# PROTECTING AMERICANS' IDENTITIES: EXAMINING EFFORTS TO LIMIT THE USE OF SOCIAL SECURITY NUMBERS

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

AND THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MAY 23, 2017

**Serial No. 115–SS02**

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PUBLISHING OFFICE

33–427 WASHINGTON : 2019

## COMMITTEE ON WAYS AND MEANS

KEVIN BRADY, Texas, *Chairman*

SAM JOHNSON, Texas
DEVIN NUNES, California
PATRICK J. TIBERI, Ohio
DAVID G. REICHERT, Washington
PETER J. ROSKAM, Illinois
VERN BUCHANAN, Florida
ADRIAN SMITH, Nebraska
LYNN JENKINS, Kansas
ERIK PAULSEN, Minnesota
KENNY MARCHANT, Texas
DIANE BLACK, Tennessee
TOM REED, New York
MIKE KELLY, Pennsylvania
JIM RENACCI, Ohio
PAT MEEHAN, Pennsylvania
KRISTI NOEM, South Dakota
GEORGE HOLDING, North Carolina
JASON SMITH, Missouri
TOM RICE, South Carolina
DAVID SCHWEIKERT, Arizona
JACKIE WALORSKI, Indiana
CARLOS CURBELO, Florida
MIKE BISHOP, Michigan

RICHARD E. NEAL, Massachusetts
SANDER M. LEVIN, Michigan
JOHN LEWIS, Georgia
LLOYD DOGGETT, Texas
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
EARL BLUMENAUER, Oregon
RON KIND, Wisconsin
BILL PASCRELL, JR. New Jersey
JOSEPH CROWLEY, New York
DANNY DAVIS, Illinois
LINDA SÁNCHEZ, California
BRIAN HIGGINS, New York
TERRI SEWELL, Alabama
SUZAN DELBENE, Washington
JUDY CHU, California

DAVID STEWART, *Staff Director*
Brandon Casey, *Minority Chief Counsel*

---

## SUBCOMMITTEE ON SOCIAL SECURITY

SAM JOHNSON, Texas, *Chairman*

TOM RICE, South Carolina
DAVID SCHWEIKERT, Arizona
VERN BUCHANAN, Florida
MIKE KELLY, Pennsylvania
JIM RENACCI, Ohio
JASON SMITH, Missouri

JOHN B. LARSON, Connecticut
BILL PASCRELL, JR., New Jersey
JOSEPH CROWLEY, New York
LINDA SÁNCHEZ, California

## COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN DUNCAN, Tennessee
DARRELL ISSA, California
JIM JORDAN, Ohio
MARK SANFORD, South Carolina
JUSTIN AMASH, Michigan
PAUL GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
DENNIS ROSS, Florida
B. MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY HICE, Georgia
STEVE RUSSELL, Oklahoma
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY PALMER, Alabama
JAMES COMER, Kentucky
PAUL MITCHELL, Michigan

ELIJAH CUMMINGS, Maryland
CAROLYN MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
ROBIN KELLY, Illinois
BRENDA LAWRENCE, Michigan
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
VAL BUTLER DEMINGS, Florida
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
PETER WELCH, Vermont
MATT CARTWRIGHT, Pennsylvania
MARK DESAULNIER, California
JOHN SARBANES, Maryland

DAVID STEWART, *Staff Director*
Brandon Casey, *Minority Chief Counsel*

---

## SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

PAUL MITCHELL, Michigan
DARRELL ISSA, California
JUSTIN AMASH, Michigan
BLAKE FARENTHOLD, Texas
STEVE RUSSELL, Oklahoma

ROBIN KELLY, Illinois
JAMIE RASKIN, Maryland
STEPHEN LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois

# CONTENTS


Page

Advisory of May 23, 2017 announcing the hearing ..... 2

WITNESSES

Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office ..... 13
Marianna LaCanfora, Acting Deputy Commissioner, Office of Retirement and Disability Policy, Social Security Administration ..... 29
David DeVries, Chief Information Officer, Office of Personnel Management .... 38
Karen Jackson, Deputy Chief Operating Officer, Centers for Medicare and Medicaid Services ..... 43
John Oswalt, Executive Director for Privacy, Office of Information and Technology, Department of Veterans Affairs ..... 55

SUBMISSIONS FOR THE RECORD

American Joint Replacement Registry, letter ..... 105
Electronic Privacy Information Center, statement ..... 107
National Council of Nonprofits, statement ..... 110

QUESTIONS FOR THE RECORD

Hearing Deliverables ..... 80
The Honorable Sam Johnson:
United States Office of Personnel Management ..... 82
Centers for Medicare and Medicaid Services ..... 86
Office of Retirement and Disability Policy ..... 90
Office of Information and Technology ..... 95
United States Government Accountability Office ..... 100

# PROTECTING AMERICANS' IDENTITIES: EXAMINING EFFORTS TO LIMIT THE USE OF SOCIAL SECURITY NUMBERS

---

**TUESDAY, MAY 23, 2017**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
joint with the
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
*Washington, DC.*

The subcommittees met, pursuant to call, at 2:00 p.m., in Room 1100, Longworth House Office Building, the Honorable Tom Rice presiding.

[The advisory announcing the hearing follows:]

# *ADVISORY*

FROM THE COMMITTEE ON WAYS AND MEANS

**SUBCOMMITTEE ON SOCIAL SECURITY**

FROM THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

**SUBCOMMITTEE ON INFORMATION TECHNOLOGY**

FOR IMMEDIATE RELEASE
Wednesday, May 23, 2017
SS–02

CONTACT: (202) 225–1721

## Chairman Johnson and Chairman Hurd Announce Joint Oversight Hearing on Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers

House Ways and Means Social Security Subcommittee Chairman Sam Johnson (R–TX) and House Oversight and Government Reform Information Technology Subcommittee Chairman Will Hurd (R–TX) announced today that the Subcommittees will hold a joint hearing entitled "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers." The hearing will focus on efforts by federal agencies to reduce the use of Social Security numbers, and the challenges these agencies face in doing so. **The hearing will take place on Tuesday, May 23, 2017 in 1100 Longworth House Office Building, beginning at 2:00 PM.**

In view of the limited time to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

**DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:**

**Please Note:** Any person(s) and/or organization(s) wishing to submit written comments for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, *http://waysandmeans.house.gov*, select "Hearings." Select the hearing for which you would like to make a submission, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word document, in compliance with the formatting requirements listed below, **by the close of business on June 6, 2017.** For questions, or if you encounter technical problems, please call (202) 225–3625.

**FORMATTING REQUIREMENTS:**

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

All submissions and supplementary materials must be submitted in a single document via email, provided in Word format and must not exceed a total of 10 pages. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. The name, company, address, telephone, and fax numbers of each witness must be included in the body of the email. Please exclude any personal identifiable information in the attached submission.

