



Report to the Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

July 2017

SOCIAL SECURITY NUMBERS

OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display

GAO Highlights

Highlights of [GAO-17-553](#), a report to the Chairman, Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

The federal government uses SSNs as unique identifiers for many purposes, including employment, taxation, law enforcement, and benefits. However, SSNs are also key pieces of identifying information that potentially may be used to perpetrate identity theft.

GAO was asked to review federal government efforts to reduce the collection and use of SSNs. This report examines (1) what governmentwide initiatives have been undertaken to assist agencies in eliminating their unnecessary use of SSNs and (2) the extent to which agencies have developed and executed plans to eliminate the unnecessary use and display of SSNs and have identified challenges associated with those efforts. To do so, GAO analyzed reports and guidance on protecting SSNs. GAO also analyzed SSN reduction plans and other documents, administered a questionnaire, and interviewed officials from the 24 CFO Act agencies.

What GAO Recommends

GAO recommends that OMB require complete plans for ongoing reductions in the collection, use, and display of SSNs, require inventories of systems containing SSNs, provide criteria for determining “unnecessary” use and display, ensure agencies update their progress in annual reports, and monitor agency progress based on clearly defined performance measures.

OMB did not comment on GAO’s recommendations. We received written comments from SSA and technical comments from eight other agencies, which were incorporated into the final report as appropriate. The other 15 agencies did not provide comments. View [GAO-17-553](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

July 2017

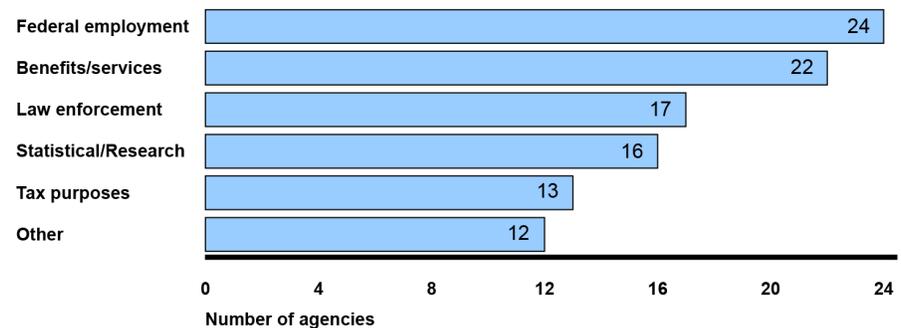
SOCIAL SECURITY NUMBERS

OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display

What GAO Found

Governmentwide initiatives aimed at eliminating the unnecessary collection, use, and display of Social Security Numbers (SSN) have been underway in response to recommendations that the presidentially appointed Identity Theft Task Force made in 2007 to the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), and the Social Security Administration (SSA). However, these initiatives have had limited success. In 2008, OPM proposed a regulation requiring the use of an alternate federal employee identifier but withdrew it in 2010 because no such identifier was available. OMB required agencies to develop SSN reduction plans and requires annual reporting on agency SSN reduction efforts. SSA developed an online clearinghouse of best practices for reducing SSN use; however, it is no longer available online. Based on responses to GAO’s questionnaire, the 24 agencies covered by the Chief Financial Officers (CFO) Act use SSNs for various purposes (see figure).

Agency Use of Social Security Numbers



Source: Agency-reported data. | GAO-17-553

All 24 CFO Act agencies developed SSN reduction plans and reported taking actions to curtail the use and display of SSNs. For example, the Department of Defense replaced SSNs, which previously appeared on its identification cards, with new identification numbers. Nevertheless, the agencies cited impediments to further reductions, including (1) statutes and regulations mandating SSN collection, (2) use of SSNs in necessary interactions with other federal entities, and (3) technological constraints of agency systems and processes.

Further, poor planning by agencies and ineffective monitoring by OMB have also limited efforts to reduce SSN use. Lacking direction from OMB, many agencies’ SSN reduction plans did not include key elements, such as time frames and performance indicators, calling into question their utility. In addition, OMB has not required agencies to maintain up-to-date inventories of their SSN holdings or provided criteria for determining “unnecessary use and display,” limiting agencies’ ability to gauge progress. OMB also has not ensured that agencies update their progress in annual reports or established performance metrics to monitor agency efforts. Until OMB requires agencies to adopt better practices for managing their SSN reduction processes, overall governmentwide reduction efforts will likely remain limited and difficult to measure.

Contents

Letter		1
	Background	3
	OMB, OPM, and SSA Have Had Limited Success in Assisting With Governmentwide Reduction in the Collection, Use, and Display of SSNs	11
	Agencies Reported Reducing Their Use and Display of SSNs and Cited Ongoing Challenges; Moreover, Poor Planning and Ineffective Monitoring Have Limited Their Efforts	16
	Conclusions	32
	Recommendations for Executive Actions	33
	Agency Comments and Our Evaluation	33
Appendix I	Objectives, Scope, and Methodology	36
Appendix II	Questionnaire Content	39
Appendix III	Comments from the Social Security Administration	42
Appendix IV	GAO Contact and Staff Acknowledgments	44
Tables		
	Table 1: Examples of Federal Statutes that Authorize or Mandate the Collection or Use of Social Security Numbers (SSN)	4
	Table 2: Key Performance Plan Elements Addressed in Original Agency Social Security Number (SSN) Reduction Plans	25
Figure		
	Figure 1: Agency Reported Use of Social Security Numbers	5

Abbreviations

CMS	Centers for Medicare & Medicaid Services
DOD	Department of Defense
Education	Department of Education
FISMA	Federal Information Security Modernization Act of 2014
HHS	Department of Health and Human Services
ICN	integration control number
IRS	Internal Revenue Service
IT	information technology
OMB	Office of Management and Budget
OPM	Office of Personnel and Management
PII	personally identifiable information
SSA	Social Security Administration
SSN	Social Security Number
USDA	U.S. Department of Agriculture
VA	Department of Veterans Affairs
VHA	Veterans Health Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



July 25, 2017

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Dear Mr. Chairman:

The federal government uses Social Security numbers (SSN) as unique identifiers for many purposes, including employment, taxation, benefits, and law enforcement. In addition, SSNs have been used in the private sector as a means to authenticate the identity of individuals seeking financial or other transactions. However, SSNs are also key pieces of personally identifiable information (PII) that potentially may be used to perpetrate identity theft. Identity thieves find SSNs especially valuable because they are the identifying link that can connect an individual's PII across many agencies, information systems, and databases.

Significant breaches of PII have occurred within the federal government in recent years that have resulted in the unauthorized disclosure of millions of SSNs. For example, the Office of Personnel Management (OPM) experienced a massive breach in June 2015 that involved the background investigation records of current and former federal employees, including the SSNs of 21.5 million federal employees and contractors.

You asked us to review the status of the federal government's efforts to reduce its reliance on SSNs. Our objectives were to determine: (1) what governmentwide initiatives have been undertaken to assist agencies in eliminating their unnecessary use of SSNs and (2) the extent to which agencies have developed and executed plans to eliminate the unnecessary use and display of SSNs and have identified challenges associated with those efforts.

To address our first objective, we analyzed documents, including reports by the presidentially appointed Identity Theft Task Force on strengthening efforts to protect against identity theft, Office of Management and Budget (OMB) guidance to agencies on protecting SSNs and other PII, and OPM guidance on protecting federal employee SSNs. We also interviewed officials from OMB, OPM, and the Social Security Administration (SSA),

which led or participated in efforts to eliminate the unnecessary use of SSNs on a governmentwide basis.

For our second objective, we analyzed documentation obtained from the 24 agencies covered by the Chief Financial Officers (CFO) Act,¹ including their SSN reduction plans and annual updates, and compared them with key elements of effective performance plans, as defined in federal guidance and the Government Performance and Results Act Modernization Act of 2010.² We also administered a questionnaire to these agencies and interviewed relevant officials to gain additional insight on their SSN reduction efforts and the associated challenges.

Further, we obtained and analyzed additional information about SSN reduction policies and activities from a selection of the 24 agencies included in this review. To select these agencies, we first identified the major agencies in the military, international, or security/national security area as well as the agencies that deliver benefits to the general public. Within these groups, we then selected the two agencies that had reported the largest number of systems and programs that use SSNs. We also selected IRS because it collects a large number of taxpayer SSNs and OPM because it collects SSNs from all federal workers. This resulted in the selection of 6 of the 24 agencies or components thereof: the Centers for Medicare & Medicaid Services (CMS), a component of the Department of Health and Human Services (HHS); the United States Department of Agriculture (USDA); Army, a component of the Department of Defense

¹The CFO Act, Pub. L. No. 101-576 (Nov. 15, 1990), established chief financial officers to oversee financial management activities at 23 major executive departments and agencies. The list now includes 24 entities, which are often referred to collectively as CFO Act agencies, and is codified, as amended, in section 901 of Title 31, U.S.C. The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

²See Pub L. No. 103-62, 107 Stat. 285 (Aug. 3, 1993) (GPRA), as amended by Pub. L. No. 111-352, 124 Stat. 3866 (Jan. 4, 2011) (GPRAMA). GPRAMA emphasizes the need for performance measures to be tied to program goals and for agencies to ensure that their activities support their organizational missions and move them closer to accomplishing their strategic goals. It requires, among other things, that federal agencies develop strategic plans that include agency wide goals and strategies for achieving those goals. We have reported that these requirements also can serve as leading practices for planning at lower levels within federal agencies, such as individual programs or initiatives.

(DOD); the Department of Veterans Affairs (VA); the Internal Revenue Service (IRS), a component of the Department of the Treasury; and OPM. See appendix I for additional details on our objectives, scope, and methodology.

