Recommendation 7)

The Secretary of Veterans Affairs should establish a reasonable time frame for when the Department of Veterans Affairs will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy program website. (Recommendation 8)

The Chair of the Equal Employment Opportunity Commission should establish a reasonable time frame for accepting remote identity proofing with authentication, digitally accepting access and consent forms from individuals who were properly identity proofed and authenticated, and posting access and consent forms on the agency's privacy program website. (Recommendation 9)

The Archivist of the United States should establish a reasonable time frame for when the National Archives and Records Administration will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the agency's privacy program website. (Recommendation 10)

The Director of the Office of Personnel Management should establish a reasonable time frame for when the agency will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the agency's privacy program website. (Recommendation 11)

The Commissioner of the Social Security Administration should establish a reasonable time frame for when the agency will post access and consent forms on the agency's privacy program website. (Recommendation 12)

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the Office of Management and Budget (OMB) and the 17 agencies included in our review. All the agencies provided responses, as further discussed.

In an email from OMB's Liaison to GAO, OMB did not state whether it agreed or disagreed with our recommendations. However, the office provided technical comments, which we incorporated as appropriate.

In written comments, the following seven agencies concurred with our recommendations and, in most cases, described steps planned or under way to address them:

- Department of Defense concurred with our recommendation and stated that the department is continuing to actively pursue viable solutions, including leveraging existing technologies, for identity proofing and authentication and for the electronic availability and submission of consent and record request forms. DOD's comments are reprinted in enclosure II.

- Department of Interior concurred with our recommendation and stated that the department will establish a reasonable time frame for when they will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy website. The department also stated that they will also work with GSA to use the Login.gov functionality for identify proofing. Interior's comments are reprinted in enclosure III.

- The Department of Justice concurred with our recommendation and stated that it is committed to developing a customer-centric identify verification process that is easy for members of the public to use and facilitates agency efficiency in processing requests. Justice also stated it believed that our report did not fully reflect the requirements in OMB's CASES Act guidance, notably the requirement that agencies implement remote identity proofing and authentication. Justice opined that the guidance required a solution that satisfies identity assurance level-2, as set forth by NIST Special Publication 800-63. It added that GSA's Login.gov does not currently offer these capabilities.

  However, in our report we do not determine whether Login.gov's adheres to NIST identity assurance level-2 standards. Rather, we described the solutions agencies reported using or considered using to address the requirements of the CASES Act. In the one case where an agency reported that it had fulfilled the requirements through the use of Login.gov, they reported receiving approval from OMB officials to do so. OMB

officials responsible for the oversight of agencies' implementation of M-21-04 stated that they developed the guidance to provide agencies some flexibility in how they address its requirements. Justice's comments are reprinted in enclosure IV.

- The Department of Health and Human Services concurred with our recommendation and stated that as the department continues to implement this recommendation, they will also take into consideration successes and lessons learned from other federal agencies. HHS's comments are reprinted in enclosure V.

- The Office of Personnel Management concurred with our recommendation and stated that the office will develop technical requirements and establish an implementation timeline to accept remote identity proofing with authentication, and to digitally accept access and consent forms from those who have been properly identity proofed and authenticated. In addition, the agency will obtain OMB approval for its access and consent forms and post them online by the third quarter of fiscal year 2023. OPM's comments are reprinted in enclosure VI.

- The Social Security Administration concurred with our recommendation and provided technical comments, which we incorporated as appropriate. SSA's comments are reprinted in enclosure VII.

- The Department of Veterans Affairs concurred with our recommendation and stated that the department intends to address the recommendation. VA's comments are reprinted in enclosure VIII.

In addition, the following four agencies either generally agreed or did not state whether they agreed or disagreed with the recommendations:

- In written comments, the Equal Employment Opportunity Commission did not state whether it agreed or disagreed with our recommendations. However, the Commission stated that it is currently working towards implementation using Login.gov to accept online access and consent forms from individuals who have been identity proofed and authenticated. EEOC's comments are reprinted in enclosure IX.

- We received technical comments via email from the USDA GAO audit liaison, DHS's Assistant Director from the GAO Office of the Inspector General Liaison Office, and Treasury's Director of Privacy and Civil Liberties. USDA stated that they generally agreed with our recommendation, while both DHS and Treasury did not state whether they agreed or disagreed with our recommendations. We incorporated their technical comments as appropriate.

Lastly, we received technical comments via email from the SEC Assistant Chief Risk Officer and incorporated them as appropriate. We also received five emails from the Department of Labor's Office of the Assistant Secretary for Policy, State's Sr. Management Analyst, Transportation's Audit Relations Specialist, EPA's Audit Follow-up Coordinator, and the NARA's Audit Liaison. All of the emails stated that these agencies had no comments on the draft report.