Failure to follow the formatting requirements may result in the exclusion of a submission. All submissions for the record are final.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days' notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

**Note***: All Committee advisories and news releases are available at http://www.waysandmeans.house.gov/*

## OPENING STATEMENT OF ACTING CHAIRMAN RICE

Mr. RICE. Good afternoon and welcome to today's hearing on the Federal Government's use of Social Security numbers.

Unfortunately, Chairman Sam Johnson was unable to be here with us today to discuss one of his favorite topics: ending the unnecessary use of Social Security numbers. I know everyone here joins me in wishing Chairman Johnson a speedy recovery.

I would like to welcome Chairman Hurd of the Oversight and Government Reform Committee's IT Subcommittee and all of the IT Subcommittee members for joining us in the Ways and Means Committee hearing room today.

Back in 1936, when Social Security began issuing Social Security numbers, they were only used to track earnings and administer the Social Security Program. Back then, it wasn't much thought about keeping your number a secret, but today, Social Security numbers are the keys to the kingdom for identity thieves. Social Security and identity security experts make a point of telling Americans how important it is to protect their numbers. Social Security numbers are valuable targets for identity theft because of their regular use by both Federal Government and private sector as a unique identifier, especially by the financial industry.

Time and again, we are reminded to protect our Social Security cards in order to avoid identity theft and to be careful with what documents we throw away in the trash. Our Social Security numbers are connected to so many personal aspects of our lives, from our Social Security benefits and finances to our medical histories and our education. But in recent years, privacy concerns have become more and more critical.

When I was in law school back in the dark ages, our grades used to be posted on the wall to keep secret whose grades they were by Social Security number. Of course, they were posted alphabetically. So it wasn't that hard to figure out whose was whose. In fact, one of my very good friends in law school's last name was Ziegler, and he was the smartest guy in the class, and he always made an A and blew the curve. So everybody just gave him a hard time. But

his Social Security number was always the one at the bottom of the list. And until not long ago, I probably could recite to you Mr. Ziegler's Social Security number.

While colleges and universities have since changed their ways, the Federal Government has yet to fully catch up. Just over 10 years ago, under President Bush's leadership, the Office of Management and Budget issued a memorandum for the safeguarding of personally identifiable information, including the Social Security number. The memo called for Federal departments and agencies to reduce or replace the use of Social Security numbers across the Federal Government.

Unfortunately, while some progress has been made in reducing the use of Social Security numbers, 10 years later, there is still much work to be done. This hearing is about making sure that Social Security numbers are only used when necessary and that the Federal Government is doing what it can and what it should to make sure that, when Social Security numbers are used and collected, they are kept safe.

The Office of Personnel Management hack in 2015 is an example of what happens when the Federal Government collects Social Security numbers but does not keep them safe. And that negligence comes with a cost to both the affected individuals and to the taxpayers. The American people rightly deserve and expect that the Federal Government protect their Social Security numbers and only use them when necessary.

I thank all of our witnesses for being here. I look forward to hearing from you about how your agencies are working to tackle this challenge and what more needs to be done.

I now recognize Mr. Larson for his opening statement.

**OPENING STATEMENT OF HON. JOHN B. LARSON**

Mr. LARSON. Thank you, Mr. Chairman.

We join with you in certainly wishing our dear friend and colleague Sam Johnson a speedy recovery and would like to add how fortunate we are on the Ways and Means Committee to have two iconic American heroes serving on the same committee. When you think about Sam Johnson and his service to this country and all that he endured on behalf of this Nation, nearly beaten to death by the Viet Cong and then you think about John Lewis and all he endured in this country and nearly beaten to death in his own country, so we have these two iconic legends. And I am so proud to serve with Sam and was happy that he asked me to introduce with him the Social Security Must Avert Identity Loss, or H.R. 1513, that required the Social Security Administration to remove Social Security numbers from mailed notices. And Mr. Johnson, as I think everybody on the committee knows, is such an incredible gentleman. We also have taken every opportunity in the subcommittee to renew a request, A, that I hope the committee will travel to Plano, Texas, and that we have an opportunity to, in as much as Mr. Johnson has indicated this is his last term, to have a meeting there in Plano, Texas, that would honor Mr. Johnson and the committee in this particular topic area that he is so vitally concerned about.

I also want to recognize Chairman Hurd, who is with us, and the lead Democrat, Robin Kelly, for being here in our meeting room as well.

Since 2014, hundreds of millions of Americans have lost their personally identified information, including their Social Security numbers, to large-scale cyber attacks. The number was originally created in 1936 for the purpose of running the Nation's new Social Security system. However, its usefulness as a unique governmental identifier has made it near ubiquitous across government and the private sector. To date, the Social Security Administration has not suffered any large-scale data breach, but ongoing vigilance is needed, including adequate support for updating and modernizing the Social Security Administration's IT structure.

All together, the Social Security Administration has been able it to remove the 9-digit SSN from about one-third of the mailings it sends out. Moving forward, they have committed to removing them from the remaining notices wherever they revise a notice, which requires computer upgrades. The severe constraints on Social Security Administration's budget, however, are preventing the agency from removing numbers from all the notices right away. As they estimated, it would cost $14 million to do so immediately rather than piecemeal.

More alarmingly, since 2010, the number of beneficiaries has grown by 13 percent as the baby boomers enter retirement, but Social Security's operating budget has fallen by more than 10 percent in that same period. The Social Security Administration simply cannot serve more and more people with less and less money each year. Social Security Administration is already struggling to serve its beneficiaries at the level they deserve. My constituents are experiencing multiyear wait times on disability appeals and hearings. Their phone calls are going unanswered. They face delays in correcting errors in their benefits and payments.

To make matters worse, the President's fiscal year 2018 budget released today also attacks Social Security benefits for those with disabilities as much as $70 billion over 10 years.

Mr. Chairman, I would like to submit for the record the 13 times that Donald Trump promised not to cut Social Security, Medicare, and Medicaid.