We conducted this performance audit from April 2016 to July 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In 1936, following the enactment of the Social Security Act of 1935³, the newly-created Social Security Board (which later became SSA) created the 9-digit SSN to uniquely identify and determine Social Security benefit entitlement levels for U.S. workers. SSA uses a process known as “enumeration” to create and assign unique SSNs for every eligible person as part of their work and retirement benefit record. As of September 2016, SSA had issued approximately 496 million unique SSNs to eligible individuals.

Originally, the SSN was not intended to serve as a personal identifier outside of SSA’s programs but, due to its universality and uniqueness, government agencies and private sector entities now use the SSN as a convenient means of identifying people. The SSN uniquely links an identity across a very broad array of public and private sector information systems.

The expansion of government use of the SSN began with Executive Order 9397, issued by President Franklin D. Roosevelt in 1943. This required all federal agencies to use the SSN exclusively for identification systems of individuals.⁴ Since Executive Order 9397 was issued, additional federal statutes have authorized or mandated the collection or use of SSNs for a wide variety of specific government activities. Table 1 lists examples of such statutes.

³Pub. L. No. 74–271 (Aug. 14, 1935).

⁴In 2008, Executive Order 13478 amended Executive Order 9397 to rescind the requirement for federal agencies to use SSNs exclusively.

Table 1: Examples of Federal Statutes that Authorize or Mandate the Collection or Use of Social Security Numbers (SSN)

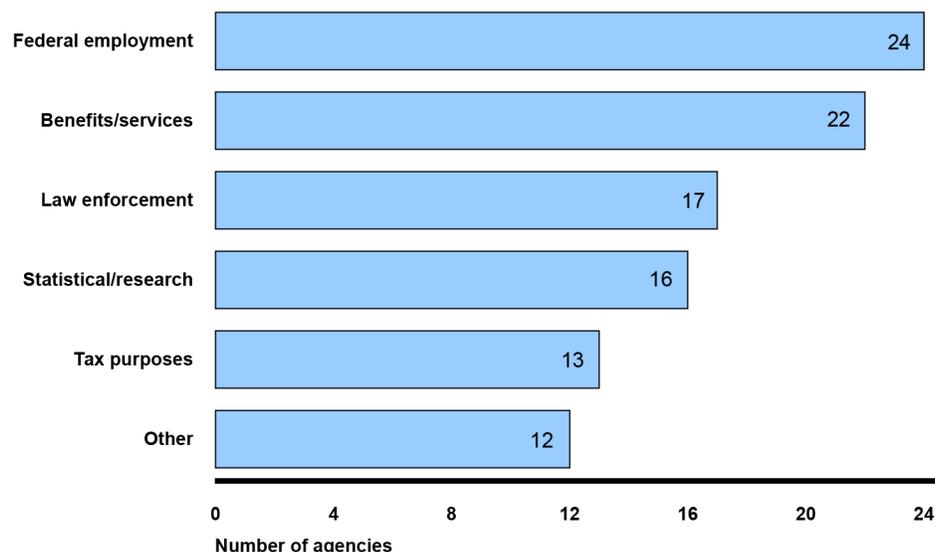
Federal Statute	Government Entity and Authorized or Required Use
Tax Reform Act of 1976, 42 U.S.C. 405(c)(2)(C)(i)	Authorizes states to collect and use SSNs in administering any tax, general public assistance, driver’s license, or motor vehicle registration law.
Food Stamp Act of 1977, 7 U.S.C. 2025(e)(1)	Mandates the Secretary of Agriculture and state agencies to require SSNs for participation in the food stamps program.
Deficit Reduction Act of 1984, 42 U.S.C. 1320b-7(1)	Requires that, as a condition of eligibility for Medicaid benefits, applicants for and recipients of these benefits furnish their SSNs to the state administering program.
Housing and Community Development Act of 1987, 42 U.S.C. 3543(a)	Authorizes the Secretary of the Department of Housing and Urban Development to require program applicants and participants to submit their SSNs as a condition of eligibility for housing assistance.
Family Support Act of 1988, 42 U.S.C. 405(c)(2)(C)(ii)	Requires states to obtain parent’s SSNs before issuing a birth certificate unless there is good cause for not requiring the number.
Technical and Miscellaneous Revenue Act of 1988, 42 U.S.C. 405(c)(2)(D)(i)	Authorizes states and political subdivisions to require that blood donors provide their SSNs.
Food, Agriculture, Conservation, and Trade Act of 1990, 42 U.S.C. 405(c)(2)(C)	Authorizes the Secretary of Agriculture to require the SSNs of officers or owners of retail and wholesale food concerns that accept and redeem food stamps.
Social Security Independence and Program Improvements Act of 1994, 42 U.S.C. 405(c)(2)(E)	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors.
Personal Responsibility and Work Opportunity Reconciliation Act of 1996, 42 U.S.C. 666(a)(13)	Requires states to include SSNs on applications for driver’s licenses and other licenses; on records relating to divorce decrees, child support orders, or paternity determinations; and on death records.
Debt Collection Improvement Act of 1996, 31 U.S.C. 7701(c)	Requires those doing business with a federal agency (i.e., lenders in a federal guaranteed loan program; applicants for federal licenses, permits, right-of-ways, grants, or benefit payments; contractors of an agency and others) to furnish SSNs to the agency.
Higher Education Act Amendments of 1998, 20 U.S.C. 1090(a)(12)	Authorizes the Secretary of Education to include the SSNs of parents of dependent students on certain financial assistance forms.
Internal Revenue Code (various amendments), 26 U.S.C. 6109(d)	Authorizes the Commissioner of the Internal Revenue Service to require that taxpayers include their SSNs on tax returns.

Source: GAO review of applicable federal laws | GAO-17-553

These and other laws and regulations have dramatically increased the extent to which the government collects and uses SSNs as a unique record identifier to determine an individual’s eligibility for government services and benefits. For example, CMS (a component of HHS) collects SSNs from approximately 57.7 million U.S. citizens or residents and displays them on Medicare enrollment cards. Other agencies collect SSNs for purposes such as federal employment (hiring, pay, and benefits), loans and other personal benefits, criminal law enforcement, statistical and other research purposes, and tax purposes. Figure 1 shows the extent to which the 24 federal agencies covered by the CFO

Act reported collecting and using SSNs for different purposes, based on responses to our questionnaire.

Figure 1: Agency Reported Use of Social Security Numbers



Source: Agency-reported data. | GAO-17-553

Key Laws Provide a Framework for Government Protection of SSNs and other PII

Requirements for protecting the privacy and security of SSNs in the federal government are derived from the provisions of laws that govern the collection and use of PII. Generally, these laws require agencies to notify the public of any such collection, collect only the information that is necessary to accomplish an agency's purpose, and perform privacy impact assessments for systems that collect, use, and store PII. Among others, three key laws establish governmentwide privacy and security protections: the Privacy Act of 1974,⁵ the E-Government Act of 2002,⁶ and the Federal Information Security Modernization Act of 2014 (FISMA).⁷

⁵Pub. L. No. 93-579 (Dec. 31, 1974); 5 U.S.C. § 552a.

⁶Pub. L. No. 107-347 (Dec. 17, 2002); 44 U.S.C. § 3501 note.

⁷The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014; 44 U.S.C. § 3551) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

The Privacy Act of 1974 requires that agencies maintain only those records containing PII that are “relevant and necessary” to accomplish agency purposes. The act describes a record as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or other personal identifier. The act defines a “system of records” as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. Section 7 of the act requires that any federal, state, or local government agency, when requesting an SSN from an individual, provide that individual with three key pieces of information.⁸ Government entities must (1) tell individuals whether disclosing their SSNs is mandatory or voluntary; (2) cite the statutory or other authority under which the request is being made; and (3) state what uses the government will make of the individual’s SSN. OMB has issued detailed guidance on implementing the act.⁹

The E-Government Act of 2002 requires agencies to conduct privacy impact assessments before developing or procuring information technology that collects, maintains, or disseminates information that is in identifiable form (such as SSNs). According to OMB guidance, a privacy impact assessment is an analysis of how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.¹⁰

FISMA sets requirements for safeguarding the confidentiality, integrity, and availability of information collected and used by federal agencies. It requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support operations and assets

⁸Section 7 of the Privacy Act is not codified with the rest of the act, but rather is found in the note section to 5 U.S.C. 552a.

⁹Office of Management and Budget, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Circular No. A-108 (Washington, DC: Dec. 23, 2016) and OMB, *Privacy Act Implementation Guidelines and Responsibilities*, 40 FR 28948 (Washington, DC: Jul. 9, 1975).

¹⁰OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum M-03-22 (Washington, DC: Sept. 26, 2003).

of an agency, including those provided or managed by another agency, contractor, or another organization on behalf of an agency. FISMA requires agencies to submit an annual report to OMB, congressional committees, and GAO on the adequacy and effectiveness of their information security policies, procedures, and practices.

OMB is responsible for developing guidelines, providing assistance, and overseeing agencies' implementation of the three acts. For example, OMB has issued guidance on the specifics of what agencies should include in their annual FISMA reports. OMB has also issued guidance on other information security and privacy-related issues including federal agency website privacy policies, interagency sharing of personal information, designation of senior staff responsible for privacy, data breach response and notification, and safeguarding PII.

The Identity Theft Task Force Made Recommendations for Reducing the Unnecessary Collection and Use of SSNs

In 2006, the President issued an Executive Order establishing the Identity Theft Task Force to strengthen efforts to protect against identity theft.¹¹ The task force was directed to review the activities of executive branch departments, agencies, and instrumentalities relating to identity theft, and prepare and submit to the President a coordinated strategic plan to further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution.

Because the unauthorized use of SSNs was recognized as a key element of identity theft, the task force assessed actions the government could take to reduce the exposure of SSNs to potential compromise. It issued a series of reports beginning with interim recommendations in 2006 that called for OPM and OMB to take steps to survey the collection and use of SSNs and take steps to eliminate, restrict, or conceal their use.¹²

In April 2007, the task force issued a strategic plan,¹³ which advocated a unified federal approach, or standard, for using and displaying SSNs. The

¹¹Executive Order 13402, *Strengthening Federal Efforts to Protect Against Identity Theft* (May 10, 2006).