- - - - -

We are sending copies of this report to the appropriate congressional committees, the Secretary of Agriculture, Secretary of Defense, Secretary of Health and Human Services, Secretary of Homeland Security, Secretary of Interior, Attorney General of the Department of

Justice, Secretary of Labor, Secretary of State, Secretary of Transportation, Secretary of Treasury, and Secretary of Veterans Affairs; the Administrator of the Environmental Protection Agency, the Chair of the Equal Employment Opportunity Commission, the Administrator of the General Services Administration, the Archivist of the United States, the Director of the Office of Management and Budget, the Director of the Office of Personnel Management, the Chairman of the Securities and Exchange Commission, and the Commissioner of the Social Security Administration, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report were Elena Epps (Assistant Director), Kami Brown (Analyst-in-Charge), Lauri Barnes, Donna Epler, Corwin Hayward, and Ahsan Nasar.

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Enclosure – 9

Enclosure I: Details on the Extent to Which Selected Agencies Addressed the Requirements in the Office of Management and Budget, M-21-04 Guidance

Office of Management and Budget (OMB) issued guidance[12] for agencies to modernize the processes by which individuals may request access to, and consent to the disclosure of, records protected under the Privacy Act of 1974.[13] The guidance outlined agency responsibilities for accepting access and consent forms provided in a digital format from individuals who are properly identity proofed and authenticated. Specifically, agencies were to

- accept remote identity proofing and authentication for the purposes of allowing individuals to request access to their records or to provide written consent authorizing disclosure of their records under the Privacy Act;
- digitally accept the access and consent forms from any individual that was properly identity-proofed and authenticated; and
- post the forms developed using the template provided in OMB's guidance on its website's privacy program webpage.

The following table provides details on the extent to which selected agencies implemented OMB guidance.

Table 1: Status of OMB's *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act* (OMB M-21-04) Implementation as Reported by Selected Federal Agencies

Agency	Status reported by agency
Department of Agriculture (USDA)	USDA is in the process of implementing FOIAXpress[a] configuration changes. Once these changes are implemented, USDA plans to provide remote identity proofing and authentication through General Services Administration's (GSA) Login.gov services. USDA also expects that these changes will allow the department to digitally accept access and consent forms from individuals who were identity-proofed and authenticated. Further, USDA has drafted access and consent forms to post on its privacy program webpage. USDA is currently reviewing and preparing the forms for public comment and the Office of Management and Budget's (OMB) review. USDA expects to meet the requirements in OMB guidance, M-21-04, by the end of the second quarter of 2023.
Department of Defense (DOD)	DOD is planning to leverage existing authentication procedures and technologies to assist many DOD-affiliated individuals, such as DOD civilians and active and retired service members, in submitting Privacy Act requests electronically. The department also stated that it would need to develop a new IT tool to accept remote identity proofing and authentication for members of the public. The department anticipates creating access and consent forms using a modified version of the templates provided in OMB M-21-04, which include appropriate language for the groups most frequently served by the department. However, DOD did not provide time frames for when the OMB M-21-04 requirements would be completed.
Department of Health and Human Services (HHS)	HHS has an existing platform to process Privacy Act requests electronically and is working towards including ID.me capabilities in its vendor software update by November 2022. HHS expects this new capability will allow the department to accept remote identity proofing and authentication from individuals requesting access to their records. In addition, the department is drafting access and consent forms. However, no time frame was given for when HHS will fully meet the OMB requirements.

[12]Office of Management and Budget, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*, OMB Memorandum M-21-04 (Washington, D.C.: Nov. 12, 2020).

[13]5 U.S.C. § 552a.

Agency	Status reported by agency
Department of Homeland Security (DHS)	DHS is transitioning to a new system to have the capability to accept remote identity proofing and authentication. With the new system, the department expects to be able to digitally accept access and consent forms from individuals who have been identity proofed and authenticated. Further, the department has not yet posted access and consent forms to its website, but anticipates fully meeting the requirements in OMB M-21-04 with the implementation of the new system by March 2023.
Department of Interior (DOI)	DOI intends to use GSA's Login.gov solution to accept remote identity proofing and authentication for users requesting access and consent to the disclosure of records. With the solution, the department expects to be able to digitally accept the access and consent forms from any individual who was properly identity proofed and authenticated. Further, once DOI receives final approval from OMB, DOI intends to update its Privacy Act request webpage to include the forms and the instructions about the options for users to submit Privacy Act requests. However, no time frame was given for when DOI will meet the requirements in OMB guidance.
Department of Justice (DOJ)	DOJ is reviewing vendors and evaluating the technical requirements via a gap analysis to determine what current capabilities it has and what is needed to meet the requirements of OMB guidance. During this evaluation, the department is also weighing the equity and accessibility challenges related to remote identity proofing and authentication. In addition, DOJ stated that once the department identifies a technical solution, it plans to post access and consent forms to the department's website. However, DOJ did not provide a time frame for when OMB's requirements will be fully implemented.
Department of Labor	Labor is developing the capability to accept remote identity proofing and authentication but has not made a decision on how the department will digitally accept access and consent forms from individuals that were identity proofed and authenticated. In addition, Labor intends to post on its website access and consent forms once they have been finalized. The department intends to meet the requirements in OMB M-21-04 by December 2024.
Department of State	State expects to have two authentication options available for requesting records: (1) individuals will be able to use the identity proofing and authentication component built into the Public Access Link (PAL) in FOIAXpress once post-configuration changes and/or updates have been addressed, and (2) individuals can use State's access and consent forms that were posted on its website in August 2022. State expects to meet OMB requirements by December 2022.
Department of Transportation	Transportation is reviewing solutions that would address OMB requirements. In addition, Transportation intends to implement a plan to meet the requirements set forth in the memo once OMB provides official implementation guidance to federal agencies. However, the department did not provide a time frame for when OMB requirements would be implemented.
Department of Treasury	Treasury reported that they have completed testing and anticipates the implementation of identity proofing and authentication software will begin by the end of fiscal year 2023 and public access will be available after implementation is completed. In addition, the department intends to use the template language provided in OMB M-21-04 to develop access and consent forms and post the forms on its website. However, Treasury did not provide a time frame for developing and posting these forms.
Department of Veterans Affairs (VA)	VA is working on addressing the requirements to accept remote identity proofing and authentication. In addition, VA does not provide or accept digital access and consent forms from individuals who have been identity proofed and authenticated. Further, VA developed a form for individuals to request their Privacy Act records, but this form cannot be submitted to VA digitally. This form was not developed using the template as required by OMB M-21-04. VA did not provide a time frame for when the department will fully implement OMB requirements.
Environmental Protection Agency (EPA)	EPA is working to replace its current identity proofing process with GSA's Login.gov services for remote identity proofing and authentication and digitally accepting access and consent forms from individuals who were identity proofed and authenticated. The agency expects to satisfy this requirement by April 2023. In addition, the agency provides a digital form on its privacy webpage for individuals requesting access to their records. However, EPA did not use the template provided in OMB M-21-04 when developing these forms. The agency is planning to update its access and consent forms to include all of the template language. EPA expects the forms to be updated on its webpage by April 2023.