[The following was received from Mr. Larson:]

# 13 Times Donald Trump Promised Not To Cut Social Security, Medicare or Medicaid

1. July 25, 2011: "The Answer to both Social Security and Medicare is a robust growing economy—not cuts on the elderly."


[https://twitter.com/realDonaldTrump/status/95563593222860800]

2. September 7, 2011: "A robust growing economy is how to fix Social Security and Medicare—not cuts on Seniors."


[https://twitter.com/realDonaldTrump/status/111464722683002880]

3. December 5, 2011: "Now I know there are some Republicans who would be just fine with allowing [Social Security and Medicare] to wither and die on the vine. The way they see it, Social Security and Medicare are wasteful 'entitlement programs.' But people who think this way need to rethink their position. It's not unreasonable for people who paid into a system for decades to expect to get their money's worth—that's not an 'entitlement,' that's honoring a deal. We as a society must also make an ironclad commitment to providing a safety net for those who can't make one for themselves." [http://www.ontheissues.org/Archive/Get_Tough_Social_Security.htm]

4. **March 15, 2013:** "As Republicans, if you think you are going to change very substantially for the worse Medicare, Medicaid and Social Security in any substantial way, and at the same time you think you are going to win elections, it just really is not going to happen."
[https://youtu.be/cXcJ_SKHQxM]

5. **January 24, 2015:** "I'm not a cutter. I'll probably be the only Republican that doesn't want to cut Social Security."
[https://www.bloomberg.com/politics/videos/2015-01-24/how-the-donald-will-save-social-security]

6. **April 18, 2015:** "Every Republican wants to do a big number on Social Security, they want to do it on Medicare, they want to do it on Medicaid. And we can't do that. And it's not fair to the people that have been paying in for years and now all of the sudden they want to be cut."
[https://youtu.be/Q9vY_MaZ8Tw]

7. **May 7, 2015:** "I was the first & only potential GOP candidate to state there will be no cuts to Social Security, Medicare & Medicaid."


[https://twitter.com/realDonaldTrump/status/596338364187602944]

8. May 7, 2015: "Huckabee is a nice guy but will never be able to bring in the funds so as not to cut Social Security, Medicare & Medicaid. I will."


[https://twitter.com/realDonaldTrump/status/596338822373343233]

9. May 21, 2015: "I am going to save Social Security without any cuts. I know where to get the money from. Nobody else does."


[https://twitter.com/realDonaldTrump/status/601544572498509824]

10. June 16, 2015: "[I will] save Medicare, Medicaid and Social Security without cuts. Have to do it… People have been paying in for years, and now many of these candidates want to cut it."
[https://youtu.be/XznUWXg6wOk]

11. November 3, 2015: "I'll save Social Security. I'll save Medicare. Ben Carson wants to get rid of Medicare. You can't get rid of Medicare. You know, Medicare's a program that works. There's fraud, there's abuse, there's waste, but you don't get rid of Medicare. You **can't do that. People love Medicare. And it's unfair to them… I'm not going to cut it."**
[https://youtu.be/Fw7EJ-GntTM]

**12.** **March 10, 2016:** "I will do everything within my power not to touch Social Security, to leave it the way it is… It's my absolute intention to leave Social Security the way it is. Not increase the age and to leave it as is."
[https://youtu.be/ihFHxKlc1uI]

**13.** **March 29, 2016:** "You know, Paul [Ryan] wants to knock out Social Security, knock it down, way down. He wants to knock Medicare way down. And, frankly—well, two things. Number one, you're going to lose the election if you're going to do that … I'm not going to cut it, and I'm not going to raise ages, and I'm not going to do all of the things that they want to do. But they want to really cut it, and they want to cut it very substantially, the Republicans, and I'm not going to do that."
[https://youtu.be/v3Ur7llwxek]

Mr. LARSON. President Trump has promised repeatedly and explicitly throughout the campaign not to cut Social Security or Medicare. This broken promise should be especially alarming to millions of people who voted for the President, who spent their working lives paying premiums into the system, believing those benefits would be there for them in retirement or should they become disabled.

The bottom line is this: Social Security is the Nation's insurance program. It is not an entitlement. It is the insurance that individuals have paid for throughout a lifetime. The problems with Social Security at its core—this issue that we're taking up today, especially as it relates to theft is vitally important to protect people's identity. But equally important and the responsibility of this committee is actuarial soundness.

This is the most efficient government-operated program in the history of the Nation. Ask any private sector insurance company if they could have a 99-percent loss ratio. They would die for that. And there's no product on the open market where you could produce old age and survivors benefits, disability, and a pension plan, and survivors benefits. That is the uniqueness of Social Security. That is why it is America's insurance plan that our citizens have paid for. This is not an entitlement, and we'll continue to make that point. I hope later this year, Mr. Chairman—and Mr. Johnson has been very gracious about saying that we'll get an opportunity to have hearings on our bills that will look at expanding and making solvent, well into the next century Social Security for all of its American citizens. It's the Nation's insurance program.

Mr. RICE. Thank you.

I now recognize Mr. Hurd for his opening statement.

**OPENING STATEMENT OF CHAIRMAN HURD**

Mr. HURD. Thank you, Mr. Chairman.

In the 2 years plus that I've been in Congress, I've learned one thing, and that is that Americans expect the Federal Government to protect their personal information. Sadly, as evidenced by the devastating data breach at OPM, which affected more than 20 million people, this is simply not the case.

American people deserve better from their government. If stolen, we all know that Social Security numbers can be used to perpetuate identity theft or worse. You never know what a piece of personal information the bad actors need to achieve their goals, whether they are looking to steal money or threaten the national security of our Nation. The Oversight Committee recently held a hearing on the IRS data breach where bad actors hacked in the Department of Education and stole income information from financial aid applications and then used that information to file fraudulent tax returns with the IRS.

All of the agencies appearing before us today collect and retain a wealth of information on individual Americans, particularly Social Security numbers. It is essential that we reduce the unnecessary use of Social Security numbers, both on printed forms and electronically, in transition and at rest. In fact, tomorrow, the House is scheduled to consider Representative Valadao's Social Security Number Fraud Prevention Act of 2017, which was passed

out of committee on a voice vote and prohibits agencies from sending Social Security numbers by mail, unless the head of the agency deems it absolutely necessary.

The Social Security Administration has 174 million wage earners and records on pretty much everybody living and dead. It is a treasure trove of information that must be protected.

The Veterans Administration has health records on over 8 million veterans and their families. I can imagine a few other records as intimate as an individual's health record. The VA currently uses Social Security numbers as a patient identifier.

Protecting these numbers is critically important for all Americans, but given that Social Security numbers are frequently exchanged with our most at-risk members of society, such as our seniors, disabled, and veterans, we must take utmost precaution to prevent the unnecessary risk of exposure for these populations.

One of recommendations that came out of the committee's investigation of the OPM breach was that agencies reduced their use of Social Security numbers in order to mitigate the risk of identity theft. As agencies undertake this transition, it is essential that they rethink how they use, collect, and store Social Security numbers and indeed all pieces of personal information they collect.

I am proud to be here today with my colleagues from the Oversight Committee as well as my colleagues from the Ways and Means Committee in this important joint hearing to examine what's working and what we can do better. Today, I hope to learn more about what efforts the Federal Government is taking to reduce its collection, use, and storage of Social Security numbers. And thank you for being here today, and I look forward to hearing from all of our witnesses.

Mr. RICE. Thank you.

I now recognize Ms. Kelly for her opening statement.

**OPENING STATEMENT OF HON. ROBIN KELLY**

Ms. KELLY. Thank you, Chairmen Rice and Hurd and Ranking Member Larson, for holding this important hearing.