¹²President's Identity Theft Task Force, *Summary of Interim Recommendations* (Washington, D.C.: Sept. 19, 2006).

¹³President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Washington, D.C.: Apr. 11, 2007).

plan proposed that OPM and OMB play key roles in restricting the unnecessary use of SSNs, offering guidance on substitutes that are less valuable to identity thieves, and promoting consistency when the use of SSNs was found to be necessary or unavoidable.

The task force's 2007 plan recommended the following key actions to reduce the unnecessary use of SSNs within the federal government:

- *Issue Guidance on Appropriate Use of SSNs.* The task force recommended that OPM issue policy guidance to the federal human capital management community on the appropriate and inappropriate use of SSNs in employee records, including the appropriate way to restrict, conceal, or mask SSNs in employee records and human resource management information systems.
- *Complete Review of Use of SSNs.* Based on a survey of uses of SSNs in federal personnel forms and records that was conducted in 2006, the task force recommended that OPM take steps to eliminate, restrict, or conceal the use of SSNs, including by assigning alternate employee identification numbers where practicable.
- *Require Agencies to Review Use of SSNs.* Noting that OMB was in the process of surveying agencies on their use of SSNs, the task force recommended that OMB complete an analysis of the surveys to determine the circumstances under which such use could be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms.
- *Establish a Clearinghouse for Agency Practices that Minimize Use of SSNs.* The task force recommended that SSA develop a clearinghouse for agency practices and initiatives that minimize the use and display of SSNs to facilitate the sharing of best practices—including the development of any alternative strategies for identity management—to avoid duplication of effort, and to promote interagency collaboration in the development of more effective measures.

An update to the plan was issued in September 2008, which offered updates on its previously issued recommendations.¹⁴

¹⁴President's Identity Theft Task Force Report, *Combating Identity Theft: A Strategic Plan* (Washington, D.C.: Sept. 2008).

The Federal Government Has Suffered Numerous Data Breaches of SSNs and Other PII

Data breaches—including the unauthorized use and disclosure of PII such as SSNs—pose a persistent threat to government operations and the personal privacy of affected individuals. Thousands of information security incidents involving PII occur every year. For example, in fiscal year 2016, federal agencies reported 8,233 data breaches involving PII to the U.S. Computer Emergency Readiness Team.¹⁵ The following are examples of attacks resulting in the loss or compromise of SSNs and other PII:

- In June 2015, OPM reported that an intrusion into its systems had compromised the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate but related incident had compromised background investigation files on 21.5 million individuals. Background investigation files contain a variety of PII, including SSNs, names, addresses, and references.
- In June 2015, the Commissioner of the IRS testified that unauthorized third parties had gained access to taxpayer information from its Get Transcript service. According to officials, criminals used taxpayer-specific data acquired from non-agency sources to gain unauthorized access to information on approximately 724,000 accounts. These data included SSNs, dates of birth, street addresses, and wage and withholding information.
- In July 2013, the Department of Energy reported that hackers had stolen a variety of PII on more than 104,000 individuals from an agency information system. Types of data stolen included SSNs, birth dates and locations, bank account numbers, and security questions and answers.
- In May 2012, the Federal Retirement Thrift Investment Board reported a sophisticated cyberattack on the computer of a contractor who provided services to the Thrift Savings Plan. As a result of the attack, PII associated with approximately 123,000 plan participants was accessed, including individuals' names and SSNs.

¹⁵U.S. Computer Emergency Readiness Team (US-CERT), a branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, is a central federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to US-CERT.

Prior GAO Reports Highlighted Actions Needed to Reduce Reliance on SSNs

Since 2006, we have issued several reports and testimonies underscoring the widespread use of SSNs in the federal government and highlighting steps that can be taken to minimize their use and display.

- In March 2006, we testified that SSN use was widespread in both the public and private sectors.¹⁶ We stated that although laws were in place at both the state and federal levels to restrict the display of SSNs and protect individuals' personal information, shortcomings remained, such as a lack of uniformity at all levels of government to assure the security of SSNs; gaps in the federal law and oversight in different industries that share SSNs with their contractors; and the exposure of SSNs in public records and government identification cards.
- In May 2006, we reported that few federal laws and no specific industry standards specified whether to display the first five or last four digits of an SSN.¹⁷ We recommended that Congress consider enacting standards for truncating SSNs or delegating authority to SSA or some other government entity to issue standards for truncating SSNs. In 2009, two laws were introduced that addressed standards for truncating SSNs.
- In June 2007, we reported that IRS and the Department of Justice were the only federal agencies that commonly provided records containing SSNs to state and local public record keepers and that both had taken steps to truncate or remove SSNs in those records.¹⁸ We also noted that both full and truncated SSNs in federally generated public records remained vulnerable to potential misuse, in part because different truncation methods used by the public and private sectors could enable the reconstruction of full SSNs. We recommended that the Commissioner of IRS implement a policy requiring the truncation of all SSNs in lien releases the agency generated and that the Attorney General implement a policy requiring,

¹⁶GAO, *Social Security Numbers: More Could Be Done to Protect SSNs*, [GAO-06-586T](#) (Washington, D.C.: March 30, 2006).

¹⁷GAO, *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs*, [GAO-06-495](#) (Washington, D.C.: May 17, 2006).

¹⁸GAO, *Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain*, [GAO-07-752](#) (Washington, D.C.: June 15, 2007).

at a minimum, SSN truncation in all lien records generated by its judicial districts. The agencies implemented both recommendations.

- In September 2013, we reported that CMS had not taken needed steps to select and implement a technical solution for removing SSNs from Medicare cards.¹⁹ We recommended that the agency initiate an IT project to identify, develop, and implement changes to CMS's affected systems, including assessing proposed approaches for the removal of SSNs from Medicare beneficiaries' cards. While CMS has initiated such a project, SSNs have not yet been removed from Medicare cards, as discussed later in this report.

OPM, OMB, and SSA Have Had Limited Success in Assisting With Governmentwide Reduction in the Collection, Use, and Display of SSNs

In response to the recommendations of the Identity Theft Task Force, OPM, OMB, and SSA undertook several actions aimed at reducing or eliminating the unnecessary collection, use, and display of SSNs. However, these actions have had limited success. OPM published a draft regulation to limit federal collection, use, and display of SSNs but withdrew the proposed rule because no alternate federal employee identifier was available that would provide the same utility as SSNs. OMB and SSA also took steps to facilitate reduction in federal SSN collection and use. OMB began requiring agency reporting on SSN reduction efforts as part of the annual FISMA reporting process. In addition, SSA developed an online clearinghouse of best practices; however, this clearinghouse is no longer available, and SSA has no records of when or why the site was discontinued.

¹⁹GAO, *Medicare Information Technology: Centers for Medicare and Medicaid Services Needs to Pursue a Solution for Removing Social Security Numbers from Cards*, [GAO-13-761](#) (Washington, D.C.: Sept. 10, 2013).

OPM Issued Guidance and a Proposed Rule that Was Subsequently Cancelled

In April 2007, the Identity Theft Task Force recommended that OPM issue policy guidance to the federal human capital management community on the appropriate and inappropriate uses of SSNs in employee records, including the appropriate way to restrict, conceal, or mask SSNs in employee records and human resource management information systems. The task force also recommended that OPM identify steps to eliminate, restrict, or conceal the use of SSNs, including by developing and assigning alternate employee identification numbers where practicable.

OPM took several actions in response to the task force recommendations. Using an inventory of its forms, procedures, and systems displaying SSNs that it had developed in 2006, the agency took action to change, eliminate, or mask the use of SSNs on OPM approved/authorized forms, which are used by agencies across the government for personnel records. In addition, in 2007, OPM issued guidance to other federal agencies on actions they should take to protect federal employee SSNs and combat identity theft.²⁰ The guidance reminded agencies of existing federal regulations that restricted the collection and use of SSNs and also specified additional measures, such as eliminating the unnecessary display of SSNs on forms, reports, and computer display screens; ensuring that individuals with authorized access to SSNs understand their responsibilities for protecting them; and ensuring that electronic records containing SSNs are transmitted or transported in an encrypted or protected format.

In addition to issuing this guidance, OPM explored options for establishing a new employee identifier to replace SSNs within the government for human resource and payroll systems. In January 2008, the agency proposed a new regulation regarding the collection, use, and display of SSNs that would have codified the practices outlined in its 2007 guidance and that also required the use of an alternate identifier.²¹

²⁰United States Office of Personnel Management, *Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft* (Washington, D.C.: June 18, 2007).

²¹73 Fed. Reg. 3410 (Jan. 18, 2008).

Specifically, the proposed rule would have required agencies to:

- collect SSNs from an employee only once, at the time of the employee's appointment to a federal position, for entry into human resources and payroll systems;
- not use the SSN as an employee's primary identifier in internal or external data processing activities;
- ensure that SSNs are not printed or displayed on computer display screens;
- restrict access to SSNs to those individuals whose official duties require such access; and
- ensure that access to SSNs, including access involving data entry, printing, and screen displays, occurs in a protected location to guard against exposure.

However, in January 2010, after reviewing comments it had received,²² OPM withdrew the notice of proposed rulemaking because the agency determined that it would be impractical to issue the rule without an alternate governmentwide employee identifier in place.²³ In withdrawing the proposed rule, OPM explained that the comments it had received cited numerous information systems and business practices, both internal and external to the government, which used the SSN as a primary identifier. Without a viable alternate identifier in place, OPM said it would be impractical to modify or stop using these systems.