Agency	Status reported by agency
Equal Employment Opportunity Commission (EEOC)	EEOC reported that they are examining solutions to address the requirements for remote identity proofing and authentication and to digitally accept access and consent forms from individuals who were identity proofed and authenticated. In addition, EEOC reported that they do not currently handle Privacy Act requests digitally but are in the process of drafting form templates that are consistent with OMB requirements. However, the EEOC did not provide a time frame for when it expects to fully meet OMB requirements.
National Archives and Records Administration (NARA)	NARA is considering adding GSA's Login.gov identity proofing and authentication solution on the front end of its existing electronic military personnel record request system to address Privacy Act requests. NARA is also looking to build a separate application for public requests for civilian records. Further, NARA reported that it has a portal for military record requests, but the agency does not use remote identity-proofing or offer electronic forms for civilian record requests. NARA did not provide a time frame for when it expects to meet OMB requirements.
Office of Personnel Management (OPM)	OPM currently accepts access requests via email and DOJ's National FOIA Portal. Specifically, the agency uses a paper and email-based process where it receives Privacy Act requests through a FOIA intake email box and the National FOIA Portal and manually identity proof requesters. In addition, OPM is in the process of standing up the PAL in FOIAXpress to permit individuals to submit both FOIA and Privacy Act requests. However, OPM did not provide a time frame for when it expects to accept remote identity proofing and authentication and to digitally accept access and consent forms from those who have been properly identity proofed and authenticated. In addition, OPM intends to obtain OMB approval for OPM's access and consent forms and post them to its public-facing website by the third quarter of fiscal year 2023.
Social Security Administration (SSA)	SSA reported that they intend to leverage their existing remote identity proofing and authentication capability to support the implementation of the CASES Act requirements. In addition, SSA intends to implement an in-house web solution using the template from OMB guidance that will require the user to be identity proofed and authenticated before giving consent to and authorizing SSA to disclose limited record types to a third party. SSA anticipates the implementation of this solution in calendar year 2023. In addition, SSA is developing access and consent forms using templates from OMB guidance and intends to post them on its privacy webpage. However, SSA did not provide a time frame for when it expects the forms to be completed and made available to the public.

Source: Agency provided information.| GAO-23-105562

[a]The purpose of FOIAXpress is to enable agencies to more efficiently receive, track, and respond to records requests and appeals made under the Freedom of Information Act and the Privacy Act.

Enclosure II: Comments from the Department of Defense

ASSISTANT TO THE SECRETARY OF DEFENSE FOR
PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

December 5, 2022

Ms. Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Ms. Cruz Cain,

Enclosed is the Department of Defense (DoD) response to the Government Accountability Office (GAO), Draft Report GAO-22-105562, "Information Management: Agencies Need to Streamline Electronic Services," dated November 9, 2022 (GAO Code 105562).

If you have any questions, please contact my action officer, Ms. Rahwa Keleta, Chief, Privacy and Civil Liberties Division, at Rahwa.a.Keleta.civ@mail.mil or (703) 801-4788.

Sincerely,

CHUNG.JOO.Y.1512306507

Digitally signed by CHUNG.JOO.Y.1512306507
Date: 2022.12.05 18:00:55 -05'00'

Joo Y. Chung

Enclosure:
As Stated

GAO DRAFT REPORT DATED NOVEMBER 9, 2022
GAO-22-105562 (GAO CODE 105562)

"Information Management: Agencies Need to Streamline Electronic Services"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should establish a reasonable time frame for when the Department of Defense (DoD) will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the Department's privacy program website.