Originally created to track the earnings of individuals and determine eligibility for Social Security benefits, the Social Security number has become the principal method used to verify an individual's identity. But the proliferation of their use poses serious challenges to data security and identity theft protection.

In 2007, when the Office of Management and Budget recognized that reducing the use of Social Security numbers at agencies could reduce the risk of identity theft, 10 years ago this week, OMB issued a memorandum directing agencies to reduce their use of Social Security numbers by examining where their collection was unnecessary and creating plans to end such collection within 18 months. Now, on the 10-year anniversary of the guidance, we have the opportunity to examine the challenges that have stymied agencies' efforts while learning from those agencies who have had success in their initiative.

The Social Security Administration no longer prints Social Security numbers on statements, cost-of-living notices, or benefits checks. The Centers for Medicare and Medicaid Services is in the middle of efforts to remove the numbers from all Medicare cards

by April 2019. Likewise, the Department of Veterans Affairs has ceased printing Social Security numbers on prescription bottles, certain forms, and correspondence, and is working to find an alternate means of identification that will maintain patient safety while reducing the visibility of Social Security numbers on patient wristbands.

These concrete steps represent real progress, and I commend the agencies on their work so far. But barriers still exist to full implementation of the OMB's guidance. One of those barriers is the lack of a strong coordinative approach from OMB itself. GAO found that the 2007 memorandum did not define unnecessary use, nor did it outline requirements such as timeline or performance goals. As a result, many agencies were vague and subject to varied interpretation over the years. Additionally, OMB did not require agencies to update their inventories of Social Security number collection points, making it difficult to determine whether agencies were actually reducing collection and use. OMB must provide clear direction to agencies and strengthen its monitoring of compliance.

In addition to poor coordination by OMB, Federal efforts to reduce Social Security numbers used have faced other challenges. Agencies are statutorily and legally required to collect Social Security numbers for identity verification in a number of programs. And Social Security numbers remain the standard for identity verification across government programs. OPM briefly took steps to address this issue by working to create an alternate identifier in 2008 and again in 2015. However, a lack of approved funding prevented these efforts from going forward. Until Congress refines the requirements mandating Social Security number collection and an alternate governmentwide identifier is created, significant reductions in Social Security numbers use seems unlikely.

Outdated legacy IT systems also cause agencies to struggle to obtain their reduction goals. Agencies do not have the funds to replace these systems and start anew. This subcommittee has spoken at great length about the need to update the Federal Government's IT infrastructure. And we must put our money where our mouth is. I'm concerned that across-the-board budget and personnel cuts proposed by the Trump administration will take us in the opposite direction and make it harder to accomplish our Social Security number reduction goals.

I hope my colleagues will keep this and the need to protect Americans from identity theft in mind as we discuss fiscal year 2018 budget proposals. I look forward to hearing from our witnesses today, and I yield back the balance of my time. Thank you.

Mr. RICE. Thank you. As is customary, any member is welcome to submit a statement for the hearing record. Before we move on to our testimony today, I want to remind our witnesses to please limit their oral statements to 5 minutes. However, without objection, all of the written testimony will be made part of the hearing record.

We have 5 witnesses today. Seated at the table are: Gregory Wilshusen, Director of Information Security Issues, Government Accountability Office; Marianna LaCanfora, Acting Deputy Commissioner, Office of Retirement and Disability Policy, Social Security Administration; David DeVries, Chief Information Officer, Of-

fice of Personnel Management; and Karen Jackson, Deputy Chief Operating Officer, Centers for Medicare and Medicaid Services; and, finally, John Oswalt, Executive Director for Privacy, Office of Information and Technology, Department of Veterans Affairs. Welcome to you all and thank you for being here.

Pursuant to the committee on Oversight and Government Reform rules, all witnesses will be sworn in before they testify. Please rise and raise your right hand.

[Witnesses sworn.]

Mr. RICE. Please be seated.

Mr. Wilshusen, welcome and thanks for being here. Please proceed. If I butchered your name, I'm sorry.

**STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. WILSHUSEN. No, you did perfect. Thank you, Chairmen Rice and Hurd, Ranking Members Larson and Kelly, and Members of the Subcommittee. Thank you for inviting me today to testify at today's hearing on executive branch efforts to reduce the unnecessary use of Social Security numbers.

My statement is based on our draft report on Federal efforts to reduce the collection, use, and display of these numbers. We have provided a draft report to 25 agencies for comment. We anticipate issuing the final report to you later this summer after we receive agency comments.

Before I begin, if I may, I'd like to recognize several members of my team who were instrumental in developing my statement or performing the work underpinning it. With me is John de Farrari and Marisol Cruz, who led this work, and Quintin Dorsey. In addition, Andrew Beggs, Shaunyce Wallace, Dave Plocher, Priscilla Smith, and Scott Pettis made significant contributions.

Beginning in 2007, OPM, OMB, and the Social Security Administration undertook several actions aimed at reducing or eliminating the unnecessary collection, use, and display of Social Security numbers on a governmentwide basis. However, these actions have had limited success. OPM issued guidance to agencies and acted to eliminate or mask Social Security numbers on personnel forms used throughout the Federal Government. It also promulgated a draft regulation to limit Federal collection, use, and display of Social Security numbers, but withdrew the proposed rule because no alternate Federal employee identifier was available that would provide the same utility.

In 2007, OMB required agencies to establish plans for eliminating the unnecessary collection and use of Social Security numbers. OMB also began requiring agency reporting on reduction efforts as part of its annual FISMA reporting process. In 2007, the Social Security Administration developed an online clearinghouse on agency's best practices for minimizing the use and display of Social Security numbers. However, this clearinghouse is no longer available.

At the individual agency level, each of the 24 CFO Act agencies report taking a variety of steps to reduce the collection, use, and display of Social Security numbers. These steps included devel-

oping and using alternate identifiers; masking, truncating, or blocking the display of these numbers on printed forms, correspondence, and computer screens; and filtering email to prevent transmittal of unencrypted numbers.

However, agency officials noted that Social Security numbers cannot be completely eliminated from Federal IT systems and records in part because no other identifier offers the same degree of universal awareness and applicability. They identified three other challenges. First, several statutes and regulations require collection and use of Social Security numbers. Second, interactions with other Federal agencies and external entities require the use of the number. And a third challenge pertained to technological hurdles that can slow replacement of the numbers in information systems.

Reduction efforts in the executive branch 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 or performance indicators, calling into question the plans' utility.

In addition, OMB has not required agencies to maintain up-to-date inventories of Social Security number collections and has not established criteria for determining when the number's use or display is unnecessary, leading to inconsistent determinations and definitions across the agencies.

OMB has also not ensured that all agencies have submitted up-to-date progress reports and has not established performance metrics to measure and monitor agencies' efforts.