With the onset of the efforts to reduce the collection and use of SSNs, OPM asserted that a new unique employee identifier would be an important tool in combating the problem of identity theft in the federal government, and it focused on creating such an identifier. However, after its proposed rule was withdrawn in 2010, the agency stopped working on the project. Officials from OPM's Office of the Chief Information Officer stated that no government-wide initiative to develop such an identifier has been undertaken since that time.

Instead, in 2015 OPM briefly began exploring the concept of developing and using multiple alternate identifiers for different programs and

²²The January 2008 notice in the *Federal Register* had solicited comments from the public on OPM's proposed rule.

²³75 Fed. Reg. 4308 (Jan. 27, 2010).

agencies. As envisioned by OPM, the unique identifier for each program would be linked to an SSN, but the SSN and the link would be protected and not used by agency systems and personnel on an everyday basis. Ideally, an SSN would be collected only once, at the start of an employee's service, after which unique identifiers specific to relevant programs, such as healthcare benefits or training, would be assigned as needed. However, work on the initiative was suspended in 2016 due to the lack of funding. OMB staff subsequently stated that, while they endorse the concept of developing and using alternate identifiers, they had not had a chance to review OPM's specific proposal.

OMB Established Reporting Requirements for Agency SSN Reduction Efforts

The Identity Theft Task Force recommended that OMB require agencies to review their use of SSNs to determine the circumstances under which such use could be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms. In its April 2007 plan, the task force noted that OMB was in the process of surveying agencies on their use of SSNs and should complete its review sometime in 2007.

In May 2007, OMB issued a memorandum officially requiring agencies to review their use of SSNs in agency systems and programs to identify instances in which the collection or use of SSNs was superfluous.²⁴ Agencies were also required to establish a plan, within 120 days from the date of the memorandum, to eliminate the unnecessary collection and use of SSNs within 18 months. Lastly, the memorandum required agencies to participate in governmentwide efforts, such as surveys and data calls, to explore alternatives to SSN use as a personal identifier for both federal employees and in federal programs. In 2016, OMB issued a revision to its Circular A-130 that reiterated its direction to agencies to take steps to eliminate unnecessary collection, maintenance, and use of SSNs and explore alternatives to the use of SSNs as a personal identifier.²⁵

Since issuing its May 2007 memorandum requiring the development of SSN reduction plans, OMB annually has instructed agencies to submit

²⁴OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Memorandum M-07-16 (Washington, D.C.: May 22, 2007).

²⁵OMB, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: 2016).

updates to their plans and documentation of their progress in eliminating unnecessary use of SSNs as part of their annual FISMA reports. In 2016, questions were added to the FISMA reporting instructions, directing agencies to report:

- whether they had a written inventory of their collection and use of SSNs;
- whether they had developed and implemented a written policy or procedure to ensure that any new collection or use of SSNs was necessary or whether any ongoing collection remained necessary; and
- whether they had developed and implemented a written policy or procedure to ensure that any collection or use of SSNs associated with agency websites, online forms, mobile applications, and other digital services, was necessary and complied with applicable privacy and security requirements.²⁶

SSA Established, but then Discontinued, an Online Information Sharing Clearinghouse

The Identity Theft Task Force recommended that, based on the results of OMB's review of agency practices on the use of SSNs, SSA should establish a clearinghouse of agency practices and initiatives that minimize the use and display of SSNs. The purpose of the clearinghouse was to facilitate the sharing of "best" practices—including the development of any alternative strategies for identity management—to avoid duplication of effort, and to promote interagency collaboration in the development of more effective measures for minimizing the use and display of SSNs.

In 2007, SSA formed the Social Security Number Collaborative as a forum for interagency meetings to jointly review and share best practices for minimizing the use of SSNs, explore possible alternatives to their use, and establish a medium for ongoing sharing of best practices and continuous improvement. The Collaborative included representatives from 36 agencies and met regularly in 2007. The same year, SSA established a clearinghouse on an electronic bulletin board website to share materials regarding agency efforts to minimize the use and display of SSNs. The clearinghouse showcased best practices and provided agency contacts for specific programs and initiatives.

²⁶Department of Homeland Security, *FY 2016 Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Reporting Metrics v1.0* (Washington, D.C.: June 2016).

According to officials in the Office of the Deputy Commissioner, the Collaborative has not met since 2007 and the clearinghouse is no longer active. The officials added that SSA did not maintain any record of the extent to which the clearinghouse was accessed or used by other agencies when it was available online. Further, the officials said SSA has no records of when or why the site was discontinued.

Agencies Reported Reducing Their Use and Display of SSNs and Cited Ongoing Challenges; Moreover, Poor Planning and Ineffective Monitoring Have Limited Their Efforts

In their responses to our questionnaire on SSN reduction efforts, the 24 CFO Act agencies reported successfully curtailing the collection, use, and display of SSNs, thereby reducing individuals' exposure to the risk of identity theft. Nevertheless, all of these agencies continue to rely on SSNs for important government programs and systems, and they have cited challenges to further reduction of SSN collection, use, and display. Moreover, poor planning by many of the 24 agencies and ineffective oversight by OMB have limited SSN reduction efforts. Most of the agencies' reduction plans lacked key elements, limiting their usefulness, and not all agencies maintained an up-to-date inventory of their SSN collections. Also, definitions of "unnecessary" collection and use have been inconsistent across the 24 agencies. Further, OMB's monitoring of agency progress has been ineffective in that it has not ensured that agencies have provided up-to-date status information about their reduction efforts or established performance metrics to assess agency progress. Without a more rigorous monitoring process, it will remain difficult for OMB to determine whether agencies have eliminated all unnecessary collection, use, and display of SSNs and thus whether they have taken all reasonable steps to reduce the risk that individuals could become victims of identity theft due to their SSNs being exposed.

Agencies Have Reported Taking Actions to Reduce the Unnecessary Use and Display of SSNs

Based on responses to our questionnaire, all of the 24 CFO Act agencies reported having taken steps to reduce the unnecessary collection, use, and display of SSNs. Examples of activities agencies undertook include developing and using alternate identifiers, removing SSNs from printed forms and other physical displays, and filtering e-mail to prevent unencrypted transmittal of SSNs. Agencies also generally reported that they have processes in place to review ongoing collection, use, and display of SSNs.

Developing and Using Alternate Identifiers

Officials from four agencies reported that they had transitioned, or were transitioning, to the use and display of alternate identifiers or the use of

alternate identification procedures for specific programs and activities. In these cases, the use of alternate identifiers or identification procedures has eliminated the need to display SSNs on identification cards or use them for identification purposes. Specifically:

- In 2012, DOD issued a department-wide policy to reduce or eliminate the use of SSNs wherever possible.²⁷ In a number of cases, the department was able to replace SSN use by substituting its 10-digit identification number, a number that is randomly generated for every person by the department's personnel system.²⁸ For example, DOD reported that its identification cards, which as of March 2017 were being used by 11 million individuals, now display the DOD identification number rather than an SSN. In addition, based on departmental policy, in November 2015, the Department of the Army began replacing SSNs on soldiers' dog tags with DOD identification numbers. The Army reported that several information systems had to be modified to use the identification number instead of the SSN.
- In 2013, the Veterans Health Administration (VHA) within VA removed SSNs from veteran health identification cards, which VHA issues to veterans when they enroll in health care. VHA developed its own integration control number (ICN) as a unique identifier in 1998 and began using it on veteran health identification cards in 2004. Nevertheless, those cards continued to include an individual's SSN on the barcode and magnetic stripe. Beginning in 2013, VHA issued redesigned cards that display the DOD identification number rather than the ICN. The ICN is still included on the card's barcode and magnetic stripe and now serves as the primary patient identifier; however, SSNs are no longer included on the cards in any form. VA's two other major components (the National Cemetery Administration and the Veterans Benefit Administration) also currently use the ICN. The department is in the process of transitioning the remainder of the agency to the ICN, as well.
- CMS (a component of HHS) recently began taking steps to remove SSNs from Medicare cards. We reported²⁹ in 2012 that Medicare

²⁷Department of Defense Instruction 1000.30: *Reduction of Social Security Number (SSN) Use Within DoD* (August 1, 2012).

²⁸The DOD Identification Number, also known as the Electronic Data Interchange Personal Identifier, is a unique personal identifier created within the Defense Enrollment Eligibility Reporting System for each person who has a direct relationship with DOD.

²⁹GAO, *Medicare: Action Needed to Remove Social Security Numbers from Medicare Cards*, [GAO-12-949T](#) (Washington, D.C.: Aug. 1, 2012).

cards displayed an SSN as part of the health insurance claim number that appeared on the card. While CMS had identified various options for removing the SSN from Medicare cards, the agency had not committed to a plan for such removal.³⁰ However, the Medicare Access and CHIP Reauthorization Act of 2015 subsequently required CMS to remove SSNs from all Medicare cards and distribute replacement cards with a new Medicare beneficiary identifier by April 2019. CMS officials stated that the agency plans to begin removing SSNs from Medicare cards and replacing them with the new identifier starting in April 2018.

- In 2015, the Department of Education’s Federal Student Aid office changed login procedures for students, parents, and borrowers, by introducing a federal student aid username and password to be used in place of previous login procedures that relied on a personal identification number associated with the user’s name, SSN, and date of birth. Education officials from the Office of the Chief Privacy Officer reported that, since being introduced, the usernames and passwords have been used over 300 million times to log in to office systems, greatly reducing the exposure of SSNs and other PII.