DoD RESPONSE: The DoD concurs with Recommendation 2, and is continuing to actively pursue viable solutions, including leveraging existing technologies, for identity proofing and authentication and for the electronic availability and submission of consent and record request forms.

Of note, DoD currently has a secure, self-service logon as an enterprise identity credentialing platform that allows individuals affiliated with DoD or the Department of Veterans Affairs (VA) (i.e., beneficiaries of DoD-related benefits or entitlements and other individuals with a continuing affiliation with the DoD), access to online digital resources using credentials. The DoD Self-Service Logon (DS Logon) provides authentication assurance and provides remote identity proofing and multi-factor authentication services. Department stakeholders are currently in the planning and development stage of a site where access and consent forms can be available to individuals with DS Logon serving as the initial point of entry for identity proofing and authentication.

Additionally, the DoD currently has six Components that use FOIAXpress and the Public Access Link (PAL) interface; however, these Components have not purchased the PAL feature that allows for identity proofing and authentication via ID.me or login.gov. The DoD is exploring configuration options and licensing requirements with the vendor of FOIAXpress to determine the feasibility of acquiring identity proofing and authentication for those Components with an existing PAL interface.

Text of Enclosure II: Comments from the Department of Defense

December 5, 2022

Ms. Marisol Cruz Cain

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office 441 G Street, NW

Washington DC 20548

Dear Ms. Cruz Cain,

Enclosed is the Department of Defense (DoD) response to the Government Accountability Office (GAO), Draft Report GAO-22-105562, "Information Management: Agencies Need to Streamline Electronic Services," dated November 9, 2022 (GAO Code 105562).

If you have any questions, please contact my action officer, Ms. Rahwa Keleta, Chief, Privacy and Civil Liberties Division, at Rahwa.a.Keleta.civ@mail.mil or (703) 801-4788.

Sincerely,

Digitally signed by CHUNG.JOO.Y.15123

Y.15123065006507

Date: 2022.12.05

18:00:55 -05'00'

Joo Y. Chung

Enclosure: As Stated

GAO DRAFT REPORT DATED NOVEMBER 9, 2022 GAO-22-105562 (GAO CODE 105562) "Information Management: Agencies Need to Streamline Electronic Services" DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should establish a reasonable time frame for when the Department of Defense (DoD) will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the Department's privacy program website.

DoD RESPONSE: The DoD concurs with Recommendation 2, and is continuing to actively pursue viable solutions, including leveraging existing technologies, for identity proofing and authentication and for the electronic availability and submission of consent and record request forms.

Of note, DoD currently has a secure, self-service logon as an enterprise identity credentialing platform that allows individuals affiliated with DoD or the Department of Veterans Affairs (VA) (i.e., beneficiaries of DoD-related benefits or entitlements and other individuals with a continuing

affiliation with the DoD), access to online digital resources using credentials. The DoD Self-Service Logon (DS Logon) provides authentication assurance and provides remote identity proofing and multi-factor authentication services. Department stakeholders are currently in the planning and development stage of a site where access and consent forms can be available to individuals with DS Logon serving as the initial point of entry for identity proofing and authentication.

Additionally, the DoD currently has six Components that use FOIAXpress and the Public Access Link (PAL) interface; however, these Components have not purchased the PAL feature that allows for identity proofing and authentication via ID.me or login.gov. The DoD is exploring configuration options and licensing requirements with the vendor of FOIAXpress to determine the feasibility of acquiring identity proofing and authentication for those Components with an existing PAL interface.

Enclosure III: Comments from the Department of Interior

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Cain,

Thank you for providing the Department of the Interior (Department, DOI) the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, *Information Management: Agencies Need to Streamline Electronic Services (GAO-22-105562)*. We appreciate the GAO's review of the Office of Management and Budget's (OMB) and Federal agencies' implementation of the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act) to determine the extent that OMB and selected agencies addressed the requirements in the CASES Act.

The Department has made progress in the areas identified in the report by completing our access and consent forms and submitting them to OMB for approval on October 21, 2022. The GAO issued several recommendations to multiple agencies, including one to the Department to address its finding. We look forward to sharing DOI's plan to address the recommendation in response to the final report. Below is a summary of actions planned to implement the recommendation.

Recommendation 4: The Secretary of the Interior should establish a reasonable time frame for when the Department of the Interior will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the [D]epartment's privacy website.

Management Response: Concur. The Department will establish a reasonable time frame for when the Department will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on DOI's privacy website. The Department will also work with the General Services Administration (GSA) to use the login.gov functionality for identify proofing.

If you have any questions or need additional information, please contact Darren B. Ash, Chief Information Officer and Senior Agency Official for Privacy, at darren_ash@ios.doi.gov.

Sincerely,

JOAN MOONEY

Digitally signed by JOAN MOONEY
Date: 2022.12.07 16:11:08 -05'00'

Joan M. Mooney
Principal Deputy Assistant Secretary
for Policy, Management and Budget
Exercising the Authority of the Assistant
Secretary for Policy, Management and Budget

Enclosure

Department of the Interior Comments on the GAO Draft Report Information Management: Agencies Need to Streamline Electronic Services (GAO-22-105562)

Technical Comments

Page 4, paragraph 4:

Current Text: USDA and SSA also provided time frames for when the requirements would be completed, but the five remaining agencies (HHS, DOI, Treasury, EEOC, and OPM) did not.