Accordingly, in our draft report, we are making five recommendations to OMB to address these shortcomings. Until OMB and agencies adopt better and more consistent practices, their reduction efforts will likely remain limited and difficult to measure. Moreover, the risk of Social Security numbers being exposed and used to commit identity theft will remain greater than it need be.

Chairman Rice, Chairman Hurd, Ranking Members Larson and Kelly, this concludes my statement. I'd be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

Testimony before the Subcommittee on Social Security, Committee on Ways and Means, and the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Tuesday, May 23, 2017

# SOCIAL SECURITY NUMBERS

# OMB and Federal Efforts to Reduce Collection, Use, and Display

Statement of Gregory C. Wilshusen, Director,
Information Security Issues

GAO-17-655T

GAO Highlights

Highlights of GAO-17-655T, a testimony before the Subcommittee on Social Security, Committee on Ways and Means, and the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives

## Why GAO Did This Study

SSNs are key pieces of identifying information that potentially may be used to perpetrate identity theft. Thieves find SSNs valuable because they are the identifying link that can connect an individual's information across many agencies, systems, and databases.

This statement summarize GAO's draft report that: (1) describes what governmentwide initiatives have been undertaken to assist agencies in eliminating their unnecessary use of SSNs and (2) assesses 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. For the draft report on which this testimony is based, GAO analyzed documentation, administered a questionnaire, and interviewed officials from the 24 CFO Act agencies that led or participated in SSN elimination efforts.

## What GAO Recommends

GAO's draft report contains five recommendations to OMB to require agencies to submit 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 of SSNs; ensure agencies update their progress in reducing the collection, use, and display of the numbers in annual reports; and monitor agency progress based on clearly defined performance measures.

View GAO-17-655T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

May 23, 2017

# SOCIAL SECURITY NUMBERS

## OMB and Federal Efforts to Reduce Collection, Use, and Display

## What GAO Found

In its draft report, GAO noted that several 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 new regulation requiring the use of an alternate federal employee identifier but withdrew its proposed regulation because no such identifier was available. OMB required agencies to develop SSN reduction plans and continues to require annual reporting on SSN reduction efforts. SSA developed an online clearinghouse of best practices associated with the reduction of SSN use; however, the clearinghouse is no longer available online.

All 24 agencies covered by the Chief Financial Officers (CFO) Act developed SSN reduction plans and reported taking actions to curtail the use and display of the numbers. Nevertheless, in their responses to GAO's questionnaire and follow-up discussions, the agencies cited impediments to further reductions, including (1) statutes and regulations mandating the collection of SSNs, (2) the 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 limited efforts to reduce SSN use. Lacking direction from OMB, many agencies' 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. In addition, OMB has not ensured that agencies update their annual progress nor has it established performance metrics to monitor agency efforts to reduce SSN use. Until OMB adopts more effective practices for guiding agency SSN reduction efforts, overall governmentwide reduction 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.

Chairmen Johnson and Hurd, Ranking Members Larson and Kelly, and Members of the Subcommittees:

Thank you for inviting me to testify at today's hearing on executive branch efforts to reduce the unnecessary use of Social Security numbers (SSN). As you know, SSNs are key pieces of personally identifiable information (PII) that potentially may be used to perpetrate identity theft. 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.

As requested, this statement summarizes key preliminary findings based on our draft report that (1) describes governmentwide initiatives that have been undertaken to assist agencies in eliminating their unnecessary use of SSNs, and (2) assesses 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. The draft report is currently out for comment. We anticipate issuing the report later this summer.

In conducting our work for that report, we addressed the first objective by analyzing 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 Office of Personnel Management (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.

To address the 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 to key elements of effective performance plans, as defined in

[1]The 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.

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 the agencies' efforts and the associated challenges.

All the work on which this statement is based was conducted or is being conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits 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 1935,[3] the newly-formed 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. Originally, the SSN was not intended to serve as a personal identifier but, due to its universality and uniqueness, government agencies and private sector entities now use it as a convenient means of identifying people. The number uniquely links identities across a very broad array of public and private sector information systems. As of September 2016, SSA had issued approximately 496 million unique SSNs to eligible individuals.

In 2006, the President issued an Executive Order establishing the Identity Theft Task Force to strengthen efforts to protect against identity theft.[4] Because the unauthorized use of SSNs was recognized as a key element of identity theft, the task force assessed the actions the government could take to reduce the exposure of SSNs to potential compromise. In April

[2]See Pub L. No. 103-62, 107 Stat. 285 (1993) (GPRA), as amended by Pub. L. No. 111-352, 124 Stat. 3866 (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.

[3]Pub. L. No. 74–271, Aug. 14, 1935.

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

2007, the task force issued a strategic plan, which advocated a unified federal approach, or standard, for using and displaying SSNs.[5] The plan proposed that OPM, OMB, and SSA play key roles in restricting the unnecessary use of the numbers, 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.

## 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, in our draft report, we determined that these actions have had limited success.

### OPM Issued Guidance and a Proposed Rule That was Subsequently Cancelled

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.[6] The guidance reminded agencies of existing federal regulations that restricted the collection and use of SSNs and also specified additional measures.

In addition to issuing this guidance, in January 2008, OPM 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.[7] However, in January

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

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

[7]73 Fed. Reg. 3410 (Jan. 18, 2008).

2010, after reviewing comments it had received,[8] 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.[9]

In 2015, OPM briefly began exploring the concept of developing and using multiple alternate identifiers for different programs and agencies. As envisioned, 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, officials from OPM's Office of the Chief Information Officer stated that work on the initiative was suspended in 2016 due to a lack of funding.

## OMB Established Reporting Requirements for Agency SSN Reduction Efforts

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 the number was superfluous.[10] 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.

Since issuing its May 2007 memorandum requiring the development of SSN reduction plans, OMB has instructed agencies to submit updates to their plans and documentation of their progress in eliminating unnecessary uses of SSNs as part of their annual reports originally required by the Federal Information Security Management Act of 2002 and now required by the Federal Information Security Modernization Act of 2014 (FISMA).[11]

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

[9]75 Fed. Reg. 4308 (Jan. 27, 2010).

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

[11]The 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).

## 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 had minimized 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 established a clearinghouse on an electronic bulletin board website to showcase best practices and provided agency contacts for specific programs and initiatives. However, according to officials in SSA's Office of the Deputy Commissioner, 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

Based on their responses to our questionnaire on SSN reduction efforts in our draft report, all of the 24 CFO Act agencies reported taking a variety of steps to reduce such collection, display, and use. However, officials involved in the reduction efforts at these 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. Even when reductions are possible, challenges in implementing them can be significant. In our draft report, three key challenges were frequently cited by these officials:

- *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. 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.