Removing SSNs from Printed Forms and Other Physical Displays

Even when SSNs continue to be used as identifiers within internal information systems, the 24 CFO Act agencies reported taking steps to mask, truncate, or block the display of these numbers on paper forms, correspondence, and computer screens. For example:

- In 2001, SSA removed the full SSN from the Social Security statement and the Social Security cost-of-living-adjustment notice and replaced it with a beneficiary notice code. These two documents represented approximately one-third of all SSA notices sent each year, with approximately 150 million Social Security statements and approximately 58 million cost-of-living-adjustment notices going out each year, according to SSA. However, SSA still displays SSNs on much of its correspondence. According to the SSA Office of the Inspector General, about 66 percent of the 352 million notices sent to

³⁰In 2013 we reported that since 2006, CMS had conducted three studies on potential approaches to replacing the SSN-based Medicare identifier that, at a high level, addressed the impact of various approaches on CMS’s IT environment. The studies were not intended to identify a specific technical solution for removing SSNs from Medicare cards. See GAO, *Medicare Information Technology: Centers for Medicare and Medicaid Services Needs to Pursue a Solution for Removing Social Security Numbers from Cards*, [GAO-13-761](#) (Washington, D.C.: Sep. 10, 2013).

individuals in 2015 included the individuals' full SSNs.³¹ SSA officials from the Office of the Deputy Commissioner for Budget, Finance, Quality, and Management stated that they had plans to further reduce SSNs on notices and would implement them as resources permit.

- IRS (a component of the Department of the Treasury) implemented a system to replace or mask the SSN displayed on many notices and letters sent to taxpayers. IRS officials in the office of Privacy, Governmental Liaison and Disclosure stated that, as of 2017, they had been able to update many notices and letters to either display a barcode, or mask the SSN by displaying only the last four digits of the number. According to the officials, these updates affected 50 million notices in fiscal year 2015 and 47 million in fiscal year 2016.
- In 2007, the VA Consolidated Mail Outpatient Pharmacy eliminated the use of SSNs on prescription bottles and mailing labels. VHA officials stated that VHA uses the truncated SSN on many of its forms, printouts, and surgical materials. In addition, according to the officials, VHA discontinued printing the full SSN on health records that are disclosed through the Release of Information process and removed or truncated the SSN from patient appointment reminders in 2013.

Filtering E-mail to Prevent Unencrypted Transmittal of SSNs

Officials from two agencies reported taking additional steps to reduce the potential for SSNs to be compromised by screening e-mail traffic for the numbers and blocking the numbers' transmittal. Specifically, the Bureau of Economic Analysis in the Department of Commerce implemented a filter on its e-mail system to block both incoming and outgoing e-mails containing SSNs. In addition, the Department of Justice upgraded its data loss prevention capabilities to automatically block e-mail traffic to external, nongovernment users when an SSN is detected either in the body of an e-mail or in an e-mail attachment.

Reviewing Ongoing Collection, Use, and Display of SSNs

Officials from the 24 CFO Act agencies generally stated that they use their already existing information security and privacy management processes and procedures to review ongoing collection, use, and display of SSNs and to ensure that SSNs are protected when stored in agency

³¹SSA Office of the Inspector General, *Evaluation Report: Social Security Administration Correspondence Containing Full Social Security Numbers*, A-04-15-50070 (Baltimore, Md.: Apr. 27, 2016).

information systems. Specifically, agencies typically reported using existing processes for developing and approving privacy impact assessments to determine whether new collection, use, or display of SSNs is necessary to achieve an agency mission. For example, CMS, IRS, Department of Transportation, USDA, and VA officials all stated that they use the privacy impact assessment or privacy risk analysis process to confirm that planned collections of SSNs are appropriate and authorized and to assess plans to mitigate the risks of such uses when they are unavoidable.

Officials from two of the agencies also reported setting restrictions on access to SSNs and limiting the ability of staff to download and store personal information covered by the Privacy Act, including SSNs, and on the transmission or electronic transfer of such data. For example, CMS officials stated that departmental policy requires encryption of all sensitive data, including SSNs, which are transmitted outside of the hhs.gov domain. VA likewise requires that full SSNs not be transmitted or stored in electronic form unless the data are encrypted. Departmental policy also requires VA components to assign access to data containing SSNs based on need-to-know and least-privilege principles and to use only VA-approved portable electronic storage media to maintain and access records that contain SSNs.

Agencies Cited Challenges in Further Reducing SSN Collection and Use

Officials from the 24 agencies stated that SSNs cannot be completely eliminated from federal IT systems and records. In some cases, no other identifier offers the same degree of universal awareness or applicability. For example, VHA officials stated that they need to collect SSNs from patients when they receive treatment because health standards require unique identifying information to be verbally provided by patients for verification purposes. According to VHA officials from the Information Access and Privacy Office, the SSN is one of the few unique identifiers that a patient can be expected to have memorized. Thus, eliminating its use is not feasible. SSA officials noted that the Social Security program, as authorized by law, uses the SSN as its primary identifier, and, thus, much of its use within that agency cannot be reduced.

Even when reductions are possible, challenges in implementing them can be significant. All of the agencies we reviewed reported experiencing such challenges. Three key challenges were frequently cited: (1) statutes and regulations that mandate the collection of SSNs, (2) requirements for using SSNs in interactions with other federal and external entities, and (3) technological impediments to implementing changes in agency systems

and processes. Of the 24 agencies we reviewed, 15 reported to us that they had experienced challenges as a result of statutes and regulations, 16 as a result of required interactions with other Federal and external entities, and 14 as a result of technological limitations, as follows:

- *Statutes and regulations require collection and use of SSNs.* In their questionnaire responses and follow-up correspondence with us, officials from 15 agencies who were involved in their agencies' SSN reduction efforts noted that they are limited in their ability to reduce the collection of SSNs because many laws authorize or require such collection. Examples of such laws are listed in table 1, and the officials cited other laws as well. These laws often explicitly require agencies to use SSNs to identify individuals who are engaged in transactions with the government or who are receiving benefits disbursed by federal agencies. For example, Commerce officials said they are required by the Debt Collection Act of 1996 to collect SSNs for all financial transactions, such as permit applications. Similarly, Department of the Interior officials stated that several statutes require the collection of SSNs for employment, payroll, tax reporting, benefits, and other processes, including the Immigration Reform and Control Act of 1986, the Consolidated Appropriations Act, 2008, and others.
- *Interactions with other federal and external entities require use of the SSN.* In order for federal agencies to exchange information about individuals with other entities, both within and outside the federal government, they must be able to cite a unique, common identifier to ensure that they are matching their information to the correct records in the other entities' systems. The SSN is typically the only identifier that government agencies and external partners have in common that they can use to match their records. USDA's National Finance Center, for example, uses SSNs to identify employees in its payroll processing systems, and, thus, agencies that use the National Finance Center must include SSNs in their payroll records. Further, other agencies rely on SSNs as unique identifiers when performing other common cross-agency functions, such as processing payments to or from external entities, conducting background investigations, and determining whether an individual has benefit coverage through another agency. For example, an official from the Department of Education stated that the Federal Student Aid program is required to use a loan applicant's SSN for several key verification functions before being able to process the loan, including with SSA to confirm that the SSN provided is legitimate and that the applicant has registered for the draft; with IRS to ensure the applicant is in good tax standing; with HHS to verify the applicant is not delinquent with child

support; and with the Department of Homeland Security to verify the applicant is not on the terrorist watch-list.

- *Technological hurdles can slow replacement of SSNs in information systems.* In their questionnaire responses and follow-up correspondence with us, officials from 14 agencies who were involved in their agency SSN reduction efforts cited the complexity of making required technological changes to their information systems as a challenge to reducing the use, collection and display of SSNs. For example, VA officials noted that key software applications and electronic health record formats used in their legacy information systems were developed over 30 years ago and would require extensive system changes and software updates because SSNs are the only identifier used by those systems. Likewise, Department of Treasury officials stated that a majority of their systems had technological limitations that kept them from masking the display of SSNs. According to these officials, they send out “hundreds” of standard notices to individuals but have been able to mask the SSN on only 110 non-payment notices, four payment notices, and 24 automated collection system notices, due to technological limitations. Likewise, although the IRS has been able to mask SSNs on notices that contain barcodes, its current payment processing system is unable to read such barcodes. As a result, the full SSN remains on display on the majority of IRS payment processing notices.

Poor Planning and Ineffective Monitoring by OMB Have Also Limited the Extent of Agency Reduction Efforts

SSN reduction efforts in the federal government have also been limited by more readily addressable shortcomings. Lacking direction from OMB, many agencies’ reduction plans did not include key elements, such as timeframes and performance indicators, calling into question the plans’ utility. In addition, OMB has not required agencies to maintain up-to-date inventories of SSN collections and has not established criteria for determining when SSN use or display is “unnecessary,” leading to inconsistent definitions across the agencies. Finally, OMB has not ensured that agencies have all submitted up-to-date status reports and has not established performance measures to monitor agency efforts.

Agency SSN Reduction Plans Lacked Key Elements, Limiting Their Usefulness

As previously mentioned, in May 2007, OMB issued a memorandum requiring agencies to develop plans to eliminate the unnecessary

collection and use of SSNs, an objective that was to be accomplished within 18 months.³² OMB did not set requirements for agencies on creating effective plans to eliminate the unnecessary collection and use of SSNs. However, other federal laws and guidance have established key elements that performance plans generally should contain. For example, GPRAMA established criteria for effective performance plans, including specific measures to assess performance. Our prior work on developing performance plans identifies additional elements of effective plans,³³ as does OMB's guidance on budget preparation.³⁴ Several key elements of an effective performance plan that were consistently referenced across these sources include:

- Performance goals and indicators: Plans should include tangible and measurable goals against which actual achievement can be compared. Performance indicators should be defined to measure outcomes achieved versus goals.
- Measurable activities: Plans should define discrete events, major deliverables, or phases of work that are to be completed toward the plan's goals.
- Timelines for completion: Plans should include a timeline for each goal to be completed that can be used to gauge program performance.
- Roles and responsibilities: Plans should include a description of the roles and responsibilities of agency officials responsible for the achievement of each performance goal.