Proposed edit: Insert the following before the sentence identified above, *Interior reported it has completed access and consent forms and submitted the forms to OMB on October 21,2022, for final approval and are awaiting a response; however, they did not provide the date the requirements would be complete.*

Text of Enclosure III: Comments from the Department of Interior

Marisol Cruz Cain

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Dear Director Cain,

Thank you for providing the Department of the Interior (Department, DOI) the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, Information Management: Agencies Need to Streamline Electronic Services (GAO-22-105562). We appreciate the GAO's review of the Office of Management and Budget's (OMB) and Federal agencies' implementation of the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act) to determine the extent that OMB and selected agencies addressed the requirements in the CASES Act.

The Department has made progress in the areas identified in the report by completing our access and consent forms and submitting them to OMB for approval on October 21, 2022. The GAO issued several recommendations to multiple agencies, including one to the Department to address its finding. We look forward to sharing DOI's plan to address the recommendation in response to the final report.

Below is a summary of actions planned to implement the recommendation.

Recommendation 4: The Secretary of the Interior should establish a reasonable time frame for when the Department of the Interior will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the [D]epartment's privacy website.

Management Response: Concur. The Department will establish a reasonable time frame for when the Department will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on DOI's privacy website. The Department will also work with the General Services Administration (GSA) to use the login.gov functionality for identify proofing.

If you have any questions or need additional information, please contact Darren B. Ash, Chief Information Officer and Senior Agency Official for Privacy, at darren_ash@ios.doi.gov.

Sincerely,

Joan M. Mooney

Enclosure

Principal Deputy Assistant Secretary for Policy, Management and Budget Exercising the Authority of the Assistant Secretary for Policy, Management and Budget

Department of the Interior Comments on the GAO Draft Report Information Management: Agencies Need to Streamline Electronic Services (GAO-22-105562)

Technical Comments

Page 4, paragraph 4:

Current Text: USDA and SSA also provided time frames for when the requirements would be completed, but the five remaining agencies (HHS, DOI, Treasury, EEOC, and OPM) did not.

Proposed edit: Insert the following before the sentence identified above, Interior reported it has completed access and consent forms and submitted the forms to OMB on October 21,2022, for final approval and are awaiting a response; however, they did not provide the date the requirements would be complete.

Enclosure IV: Comments from the Department of Justice

U.S. Department of Justice

Justice Management Division

Washington, D.C. 20530

Marisol Cruz Cain
Director
Information Technology and Cybersecurity Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Cruz Cain:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled "*Information Management: Agencies Need to Streamline Electronic Services.*" (GAO-23-105562) The Department of Justice (the Department or DOJ) has reviewed the report and has the following response.

DOJ concurs with GAO's recommendation that the Attorney General should establish a reasonable time frame for when the Department of Justice will be able to fulfill the requirements of the CASES Act and the Office of Management and Budget's (OMB) implementation guidance, M-21-04. However, DOJ believes that GAO's report does not fully reflect the requirements of M-21-04, notably the requirement that agencies implement "remote identity proofing and authentication," which means a solution that satisfies Identity Assurance Level-2 (IAL2), as set forth by National Institute for Standards and Technology Special Publication 800-63, *Digital Identity Guidelines.* The General Service Administration's (GSA) Login.gov authentication and identity verification solution does not currently offer IAL2 capabilities. In order to be as accurate as possible about the most challenging aspect of the CASES Act, as implemented by M-21-04, GAO should explicitly recognize (e.g., under "Technical Delays and Challenges on p. 5 of the Report) the fact that Login.gov does not currently meet the requirement to provide IAL2 capabilities.

Remote IAL2 proofing requires the user to submit biometric information, such as a photo or video of themselves, alongside primary documents, such as a driver's license, and then utilizes facial recognition software to compare and verify the veracity of the user's documentation. When this type of technology was deployed by other agencies, it raised privacy, security, and equity concerns from the public and members of Congress. Navigating these concerns, along with no additional funds authorized by the Act and the lack of a government solution that meets IAL2 standards, has become a key part of the Department's efforts to implement M-21-04 and has directly contributed to the delays in finding a solution to satisfy CASES Act requirements.

As part of its CASES Act implementation, DOJ is committed to developing a customer-centric identify verification process that is easy for members of the public to use and facilitates agency efficiency in processing requests. DOJ's decentralized processing of requests across thirty-one agency components each with their own case management system makes this particularly challenging, but we are committed to finding a solution that satisfies the requirements of the statute and the OMB guidance while alleviating concerns about privacy, security, and equity.

If I may be of further assistance to you, please do not hesitate to contact me. Your staff may also contact Louise Duhamel, DOJ Audit Liaison, Audit Liaison Group on 202-514-4006.