- *Interactions with other federal and external entities require use of the SSN.* In their questionnaire responses and follow-up correspondence with us, officials from 16 agencies noted that the necessity to communicate with other agencies and external entities limited their reduction efforts. Federal agencies 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 in order to exchange information about individuals with other entities, both within and outside the federal government. The SSN is typically the only identifier that government agencies and external partners have in common that they can use to match their records.
- *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.

Our preliminary results indicate that SSN reduction efforts in the federal government also have been limited by more readily addressable shortcomings. Lacking direction from OMB, many agencies' reduction plans did not include key elements, such as time frames 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 all agencies have submitted up-to-date status reports on their SSN reduction efforts and has not established performance measures to monitor progress on those 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.[12] OMB did not set requirements for agencies on

[12]Office 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).

creating effective plans to eliminate the unnecessary collection and use of SSNs. However, other federal laws and guidance[13] have established key elements that performance plans generally should contain, including:

- *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.

Our preliminary results show that the majority of plans that the 24 CFO Act agencies originally submitted to OMB in response to its guidance lacked key elements of effective performance plans. For example, only two agencies (the Departments of Commerce and Education) developed plans that addressed all four key elements. Four agencies' plans did not fully address any of the key elements, 9 plans addressed one or two of the elements, and the remaining 9 plans addressed three of the elements.

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, the officials were not aware that they should address these elements. Yet, without complete performance plans containing clearly defined performance goals and indicators, measurable activities, timelines for completion, and roles and responsibilities, it is difficult to determine what overall progress agencies have achieved in reducing the unnecessary collection and use of SSNs

[13]The Government Performance and Results Act Modernization Act of 2010, established criteria for effective performance plans, including specific measures to assess performance. See Pub L. No. 103-62, 107 Stat. 285 (1993) (GPRA), as amended by Pub. L. No. 111-352, 124 Stat. 3866 (2011) (GPRAMA). In addition, GAO guidance on developing performance plans identifies additional elements of effective plans, as does OMB's guidance on budget preparation. See GAO, *Managing for Results: Critical Issues for Improving Federal Agencies' Strategic Plans*, GAO/GGD-97-180 (Washington, D.C. Sep. 16, 1997) and OMB, *Circular No. A-11, Preparation, Submission, and Execution of the Budget*, Section 6 (Washington, D.C.: Jul. 1, 2016).

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 the inventory 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. *Standards for Internal Control in the Federal Government* state that 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 we reviewed, 22 reported that, at the time that they developed their original SSN reduction plans in fiscal years 2007 and 2008, they compiled an inventory of systems and programs that collected SSNs. However, as of August 2016, 6 of the 24 agencies did not have up-to-date inventories: 2 agencies that had no inventories initially and 4 agencies that originally developed inventories but subsequently reported that those inventories were no longer up-to-date.

These agencies did not have up-to-date inventories, in part, because OMB M-07-16 did not require agencies to develop an inventory or to update the inventory periodically to measure the reduction of SSN collection and use. However, OMB has issued separate guidance that requires agencies to maintain an inventory of systems that "create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII."[14] This guidance states that agencies are to maintain such an inventory, in part, to allow them to reduce PII to the minimum necessary. Without enhancing these 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.

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

### Agency definitions of "unnecessary" collection and use have been inconsistent

Achieving consistent results from any management initiative can be difficult when the objectives are not clearly defined. *Standards for Internal Control in the Federal Government* state 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.[15]

In our draft report, we noted that of the 24 CFO Act agencies, 4 reported that they had no definition of "unnecessary collection and use" of SSNs. Of the other 20 agencies, 8 reported that their definitions were not documented. Officials from many agencies stated that the process of reviewing and identifying unnecessary uses of SSNs was an informal process that relied on subjective judgments.

These agencies did not have consistent definitions of the "unnecessary collection and use" of SSNs, in part, because 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.

Given the varying approaches that agencies have taken to determine whether proposed or actual collections and uses of SSNs are necessary, it is doubtful that the goal of eliminating unnecessary collection and use of SSNs is being implemented consistently across the federal government. Until guidance for agencies is developed in the form of criteria for making decisions about what types of collections and uses of SSNs are unnecessary, agency efforts to reduce the unnecessary use of SSNs likely will continue to vary, and, as a result, the risk of unnecessarily exposing SSNs to identity theft may not be thoroughly mitigated.

### Agencies have not always submitted up-to-date status reports, and OMB has not set performance measures to monitor agency efforts

In its *Fiscal Year 2008 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*, OMB recognized that agencies' SSN reduction plans needed to be monitored. OMB reported that the reduction plans that agencies submitted for fiscal year

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

2008 displayed varying levels of detail and comprehensiveness and stated that agency reduction efforts would require ongoing oversight.[16] Subsequently, OMB required agencies to report on the progress of their SSN reduction efforts through their annual FISMA reports.[17]

However, preliminary findings in our draft report show that annual updates submitted by the 24 CFO Act agencies as part of their FISMA reports from fiscal year 2013 through fiscal year 2015 did not always include updated information about specific agency efforts and results achieved, making it difficult to determine the status of activities that had been undertaken. Further, the annual updates did not include performance metrics. OMB did not establish specific performance metrics to monitor implementation of planned reduction efforts. Its guidance asked agencies to submit their most current documentation on their plans and progress, but it did not establish performance metrics or ask for updates on achieving the performances metrics or targets that agencies had defined in their plans.

Although in 2016, OMB began requesting additional status information related to agency SSN reduction programs, it did not establish metrics for measuring agency progress in reducing the unnecessary collection and use of SSNs. Without performance metrics, 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 corrective actions are needed.

In conclusion, based on preliminary information from our study of federal SSN reduction efforts, the initiatives that the 24 CFO Act agencies have undertaken 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. Not all agencies developed effective SSN reduction plans, maintained up-to-date inventories of their SSN collection and use, or applied consistent definitions of "unnecessary" collection, use, and display of SSNs. Further, agencies have not always submitted up-to-date status reports to OMB, and OMB has not established performance measures to monitor agency efforts. Until OMB and agencies adopt better

[16]Office of Management and Budget, *Fiscal Year 2008 Report to Congress on Implementation of the Federal Information Security Management Act of 2002.* (Washington, D.C.: undated).

[17]Office 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).

and more consistent practices for managing their SSN reduction processes, overall governmentwide reduction efforts will likely remain limited and difficult to measure; moreover, the risk of SSNs being exposed and used to commit identity theft will remain greater than it need be.

Accordingly, our draft report contains five recommendations to OMB to improve the consistency and effectiveness of governmentwide efforts to reduce the unnecessary use of SSNs and thereby mitigate the risk of identity theft. Specifically, the report recommends that OMB:

- 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.