The majority of plans originally submitted to OMB by the 24 CFO Act agencies lacked key elements of effective performance plans. For example, only two agencies (the Departments of Commerce and Education) developed a plan that addressed all four key elements. Three agencies' plans did not fully address any of the key elements, nine plans

³²Office of Management and Budget, *Safeguarding and Responding to the Breach of Personally Identifiable Information*, Memorandum M-07-16 (Washington, D.C.: May 22, 2007). OMB recently rescinded and replaced this guidance with an updated memorandum. See OMB, *Preparing for and Responding to a Breach of Personally Identifiable Information*, Memorandum M-17-12 (Washington, D.C.: Jan. 3, 2017).

³³GAO, *Managing for Results: Critical Issues for Improving Federal Agencies' Strategic Plans*, [GAO/GGD-97-180](#) (Washington, D.C. Sep. 16, 1997).

³⁴OMB, Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, Section 6 (Washington, D.C.: Jul. 1, 2016).

addressed between one and two of the elements, and the remaining 10 plans addressed three of the elements. Table 2 shows the key elements addressed in each agency's plan.

Table 2: Key Performance Plan Elements Addressed in Original Agency Social Security Number (SSN) Reduction Plans

Agency	Performance Goals and Indicators	Measurable Activities	Timelines for Completion	Roles and Responsibilities
Department of Agriculture	○	●	●	●
Department of Commerce	●	●	●	●
Department of Defense	○	○	○	●
Department of Education	●	●	●	●
Department of Energy	○	○	○	○
Department of Health and Human Services	○	●	●	○
Department of Homeland Security	○	●	○	●
Department of Housing and Urban Development	○	●	●	●
Department of the Interior	○	●	●	●
Department of Justice	○	●	●	●
Department of Labor	○	●	●	○
Department of State	○	●	●	○
Department of Transportation	○	○	○	○
Department of the Treasury	○	●	●	●
Department of Veterans Affairs	○	●	○	●
Environmental Protection Agency	○	●	○	○
General Services Administration	○	○	○	○
National Aeronautics and Space Administration	○	●	●	●
National Science Foundation	○	●	○	○
Nuclear Regulatory Commission	○	●	●	●
Office of Personnel Management	○	●	●	●
Small Business Administration	○	●	●	●
Social Security Administration	○	●	●	○
U.S. Agency for International Development	●	●	●	○
Total Met	3	20	16	14

Legend: ● Met—the agency addressed the key element in its SSN reduction plan. ○ Not met—the agency did not fully address the key element in its SSN reduction plan.

Source: GAO analysis of agency SSN reduction plans | GAO-17-553

Across the 24 agencies, the most frequently met criterion was establishing measurable SSN reduction activities and the least frequently met was the development of overall performance goals. For example:

- *Performance goals and indicators:* Three agencies established performance goals and indicators to measure progress in their SSN reductions plan. For example, the Department of Education

established a goal of eliminating unnecessary SSN use by 5 percent by the second quarter of fiscal year 2010.

- *Measurable activities:* Twenty agencies established specific measurable activities in their SSN reduction plans. For example, HHS's activities included categorizing SSN collections as mandatory or discretionary, developing guidance for review of SSN use, scheduling all 2009-2010 information collections for SSN review, and reviewing expiring 2008 information collections for SSN use. Similarly, the Department of Commerce's planned activities included eliminating the use of SSNs within four economic surveys at the Census Bureau, the EZ Tracker Training System, and in building access systems at four major facilities.
- *Timelines for completion:* Sixteen agencies provided a timeline for completion. For example, the Department of the Interior set completion dates for its major SSN reduction activities, such as establishing an information reduction team by October 12, 2007 and obligating the team to complete all tasks, including updating system of record notices, and enacting component reduction activities, by December 31, 2007.
- *Roles and responsibilities:* Fourteen agencies identified roles and responsibilities for reducing agency SSN collection, use, and display. For example, USDA assigned responsibility for departmental compliance with the requirements of OMB M-07-16 to its Chief Information Officer. In addition, the Department of Housing and Urban Development assigned responsibility for tracking progress of SSN reduction activities to its Privacy Act Officer.

Agency officials stated that because OMB did not set a specific requirement that SSN reduction plans contain clearly defined performance goals and indicators, measurable activities, timelines for completion, or roles and responsibilities, they were not aware that they should address these elements. Yet, without complete performance plans, it is difficult to determine what overall progress agencies have achieved in reducing the unnecessary collection and use of SSNs and the concomitant risk of exposure to identity theft. Continued progress toward reducing that risk is likely to remain difficult to measure until agencies develop and implement effective plans.

Not All Agencies Maintain an Up-to-Date Inventory of Their SSN Collections

Developing a baseline inventory of systems that collect, use, and display SSNs and ensuring that it is periodically updated can assist managers in

maintaining an awareness of the extent to which they collect and use SSNs and their progress in eliminating unnecessary collection and use. GAO's *Standards for Internal Control in the Federal Government* states that a baseline should be established to monitor progress towards an objective.³⁵ An accurate inventory provides a detailed description of an agency's current state and helps to clarify what additional work remains to be done to reach the agency's goal.

Of the 24 CFO Act agencies, 22 reported having compiled an inventory of systems and programs that collected SSNs at the time they developed their original SSN reduction plans in fiscal years 2007 and 2008. Of the two agencies that reported not developing an initial inventory, one (U. S. Agency for International Development) reported that it did not have a comprehensive inventory of systems containing SSNs because it has no visibility over unofficial programs and systems, especially those created by overseas missions to address site-specific programmatic and administrative requirements. The agency stated that it was undertaking an effort to create such an inventory and that as part of that process it intended to identify systems that collect and maintain SSNs. The agency anticipated completing its inventory by the end of fiscal year 2017. The other agency without an SSN inventory (Small Business Administration) likewise stated that it was in the process of creating such an inventory, but it did not provide details on when this effort began or when it was expected to be completed.

Of the 22 agencies that reported having developed an initial inventory, 18 stated that they had inventories that were up-to-date and complete. However, the inventories of these agencies did not always identify which systems contained SSNs. For example, DOD and SSA officials stated that they maintain an inventory of systems containing PII but do not always track which systems in the inventory contain SSNs.

Beyond simply determining which systems contain SSNs, identifying the approximate number of individual records containing SSNs would also be a useful measure for agencies to understand the extent to which any given system contains SSNs. However, agencies have not always captured this information. Education officials, for example, noted that they did not have figures for how many records within each of their student

³⁵GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

loan systems contained SSNs. DOD, Interior, and State all have many systems containing PII but no estimate of the number of records that include SSNs within each of these systems.

Of the 22 agencies that reported having developed an initial inventory, the four remaining agencies stated that they did not have up-to-date inventories of systems containing SSNs. Two of them (Energy and VA) reported having efforts underway to correct or update their inventories. Officials from the Department of Housing and Urban Development and the National Science Foundation stated they faced technical difficulties identifying systems, including contractor-operated systems that contain SSNs.

Part of the reason agencies do not have up-to-date inventories is that OMB M-07-16 did not require agencies to develop an inventory or to update the inventory periodically to measure reduction of SSN collection and use. Nevertheless, OMB has recognized the value of maintaining an accurate inventory and as part of the fiscal year 2016 FISMA submission asked agencies to state whether they maintain a written inventory of the collection and use of SSNs.³⁶ OMB staff stressed that, despite these instructions, they were not requiring agencies to maintain inventories of systems that contain SSNs.

However, OMB guidance does require agencies to maintain an inventory of systems that “create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.”³⁷ The OMB guidance states that agencies are required to maintain that inventory in part to allow the agency to reduce its PII to the minimum necessary. Without modifying these PII inventories to indicate which systems contain SSNs and using them to monitor their SSN reduction efforts, agencies will likely find it difficult to measure their progress in eliminating the unnecessary collection and use of SSNs.

³⁶OMB, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-16-03 (Washington, D.C.: Oct. 30, 2015) and Department of Homeland Security, *FY 2016 Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Reporting Metrics* (Washington, D.C.: June 29, 2016).

³⁷OMB, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: 2016).

Agency Definitions of “Unnecessary” Collection and Use Have Been Inconsistent

It can be difficult to achieve consistent results from any management initiative when the objectives are not clearly defined. GAO’s *Standards for Internal Control in the Federal Government* states that management should define objectives in measurable terms so that performance toward achieving those objectives can be assessed. Further, measurable objectives should generally be free of bias and not require subjective judgments to dominate their measurement.³⁸

However, OMB M-07-16 did not provide clear criteria for determining what would be an unnecessary collection or use of SSNs, leaving agencies to develop their own interpretations. Of the 24 CFO Act agencies, 4 reported that they had no definition of “unnecessary collection and use.” Of the other 20 agencies, 7 reported that their definitions were not documented. Officials from the 7 agencies with undocumented definitions stated that the process of reviewing and identifying unnecessary uses of SSNs was informal and relied on subjective judgments. For example:

- Other agency officials, including the Privacy Officer from the General Services Administration, the Chief Information and Privacy Officer from the National Science Foundation, and the Chief Privacy Officer from the Small Business Administration, stated that the determination of whether a specific collection or proposed use was necessary was the decision of agency officials involved in various system reviews, including privacy impact assessment review processes and system authority-to-operate approvals.
- In contrast, officials from the Office of the Chief Privacy Officer of the Department of Education stated that, while they had no written definition of “unnecessary collection and use,” their departmental policy was that SSNs could not be collected or used unless authorized by law, regulation, or executive order, and/or necessary for a documented agency purpose. Further, their policy required documentation indicating that no reasonable alternative existed.