Sincerely,

JOLENE LAURIA

Digitally signed by JOLENE LAURIA
Date: 2022.12.08 22:19:27 -05'00'

Jolene Lauria
Acting Assistant Attorney General
for Administration
Justice Management Division
U.S. Department of Justice

cc: The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Room 7071
Washington, DC 20548

Charles Johnson, Jr.
Managing Director
Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Rm. 6153
Washington, DC 20548

Elena Epps
Assistant Director
Information Technology and Cybersecurity Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Louise Duhamel
Assistant Director
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division
145 N Street, NE Suite 8W.300
Washington, DC 20002

Text of Enclosure IV: Comments from the Department of Justice

Marisol Cruz Cain Director

Information Technology and Cybersecurity Team

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Dear Ms. Cruz Cain:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled “Information Management: Agencies Need to Streamline Electronic Services.” (GAO-23-105562) The Department of Justice (the Department or DOJ) has reviewed the report and has the following response.

DOJ concurs with GAO’s recommendation that the Attorney General should establish a reasonable time frame for when the Department of Justice will be able to fulfill the requirements of the CASES Act and the Office of Management and Budget’s (OMB) implementation guidance, M-21-04. However, DOJ believes that GAO’s report does not fully reflect the requirements of M-21-04, notably the requirement that agencies implement “remote identity proofing and authentication,” which means a solution that satisfies Identity Assurance Level-2 (IAL2), as set forth by National Institute for Standards and Technology Special Publication 800-63, Digital Identity Guidelines. The General Service Administration's (GSA) Login.gov authentication and identity verification solution does not currently offer IAL2 capabilities. In order to be as accurate as possible about the most challenging aspect of the CASES Act, as implemented by M-21-04, GAO should explicitly recognize (e.g., under “Technical Delays and Challenges on p. 5 of the Report) the fact that Login.gov does not currently meet the requirement to provide IAL2 capabilities.

Remote IAL2 proofing requires the user to submit biometric information, such as a photo or video of themselves, alongside primary documents, such as a driver’s license, and then utilizes facial recognition software to compare and verify the veracity of the user’s documentation.

When this type of technology was deployed by other agencies, it raised privacy, security, and equity concerns from the public and members of Congress. Navigating these concerns, along with no additional funds authorized by the Act and the lack of a government solution that meets IAL2 standards, has become a key part of the Department’s efforts to implement M-21-04 and has directly contributed to the delays in finding a solution to satisfy CASES Act requirements.

As part of its CASES Act implementation, DOJ is committed to developing a customer- centric identify verification process that is easy for members of the public to use and facilitates agency efficiency in processing requests. DOJ’s decentralized processing of requests across thirty-one agency components each with their own case management system makes this particularly challenging, but we are committed to finding a solution that satisfies the requirements of the statute and the OMB guidance while alleviating concerns about privacy, security, and equity.

If I may be of further assistance to you, please do not hesitate to contact me. Your staff may also contact Louise Duhamel, DOJ Audit Liaison, Audit Liaison Group on 202-514-4006.

Sincerely,

Jolene Lauria

Acting Assistant Attorney General for Administration

Justice Management Division

U.S. Department of Justice

cc: The Honorable Gene L. Dodaro Comptroller General of the United States

U.S. Government Accountability Office 441 G Street, NW

Room 7071

Washington, DC 20548

Charles Johnson, Jr.

Managing Director

Homeland Security and Justice

U.S. Government Accountability Office 441 G Street, NW

Rm. 6153

Washington, DC 20548

Elena Epps Assistant Director

Information Technology and Cybersecurity Team

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Louise Duhamel Assistant Director Audit Liaison Group

Internal Review and Evaluation Office Justice Management Division

145 N Street, NE Suite 8W.300 Washington, DC 20002

Enclosure V: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

December 9, 2022

Marisol Cruz Cain
Director, GAO Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Cain:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"Information Management: Agencies Need to Streamline Electronic Services" (GAO-22-105562).**

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

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT - "INFORMATION MANAGEMENT: AGENCIES NEED TO STREAMLINE ELECTRONIC SERVICES" (GAO-23-105562)

Recommendation 3

The Secretary of Health and Human Services should establish a reasonable time frame for when the Department of Health and Human Services will be able to digitally accept access and consent forms from individuals who were properly identify proofed and authenticated and post access and consent forms on the department's privacy program website.

HHS Response

HHS concurs with this recommendation. As HHS continues to implement this recommendation, we will also take into consideration successes and lessons learned from other federal agencies. HHS will provide another update in its Statement of Actions as required by OMB Circular A-50 and 31 U.S.C. 720, and in subsequent updates.

Text of Enclosure V: Comments from the Department of Health and Human Services

December 9, 2022

Marisol Cruz Cain

Director, GAO Information Technology and Cybersecurity

U.S. Government Accountability Office 441 G Street NW

Washington, DC 20548

Dear Ms. Cain:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "Information Management: Agencies Need to Streamline Electronic Services" (GAO-22-105562).

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

Sincerely,

Melanie Anne Egorin, PhD Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT - "INFORMATION MANAGEMENT: AGENCIES NEED TO STREAMLINE ELECTRONIC SERVICES" (GAO-23-105562)

Recommendation 3

The Secretary of Health and Human Services should establish a reasonable time frame for when the Department of Health and Human Services will be able to digitally accept access and consent forms from individuals who were properly identify proofed and authenticated and post access and consent forms on the department's privacy program website.