Chairmen Johnson and Hurd, Ranking Members Larson and Kelly, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

## Contact and Acknowledgments

If you have any questions regarding this statement, 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 statement. GAO staff who made key contributions to this testimony are John A. de Ferrari (assistant director), Marisol Cruz, Quintin Dorsey, David Plocher, Priscilla Smith, and Shaunyce Wallace.

Mr. RICE. Thank you, sir.

Ms. LaCanfora, welcome and thanks for being here. Please proceed.

**STATEMENT OF MARIANNA LACANFORA, ACTING DEPUTY COMMISSIONER, OFFICE OF RETIREMENT AND DISABILITY POLICY, SOCIAL SECURITY ADMINISTRATION**

Ms. LACANFORA. Acting Chairman Rice, Chairman Hurd, Ranking Member Larson, Ranking Member Kelly, and Members of the Subcommittees, thank you, for inviting me to discuss the history of the Social Security number, how the Social Security Administration uses it to administer its programs, and efforts to reduce the number's use. I am Mariana LaCanfora, Acting Deputy Commissioner for Retirement and Disability Policy.

There's a rich history surrounding the Social Security number. Those responsible for implementing the new Social Security Program understood that crediting earnings to the correct individual would be critical to the program's success. Names alone would not ensure accurate reporting. Accordingly, in 1936, we designed the 9-digit SSN and SSN card to allow employers to accurately report earnings.

Today, over 80 years since the program's inception, we have issued around 500 million unique numbers to eligible individuals. The SSN continues to be essential to how we maintain records. Without it, we could not carry out our mission. However, the SSN and SSN card were never intended, nor do they serve, as identification. We strongly encourage other agencies and the public to minimize their use.

We also provide electronic verifications of SSNs to our Federal and State partners to prevent improper payments. In 2016, we performed over 2 billion automated SSN verifications.

Although we created the SSN, its use has increased dramatically by other entities over time. A 1943 executive order require Federal agencies to use the SSN. Advances in computer technology and data processing in the 1960s further increased the use of the number. Congress also enacted legislation requiring the number for a variety of Federal programs. Use of the SSN grew not just in the Federal Government but throughout State and local governments to banks, credit bureaus, hospitals, educational institutions, and other parts of the private sector.

As use of the SSN has become more pervasive so has the opportunity for misuse. We have taken numerous measures to help protect the integrity of the SSN.

In 2001, we removed the full SSN from two of our largest mailings: the Social Security statement and the Social Security cost-of-living adjustment notice. These notices account for about a third of the roughly 352 million notices that we send out each year.

In 2007, OMB issued a memo requiring agencies to review their use of the SSN and identify unnecessary use of the number. We recognized that although we need the SSN to administer our programs, we could and did refine all of our personnel policies to reduce reliance on the number.

Still, we recognize that we need to do more. Two-thirds of our notices have the Social Security number. Our notice infrastructure is

complex. About 60 different applications generate notices and every notice is created to respond to an individual's unique circumstances. Nevertheless, we are committed to replacing the SSN with a beneficiary notice code, or BNC, as we modify existing notices or create new ones. The BNC is a secure, 13-character, alphanumeric code that helps our employees identify the notice and the beneficiary and respond to inquiries quickly. We initially developed the BNC for use in the Social Security cost-of-living adjustment notice.

Additionally, next year, we will replace the SSN with the BNC on benefit verification letters as well as appointed representative and Social Security post-entitlement notices. Together these mailings account for 42 million annual notices.

We take great care to protect the integrity of the SSN and the personal information of the public we serve.

Thank you for the opportunity to describe our efforts. I'd be happy to answer any questions.

[The prepared statement of Ms. LaCanfora follows:]


**HEARING BEFORE**

**COMMITTEE ON WAYS AND MEANS, SUBCOMMITTEE ON SOCIAL SECURITY, AND COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON INFORMATION TECHNOLOGY**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**MAY 23, 2017**

**STATEMENT**
**OF**
**MARIANNA LACANFORA**
**ACTING DEPUTY COMMISSIONER FOR RETIREMENT AND DISABILITY POLICY**
**SOCIAL SECURITY ADMINISTRATION**

Chairman Johnson, Chairman Hurd, Ranking Member Larson, Ranking Member Kelly, and Members of the Subcommittees:

Thank you for inviting me to discuss the history of the Social Security number (SSN), how the Social Security Administration (SSA) uses it to administer its benefit programs, and recent efforts to reduce the number's use. I am Marianna LaCanfora, Acting Deputy Commissioner for Retirement and Disability Policy.

Our Programs

I want to begin by pointing out the unique role of the SSN for Social Security. We designed the SSN and SSN card in 1936 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 around 500 million unique numbers to eligible individuals.

The SSN continues to be 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, commonly referred to as "Social Security," which includes retirement, survivors, and disability insurance. We also use the number to administer the Supplemental Security Income (SSI) program, which provides monthly payments to people with limited income and resources who are aged, blind, or disabled.

On average, each month we pay Social Security benefits to approximately 62 million individuals, consisting of 42 million retired workers and 3 million of their spouses and children; 9 million workers with disabilities and 2 million dependents; and 6 million surviving widows and widowers, children, and other dependents of deceased workers. During fiscal year (FY) 2017, we expect to pay more than $940 billion to Social Security beneficiaries. Additionally, in FY 2017, we expect to pay nearly $55 billion in Federal benefits to a monthly average of approximately 8 million SSI recipients.

History of the SSN

When the Social Security program was enacted under the Social Security Act of 1935 (Act), the Act did not mandate the use of SSNs. However, the Act did authorize the creation of some type of record-keeping system. A 1936 Treasury Regulation provided that employees covered by the new program must apply to SSA for account numbers.

There is a rich history surrounding the development of the SSN. In brief, those responsible for implementing the new Social Security program understood that properly crediting earnings to the correct individual would be critical to the program's success. The agency could not use names alone to ensure accurate reporting; therefore, the agency designed the nine-digit SSN. The SSN allows employers to report workers' covered earnings accurately, and ensures that we can determine eligibility for benefits and pay the correct benefit amount. If we cannot properly record a worker's earnings, he or she may not qualify for Social Security benefits or the amount of benefits paid may be incorrect.

We also developed the SSN card, which shows the SSN we assigned to a particular individual, and assists employers in properly reporting earnings. It is important to note that the SSN card was never intended, nor does it serve, as a personal identification document. Although we have made many changes over the years to make the card counterfeit-resistant and continue to work to strengthen its security, we encourage agencies and the public to minimize the use of SSN cards whenever possible. To this end, we continue to expand electronic verification of the number with our Federal and State partners to reduce unnecessary use of the card and provide better service to the public. I will discuss these verifications in more detail shortly.