Given the varying approaches that agencies have taken to determining whether proposed or actual collections and uses of SSNs are necessary, it is doubtful whether the goal of eliminating unnecessary collection and

³⁸GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

use of SSNs is being implemented consistently across the federal government. OMB has not subsequently provided criteria for determining “unnecessary collection and use” of SSNs. OMB staff in the Office of Information and Regulatory Affairs stated that they had not developed a precise definition of “unnecessary collection and use” because the circumstances of collection and use of SSNs varied across agencies. However, developing guidance for agencies in the form of criteria for making decisions about what types of collections and uses of SSNs are unnecessary need not be narrowly prescriptive. Until such criteria are established, agency efforts to reduce the unnecessary use of SSNs will likely continue to vary, and, as a result, the risk of unnecessarily exposing SSNs to identity theft may not be mitigated as thoroughly as it could be.

Agencies Have Not Always Submitted Up-to-Date Status Reports to OMB, and OMB Has Not Set Performance Measures to Monitor Agency Efforts

GAO’s Standards for Internal Control in the Federal Government calls for management to conduct activities to monitor and evaluate performance. The activities can occur at a specific time or for a specific function or process, while the scope and frequency depend primarily on the assessment of risks. Monitoring is essential to help keep initiatives aligned with changing objectives, environment, laws, resources, and risks. It also assesses the quality of performance over time and allows corrective actions to be identified, if necessary, to achieve the original objectives.

OMB initially recognized that agency SSN reduction plans needed to be monitored. After reviewing the reduction plans that agencies submitted for fiscal year 2008, OMB reported that the plans displayed varying levels of detail and comprehensiveness and stated that agency reduction efforts would require ongoing oversight.³⁹ Subsequently, it required agencies to report on their progress annually through their annual FISMA reports.⁴⁰

³⁹Office of Management and Budget, *Fiscal Year 2008 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*, Memorandum M-08-21 (Washington, D.C.: August 13, 2008, revised).

⁴⁰Office of Management and Budget, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Memorandum M-09-29 (Washington, D.C.: August 20, 2009).

However, OMB did not establish specific performance measures to monitor implementation of agency reduction efforts. OMB's guidance directed agencies to submit their most current documentation related to their implementation plans and report on progress they had made in eliminating unnecessary uses of SSNs. However, the guidance did not ask for progress in achieving performance measures or targets that had been identified in agency plans.

Annual updates submitted by the 24 agencies from fiscal year 2013 through 2015 did not always include up-to-date information about agency efforts and results achieved, making it difficult to monitor whether progress had been made. For example, in each of its reports over this period, the Department of State indicated that it had a review of over 100 systems underway, with little description of whether any progress had been made. Similarly, the Department of Transportation stated in each of its reports that privacy officials continue to work with departmental components to justify, and as appropriate, reduce holdings of PII across systems and business processes. However, none of the reports indicated whether these efforts had been completed or what the results were. Small Business Administration's updates for all three years consisted of the same document, dated August 2013. OMB staff from the Office of Information and Regulatory Affairs agreed that some agencies had provided the same information year after year in their annual updates, arguing that it was acceptable to do so if all reduction efforts had been completed. However, this was not the case with any of the three agencies, which all indicated that reduction efforts were still underway.

Further, other than its initial review in 2008, OMB has only recently begun monitoring agency efforts to reduce SSNs. Specifically, staff from the Office of Information and Regulatory Affairs reported that they performed a review in 2015 and determined that agency efforts had been largely successful. While they did not set specific criteria for measuring performance, they noted that the agencies with the most robust and mature SSN reduction efforts had developed inventories for their SSN collections, defined unnecessary use, and established processes to continue assessing whether SSN collections were necessary over time. However, the OMB staff were unable to provide any documentation of their review.

In fiscal year 2016, OMB began asking agencies additional questions about their reduction of SSNs. For example, questions were added to the FISMA reporting metrics which require each agency to indicate whether it has (1) compiled a written inventory of the agency's collection and use of

SSNs, (2) developed and implemented written policies or procedures to ensure that any new collection or use of SSNs is necessary and remains necessary over time, and (3) determined that any existing collection or use of SSNs associated with agency websites, online forms, mobile applications, and other digital services, is necessary and complies with privacy and security requirements.⁴¹ OMB staff in the Office of Information and Regulatory Affairs stated that they expect that the answers to these questions will help inform future reviews of agency programs and will help define metrics for use in future years.

Thus, although OMB has taken steps to gather additional information related to agency SSN reduction programs, its monitoring process is still not based on performance measures that could be used to ensure consistent and effective implementation of agency reduction efforts. Without a more rigorous process, it will remain difficult for OMB to determine whether agencies have achieved their goals in eliminating the unnecessary collection and use of SSNs or whether additional actions could be taken to minimize the risk of unnecessarily exposing SSNs to identity theft.

Conclusions

Beginning in 2007, following the report of the Identity Theft Task Force, OPM, SSA, and OMB took steps to promote elimination of the unnecessary collection, use, and display of SSNs. However, those efforts had limited success. OPM's effort to define an alternate identifier ended when it withdrew its proposed rulemaking on the use of SSNs, and SSA's clearinghouse of key SSN reduction practices is no longer available online. Only OMB's annual reporting requirement is still ongoing.

The 24 agencies we reviewed have responded by taking a number of actions to reduce the use and display of SSNs, either by substituting alternate identifiers or limiting the display of the SSN on forms and/or computer screens. The initiatives agencies have taken show that it is possible to identify and eliminate the unnecessary use and display of SSNs. However, it is difficult to determine what overall progress has been made in achieving this goal across the government. Lacking OMB direction to do so, not all agencies have developed effective SSN reduction plans. In addition, OMB has not required agencies to maintain

⁴¹Department of Homeland Security, *FY 2016 Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Reporting Metrics v1.0* (Washington, D.C.: June 2016).

up-to-date inventories of their collection and use of SSNs and has not established criteria for determining when the collection, use, or display of SSNs is “unnecessary,” leading to inconsistent definitions across the agencies. Finally, OMB has not ensured that agencies have all submitted up-to-date status reports and has not established performance measures to monitor agency efforts. Until OMB adopts more effective practices for guiding agency SSN reduction processes, overall governmentwide reduction efforts will likely remain limited and difficult to measure, and the risk of SSNs being exposed and used to commit identity theft will remain greater than it need be.

Recommendations for Executive Actions

To improve the consistency and effectiveness of governmentwide efforts to reduce the unnecessary use of SSNs and thereby mitigate the risk of identity theft, we are recommending that the Director of OMB take the following five actions:

- specify elements that agency plans for reducing the unnecessary collection, use, and display of SSNs should contain and require all agencies to develop and maintain complete plans;
- require agencies to modify their inventories of systems containing PII to indicate which systems contain SSNs and use the inventories to monitor their reduction of unnecessary collection and use of SSNs;
- provide criteria to agencies on how to determine unnecessary use of SSNs to facilitate consistent application across the federal government;
- take steps to ensure that agencies provide up-to-date status reports on their progress in eliminating unnecessary SSN collection, use, and display in their annual FISMA reports; and
- establish performance measures to monitor agency progress in consistently and effectively implementing planned reduction efforts.

Agency Comments and Our Evaluation

We provided draft copies of this report to OMB and the 24 CFO Act agencies included in our review. OMB did not provide comments on the draft report or our recommendations.

We received written comments from one agency, SSA, which are reprinted in appendix III. In its comments, the agency stated that it has taken steps, where possible, to discontinue the use of the SSN in its two largest annual notice workloads and in many internal administrative

processes. SSA added that it remains committed to removing the SSN from its remaining notices.

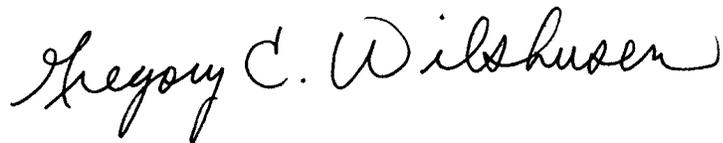
In addition, SSA, along with eight other agencies, provided technical comments or information on their current SSN reduction policies, which have been incorporated into the final report as appropriate. These agencies are the Departments of Commerce, Education, Health and Human Services, Homeland Security, the Interior, Justice and Veterans Affairs, and the General Services Administration. For example, a Program Analyst in General Services Administration's Audit Management Division stated that each system containing PII requires a full privacy impact assessment that is completed by the system owner or program manager in coordination with the Privacy Office. The official also stated that new and current system owners are encouraged not to collect SSNs or other PII unless there is a good business case. Further, the Department of Interior Audit Liaison stated that the department is revising its SSN reduction policy to address the findings and recommendations to OMB outlined in our report. The official stated that the department will work closely with its bureaus and offices to implement the updated SSN reduction policy, maintain current SSN inventories, and establish procedures and a standard reporting template to identify and eliminate the unnecessary collection and use of SSNs.

Lastly, 15 agencies indicated via e-mail that they had no comments on the report. These agencies were the Departments of Agriculture, Defense, Energy, Housing and Urban Development, Labor, State, Transportation, and the Treasury, and the Agency for International Development, Environmental Protection Agency, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, and Small Business Administration.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until two days from the report date. At that time, we will send copies to the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Agency for International Development; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Management and Budget; Office of Personnel Management; Small Business Administration; and Social Security Administration. In addition, the report is available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@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 key contributions to this report are listed in appendix IV.

Sincerely yours,

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, stylized "G" and "W".

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) what governmentwide initiatives have been undertaken to assist agencies in eliminating their unnecessary use of SSNs and (2) the extent to which agencies have developed and executed plans to eliminate the unnecessary use and display of SSNs and have identified challenges associated with those efforts.

To determine what governmentwide initiatives have been undertaken to assist agencies in eliminating their unnecessary use of SSNs, we examined key governmentwide guidance documents, including reports issued by the Identity Theft Task Force and identified roles and responsibilities assigned to the Office of Management and Budget (OMB), the Office of Personnel Management (OPM), and the Social Security Administration (SSA). We also reviewed federal laws, including the Privacy Act,¹ the E-Government Act,² and Federal Information Security Modernization Act of 2014³ to clarify roles and responsibilities. To identify the results of governmentwide efforts, we analyzed reports and guidance on protecting SSNs issued by OMB, OPM, and SSA, and interviewed agency officials knowledgeable about the reduction efforts regarding their activities.