HHS Response

HHS concurs with this recommendation. As HHS continues to implement this recommendation, we will also take into consideration successes and lessons learned from other federal agencies. HHS will provide another update in its Statement of Actions as required by OMB Circular A-50 and 31 U.S.C. 720, and in subsequent updates.

Enclosure VI: Comments from the Office of Personnel Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of Privacy
and Information
Management

Ms. Marisol Cruz Cain
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Ms. Cain:

Thank you for providing the U.S. Office of Personnel Management (OPM) the opportunity to respond to the U.S. Government Accountability Office's (GAO) draft report, *"Information Management: Agencies Need to Streamline Electronic Services," Report Number GAO-22-105562*.

We have provided a detailed response to the GAO recommendation below.

Recommendation 11: The Director of the Office of Personnel Management should establish a reasonable time frame for when the agency will be able to accept remote identity proofing with authentication, digitally accept access and consent forms who were properly identity proofed and authenticated, and post access and consent forms on the agency's privacy program website.

OPM's Response: Concur. The Office of Executive Secretariat and Privacy and Information Management (OESPIM) and the Office of the Chief Information Officer will work together to develop technical requirements and establish an implementation timeline to accept remote identity proofing with authentication, and to digitally accept access and consent forms from those who have been properly identity proofed and authenticated. OESPIM will, separately, obtain Office of Management and Budget approval for OPM's access and consent forms and post them at www.opm.gov/privacy by the third quarter of FY 23.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact me at (202) 936-2474 or email me at Kellie.Riley@opm.gov.

Sincerely,

KELLIE RILEY Digitally signed by KELLIE RILEY Date: 2022.12.07 10:01:22 -05'00'

Kellie Cosgrove Riley
Executive Director
Office of Executive Secretariat
and Privacy and Information Management

Text of Enclosure VI: Comments from the Office of Personnel Management

Ms. Marisol Cruz Cain

Director, Information Technology and Cybersecurity United States Government Accountability Office 441 G St., NW

Washington, DC 20548

Dear Ms. Cain:

Thank you for providing the U.S. Office of Personnel Management (OPM) the opportunity to respond to the U.S. Government Accountability Office's (GAO) draft report, "Information Management: Agencies Need to Streamline Electronic Services," Report Number GAO-22-105562.

We have provided a detailed response to the GAO recommendation below.

Recommendation 11: The Director of the Office of Personnel Management should establish a reasonable time frame for when the agency will be able to accept remote identity proofing with authentication, digitally accept access and consent forms who were properly identity proofed and authenticated, and post access and consent forms on the agency's privacy program website.

OPM's Response: Concur. The Office of Executive Secretariat and Privacy and Information Management (OESPIM) and the Office of the Chief Information Officer will work together to develop technical requirements and establish an implementation timeline to accept remote identity proofing with authentication, and to digitally accept access and consent forms from those who have been properly identity proofed and authenticated. OESPIM will, separately, obtain Office of Management and Budget approval for OPM's access and consent forms and post them at www.opm.gov/privacy by the third quarter of FY 23.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact me at (202) 936-2474 or email me at Kellie.Riley@opm.gov.

Sincerely,

Kellie Cosgrove Riley Executive Director

Office of Executive Secretariat and Privacy and Information Management

Enclosure VII: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

December 7, 2022

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Cain,

Thank you for the opportunity to review the draft report, "Information Management: Agencies Need to Streamline Electronic Services" (105562). We agree with the recommendation.

Please contact me at (410) 965-2611 if I can be of further assistance. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Scott Frey
Chief of Staff

Text of Enclosure VII: Comments from the Social Security Administration

December 7, 2022

Marisol Cruz Cain

Director, Information Technology and Cybersecurity United States Government Accountability Office 441 G Street, NW

Washington, DC 20548

Dear Director Cain,

Thank you for the opportunity to review the draft report, "Information Management: Agencies Need to Streamline Electronic Services" (105562). We agree with the recommendation.

Please contact me at (410) 965-2611 if I can be of further assistance. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Scott Frey Chief of Staff

Enclosure VIII: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

December 2, 2022

Ms. Marisol Cruz Cain
Director
Information Security and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Cain:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***Information Management: Agencies Need to Streamline Electronic Services*** (GAO-22-105562).

The enclosure contains information regarding how VA plans to address the draft report recommendation. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Tanya J. Bradsher
Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report,
Information Management: Agencies Need to Streamline Electronic Services
(GAO-22-105562)

Recommendation 8: The Secretary of Veterans Affairs should establish a reasonable time frame for when the Department of Veterans Affairs will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy program website.

VA Comment: Concur. VA concurs with GAO's recommendation to the Department. VA will provide the actions to be taken to address the GAO draft report recommendation in the 180-day update to the final report.

Department of Veterans Affairs
December 2022

Text of Enclosure VIII: Comments from the Department of Veterans Affairs

December 2, 2022

Ms. Marisol Cruz Cain Director

Information Security and Cybersecurity

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Dear Ms. Cain:

The Department of Veterans Affairs {VA) has reviewed the Government Accountability Office (GAO) draft report: Information Management: Agencies Need to Streamline Electronic Services (GAO-22-105562).

The enclosure contains information regarding how VA plans to address the draft report recommendation. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Tanya J. Bradsher

Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs (VA) Response to Government Accountability Office (GAO) Draft Report, Information Management: Agencies Need to Streamline Electronic Services (GAO-22-105562)

Recommendation 8: The Secretary of Veterans Affairs should establish a reasonable time frame for when the Department of Veterans Affairs will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the department's privacy program website.

VA Comment: Concur. VA concurs with GAO's recommendation to the Department. VA will provide the actions to be taken to address the GAO draft report recommendation in the 180-day update to the final report.

Department of Veterans Affairs December 2022

Enclosure IX: Comments from the Equal Employment Opportunity Commission

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Washington, D.C. 20507

December 9, 2022

Ms. Marisol Cruz Cain
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Cain:

Thank you for the opportunity to review the Government Accountability Office's (GAO) draft report entitled *Information Management: Agencies Need to Streamline Electronic Services* (draft report). In the draft report, GAO examined the implementation of the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act) to determine the extent to which certain agencies, including the U.S. Equal Employment Opportunity Commission (EEOC), have addressed the requirements of the CASES Act.

As noted in the draft report, the CASES Act directed agencies to adopt forthcoming guidance from the Office of Management and Budget (OMB) on procedures for individuals to establish their identity and request access to or provide written consent for disclosure of their records under the Privacy Act. Specifically, the CASES Act instructed agencies to adopt OMB's guidance on accepting electronic identity proofing and authentication; creating a template for electronic consent and access forms; and accepting electronic consent and access forms from individuals that have been properly identity proofed and authenticated.

In November 2021, the General Services Administration (GSA) began examining whether a potential government-wide solution could be developed that would assist agencies with meeting the technical requirements of the CASES Act. Due to the small number of Privacy Act requests the EEOC receives each year, the EEOC expressed interest in working with GSA on a government-wide shared solution. In anticipation of the shared solution, the EEOC began drafting form templates that were consistent with OMB's guidance on the CASES Act.

During this audit, GAO informed the EEOC that GSA decided against moving forward with a government-wide shared solution. Since receiving notification of GSA's decision, the EEOC has examined other solutions to address the requirements of the CASES Act. As such, the EEOC is currently implementing login.gov authentication for our public-facing Freedom of Information Act (FOIA) portal. Once the login.gov authentication is fully implemented on the agency's FOIA public portal, the EEOC intends to work with the FOIA portal vendor to similarly connect Privacy Act requesters through login.gov to accept online access and consent forms from individuals who have been identity proofed and authenticated.

We appreciate the opportunity to review the draft report and to submit these comments for your consideration. We hope that you find this information helpful.

Sincerely,

Charlotte A. Burrows
Chair

Text of Enclosure IX: Comments from the Equal Employment Opportunity Commission

December 9, 2022

Ms. Marisol Cruz Cain Director

Information Technology and Cybersecurity

U.S. Government Accountability Office 441 G Street, N.W.

Washington, D.C. 20548

Dear Ms. Cain:

Thank you for the opportunity to review the Government Accountability Office's (GAO) draft report entitled I11formatio11 Management: Agencies Need to Streamline Electronic Sen1ices (draft report). In the draft report, GAO examined the implementation of the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act) to determine the extent to which certain agencies, including the U.S. Equal Employment Opportunity Commission (EEOC), have addressed the requirements of the CASES Act.

As noted in the draft report, the CASES Act directed agencies to adopt forthcoming guidance from the Office of Management and Budget (0MB) on procedures for individuals to establish their identity and request access to or provide written consent for disclosure of their records under the Privacy Act. Specifically, the CASES Act instructed agencies to adopt OMB's guidance on accepting electronic identity proofing and authentication; creating a template for electronic consent and access forms; and accepting electronic consent and access forms from individuals that have been properly identity proofed and authenticated.

In November 2021, the General Services Administration (GSA) began examining whether a potential government-wide solution could be developed that would assist agencies with meeting the technical requirements of the CASES Act. Due to the small number of Privacy

Act requests the EEOC receives each year, the EEOC expressed interest in working with GSA on a government-wide shared solution. In anticipation of the shared solution, the EEOC began drafting form templates that were consistent with OMB's guidance on the CASES Act.

During this audit, GAO informed the EEOC that GSA decided against moving forward with a government-wide shared solution. Since receiving notification of GSA's decision, the EEOC has examined other solutions to address the requirements of the CASES Act. As such, the EEOC is currently implementing login.gov authentication for our public-facing Freedom of Information Act (FOIA) portal. Once the login.gov authentication is fully implemented on the agency's FOIA public portal, the EEOC intends to work with the FOIA portal vendor to similarly connect Privacy Act requesters through login.gov to accept online access and consent forms from individuals who have been identity proofed and authenticated.

We appreciate the opportunity to review the draft report and to submit these comments for your consideration. We hope that you find this information helpful.

Sincerely,

Charlotte A. Burrows Chair

(105562)