To determine the extent to which agencies developed and executed plans to eliminate the unnecessary use and display of SSNs, we analyzed documents from the 24 agencies covered by the Chief Financial Officers (CFO) Act which described the progress of efforts in this area. For example, we reviewed agency implementation plans and updates submitted as part of their Federal Information Security Modernization Act reports for fiscal years 2007 and 2008 (the first two years that such reports addressed SSN reduction efforts) as well as for 2013, 2014 and 2015 (the three most recent reports available at the time of our review). We compared agency plans with key elements of effective performance plans, as defined in federal guidance and the Government Performance and Results Act Modernization Act of 2010. To identify challenges that agencies experienced in implementing these efforts we interviewed relevant officials at each of the 24 agencies.

¹Pub. L. No. 93-579 (Dec. 31, 1974); 5 U.S.C. § 552a.

²Pub. L. No. 107-347 (Dec. 17, 2002); 44 U.S.C. § 101.

³The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014; 44 U.S.C. § 3551) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

We obtained and analyzed additional information about SSN reduction policies and activities from a selection of the 24 agencies included in this review. To select these agencies, we identified major agencies in the military, international, or security/national security area as well as agencies that deliver benefits to the general public. Within these groups, we selected the two agencies with the largest number of systems and programs that use SSNs. We also selected the Internal Revenue Service (IRS) because it collects a large number of taxpayer SSNs and OPM because it collects SSNs from all federal workers. This resulted in the selection of six of the 24 agencies or components thereof: the Centers for Medicare & Medicaid Services (CMS), a component of the Department of Health and Human Services (HHS); the United States Department of Agriculture (USDA); Army, a component of the Department of Defense (DOD); the Department of Veterans Affairs (VA); the IRS, a component of the Department of the Treasury; and OPM.

To obtain additional information on agency SSN use and efforts to reduce the unnecessary collection and use of SSNs, we administered a questionnaire to the 24 CFO Act agencies. After we drafted the questionnaire, we consulted with GAO survey methodologists to ensure the wording of our questions was objective. We also conducted pretests to ensure that (1) the questions were clear and unambiguous, (2) terminology was used correctly, (3) the questionnaire did not place an undue burden on agency officials, (4) the information could feasibly be obtained, and (5) the questionnaire was comprehensive and unbiased.

We chose to pretest the questionnaire with the Chief Privacy Officer at the Department of Energy and with GAO's Record's Officer because of their knowledge of SSN use and protection issues. We conducted the pretests in person and made changes to the content and format of the questionnaire after the pretests, based on the feedback we received. The finalized questionnaire used for this study is reprinted in appendix II.

We sent the questionnaire to all 24 CFO Act agencies by e-mail in an attached PDF form that respondents could return electronically after marking checkboxes or entering responses into open answer boxes. Alternatively, respondents could return the questionnaire by mail after printing the form and completing it by hand.

We sent the questionnaire with an e-mail on July 25, 2016. Two weeks later, we sent a reminder e-mail to each agency that had not responded. We e-mailed or telephoned all respondents who had not returned the

questionnaire after 3 weeks and reminded them to participate. All questionnaires were returned by August 22, 2016.

Because this was not a sample questionnaire, it has no sampling errors. However, the practical difficulties of conducting any questionnaire may introduce errors, commonly referred to as nonsampling errors. For example, difficulties in interpreting a particular question, sources of information available to respondents, or the types of people who do not respond can introduce unwanted variability into the results. We took steps in developing the questionnaire, collecting the data, and analyzing them to minimize such nonsampling error. For example, survey specialists designed the questionnaire in collaboration with GAO staff who had subject matter expertise.

Lastly, to identify specific examples of agency actions to reduce the collection, use, and display of SSNs, we obtained additional information from the six agencies or components that we selected for further review. We obtained and analyzed additional documentation from these agencies and held additional discussions with agency officials.

We conducted this performance audit from April 2016 to July 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Questionnaire Content

To obtain more detailed information on agency SSN use and efforts to reduce the unnecessary collection and use of SSNs, we administered a questionnaire to the 24 agencies that we selected for review. We sent the questionnaire on July 25, 2016 and received all responses by August 22, 2016. In the questionnaire, we asked the following questions:

1. Does your agency and/or contractors collect and use SSNs in any systems and programs?
 - Yes (Continue to Question 2)
 - No (STOP. Please return survey to GAO)
2. How many of your agency's and contractors' systems and programs collect and use SSNs?
Number of Systems and Programs: # _____
3. For which of the following reasons do your systems and programs collect and use SSNs? (Check all that apply)
 - A. Federal Employment (hiring, pay, benefits)
 - B. Government Benefits/Services (including, but not limited to: debt collection, entitlement programs or benefits, grant programs, healthcare, loans, and other services)
 - C. Criminal Law Enforcement
 - D. Statistical and other Research Purposes
 - E. Tax Purposes
 - F. Other (please describe)
4. Does your agency and/or contractors collect and use SSNs from the members of the public, contractors, or agency employees? (Check all that apply)
 - Members of the Public
 - Agency Employees/Contractors
5. The Office of Management and Budget (OMB) Memorandum M-07-16 required agencies to develop a plan to reduce the unnecessary collection and use of SSNs. For this purpose, did your agency define what would constitute an unnecessary collection and use of SSNs?
 - Yes. Please add your agency's definition of unnecessary here:
 - No.
6. In response to OMB M-07-16, did your agency develop a baseline inventory of agency and contractor systems and programs² that

collected SSNs as part of your initial plan/efforts to reduce the unnecessary collection and use of SSNs?

- Yes.
- No. If no, please explain why.

7. Does your agency have a current and complete inventory of agency and contractor systems and programs that collect and use SSNs?

- Yes. If yes, please provide the inventory to GAO in an EXCEL file format. Please include the name of each system and program and the approximate number of records in each, as of June 30, 2016.
- No. If no, please explain why.

8. Since the issuance of OMB M-07-16, has your agency conducted or participated in any: committees, task forces, inter-agency committees, external groups or associations, or other governance groups whose purpose included the reduction of unnecessary collection and use of SSNs in governmental systems and programs?

- Yes – Please answer question 9
- No – Please continue to question 10
- Don't know – Please continue to question 10

9. Please provide the following information regarding your participation in EACH group.

Group 1: _____

- Internal to department/agency
- Governmentwide
- External Group (private sector)

a. When was the group formed? (MM/YYYY) _____

b. Is the group still in operation?

- Yes
- No. If No, when did the group stop operating? (MM/YYYY)

c. What is your level of participation in this group?

- Contributing Member
- Advisory Role
- Leadership Role (chair, co-chair)

d. Briefly describe the purpose and major goals or initiatives of this group: _____

10. Since the issuance of OMB M-07-16, please describe the challenges, if any, your agency has faced in reducing the unnecessary collection and use of SSNs.
11. Does your agency have any suggestions or additional information that could be helpful to the continued government efforts to reduce of unnecessary collection and use of SSNs?

Appendix III: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

June 19, 2017

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review the draft report, "SOCIAL SECURITY NUMBERS: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display" (GAO-17-555). Please see our enclosed comments. We also provided technical comments at the staff level.

If you have any questions, please contact Gary S. Hatcher, Senior Advisor for the Audit Liaison Staff, at (410) 965-0680.

Sincerely,

A handwritten signature in cursive script that reads "Stephanie Hall".

Stephanie Hall
Acting Deputy Chief of Staff

Attachment

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "SOCIAL SECURITY NUMBERS: OMB ACTIONS NEEDED TO STRENGTHEN FEDERAL EFFORTS TO LIMIT IDENTITY THEFT RISKS BY REDUCING COLLECTION, USE, AND DISPLAY" (GAO-17-553)

While we are not responsible for implementing the recommendations, below are our general comments. We also provided technical comments at the staff level.

GENERAL COMMENTS

It is important that the report highlight the unique role of the Social Security number (SSN) for Social Security. Upon its enactment in 1935, the *Social Security Act* (the Act) did not mandate the use of SSNs. However, the Act did authorize the creation of a record-keeping system. In 1936, a Department of Treasury regulation required employees covered by the new program apply for an account number. Accordingly, we designed the number and card to allow employers to uniquely identify, and accurately report, an individual's earnings covered under the new Social Security program.

Today, over 80 years since the program's inception, we have issued approximately 500 million unique numbers to eligible individuals. The SSN is essential to how we maintain records for our programs. Without it, we could not carry out our mission. We use the number to administer the Old-Age, Survivors, and Disability Insurance program, "Social Security," including retirement, survivors, and disability insurance. We also use the number to administer the Supplemental Security Income (SSI) program that provides monthly payments to people with limited income and resources who are aged, blind, or disabled. As noted above, we created the number to track worker earnings and eligibility for benefits. We are committed to maintaining the integrity of the SSN. Much of our use of the SSN is required by statute, and the number, is a necessary identifier throughout our core business processes.

We support government-wide efforts to reduce the use of the SSN. As the agency responsible for assigning SSNs, we take great care to protect the integrity of the SSN from misuse. Thus, we have taken steps, where possible, to discontinue the use of the SSN in our two largest annual notice workloads and in many internal administrative processes. We remain committed to removing the SSN from our remaining notices as we modify existing notices or develop new ones.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, John de Ferrari (Assistant Director), Andrew Beggs, Marisol Cruz, Quintin Dorsey, David Plocher, Priscilla Smith, and Shaunyce Wallace made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [LinkedIn](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov and read [The Watchblog](#).

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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



Please Print on Recycled Paper.