SSN Assignment

In the 1930s, and for many years thereafter, we assigned SSNs and issued cards based solely on the applicant's allegation of name, date of birth, and other personal information. We required no documentation to verify that information. Today, we use a robust application process requiring SSN applicants to submit evidence of age, identity, and United States citizenship or current work-authorized immigration status. In most cases, individuals (other than newborns) must come into a Social Security field office or Card Center to apply for an SSN and card. We require an in-person interview of all applicants age 12 or older. During the interview, we attempt to locate a prior SSN to help ensure that we do not assign an SSN to an individual assuming a false identity. We verify the birth records for United States citizens requesting an original card and the immigration documents presented by noncitizens requesting original or replacement cards.

Assigning SSNs and issuing SSN cards has always been one of our most significant workloads. In FY 2016, we assigned over 6 million original SSNs and issued nearly 11 million replacement SSN cards.

Expansion of SSN Use for Other Purposes

A confluence of factors led to the expanded use of the SSN over time. The universality and ready availability of the number made the SSN an incredibly convenient means of identifying people in other large systems of records. In 1943, for example, Executive Order 9397 required Federal agencies to use the SSN in any new system for identifying individuals. Then, beginning in the 1960s, SSN use expanded quickly due to advances in computer technology as government agencies and private organizations began using automated data processing and record keeping.

In 1961, the Federal Civil Service Commission began using the SSN as the identification number for all Federal employees. The next year, the Internal Revenue Service (IRS) began using the number as its taxpayer identification number. In 1967, the Department of Defense adopted the SSN as the service number for military personnel. At the same time, use of the SSN for computer and other accounting systems spread throughout State and local governments, to banks, credit bureaus, hospitals, educational institutions, and other parts of the private sector.

In the 1970s, Congress enacted legislation requiring an SSN to receive assistance under the Aid to Families with Dependent Children program (succeeded by Temporary Assistance for Needy Families), Medicaid, and food stamps. Additional legislation authorized States to use the SSN in the administration of tax, general public assistance, driver's license, or motor vehicle registration

laws within their jurisdiction. In the 1980s and 1990s, legislation required the use of the SSN in employment eligibility verification and military draft registration, among other things. The 1996 welfare reform law required the SSN to be recorded in a broad array of records—including applications for professional licenses, marriage licenses, divorce decrees, support orders, and paternity determinations—to improve child support enforcement.

SSN Verifications

As use of the SSN has expanded, so have our workloads relating to the SSN. For example, we routinely receive requests to verify the SSN in computer matching activities with other Federal and State agencies to reduce or prevent improper payments and to ensure better program integrity. We also provide SSN verifications to employers to ensure accurate wage reporting, and to private entities with consent of the SSN holder in certain circumstances. To help manage this work, and ensure it does not affect other critical workloads, we work with entities to process these requests electronically through automated data exchanges. In FY 2016, we performed over 2 billion automated SSN verifications for such varied purposes as the Department of Homeland Security's (DHS) E-Verify program, health care programs, voter registration and drivers' licensing, and many other government programs. Our robust verification and data exchange program, coupled with government agencies' increasing provision of online services, may, in time, drastically reduce the need for the SSN card.

Efforts to Reduce the Use of the SSN

As the agency responsible for assigning SSNs and issuing SSN cards, we are particularly aware of the harm SSN misuse can cause members of the public. Thus, we are always looking for opportunities to increase the protection of the SSN. In the early 2000s, we began taking steps to remove or truncate the SSN where possible. For example:

- *2001—Annual Notice Workloads*. We removed the full SSN from two of our largest annual notice workloads—the S*ocial Security Statements* and Social Security Cost of Living Adjustment (COLA) notices. These notices typically account for about a third of the notices we send our beneficiaries each year. On the *Statement*, we began displaying the last four digits of the SSN. On Social Security COLA notice, we began displaying a Beneficiary Notice Code (BNC). The BNC is an encrypted 13-character alphanumeric code that helps our employees identify the notice and the beneficiary, and further eliminates the need to include the SSN.

- *2004—Benefit Checks*. We worked with the Department of the Treasury to remove the SSN from all Social Security and SSI benefit checks. Instead of the SSN, Treasury began including a check number assigned during payment processing.

- *2006—President's Identity Theft Task Force Recommendations*. In September 2006, OMB released a memorandum highlighting the recommendations from the President's Identity Theft Task Force report. Pursuant to the report recommendations, we formed the SSN Best Practices Collaborative, which included representatives from 36 Federal departments and agencies and met regularly in 2007 to explore, develop, and share best practices for reducing reliance on SSNs. The Collaborative formed a subcommittee,

chaired by the IRS, and comprising agencies that handle high volumes of SSNs and personally identifiable information (PII), such as the Department of Defense, Department of Veterans Affairs, DHS, and the Centers for Medicare and Medicaid Services (CMS). We also established a clearinghouse on a bulletin board website in July 2007 that highlighted best practices for reducing the unnecessary use and display of the SSN, as well as contacts for specific programs and initiatives. While the website is no longer available, at the time over 25 agencies were registered to use it.

OMB May 2007 Memorandum

When OMB issued its May 2007 memo (M-07-16) requiring agencies to review their use of SSNs and eliminate any unnecessary uses, we immediately took a broader look at our use of the SSN, not only in Social Security programs, but also in our internal personnel practices. We recognized that, although Social Security programs rely on the necessary use of the SSN, our personnel processes could likely be refined to reduce superfluous uses of the number. Through this effort, we found opportunities to discontinue the use of the SSN in our personnel records and implemented various changes beginning in 2007, including:

- *Time and Attendance System*. We now only use an employee's SSN when we initially enter it into the system.
- *Training*. The sign-in process for our national Interactive Video training previously required employees to use their SSNs to log on to the system.
- *Labor Relations Grievance Tracking*. The new system uses a combination of name and locator, rather than SSN.
- *Employee Assistance Program*. We created a new application that uses the SSN only to assign a case number, which we use throughout the process.
- *Equal Employment Opportunity (EEO) Complaints*. The new system masks the SSN.

We recognize there may be opportunities for us to further reduce the use of the SSN in personnel records and will continue to pursue this in the future.

We also limited our use of the SSN in other systems, such as our performance appraisal systems and forms, (e.g., the Performance Assessment and Communication System, or PACS), and in 2015, we eliminated the use of the SSN in the form used to process employee requests for systems access (SSA-120). Furthermore, we continue to work closely with other Federal agencies to remove or eliminate the SSN from their documents when possible. For example, we are currently supporting CMS' efforts to remove the SSN from the Medicare Card, as required by the *Medicare Access and CHIP Reauthorization Act of 2015* (P.L. 114-10). We also participate in ongoing discussions with IRS on its efforts to allow for truncation of SSNs on employee copies of Forms W-2, as part of the Protecting Americans from Tax Hikes (PATH) Act of 2015, (P.L. No. 114-113, div. Q, title IV, 129 Stat. 2242).

The SSN on Social Security Notices

As noted above, the SSN is integral to all our internal business processes. We must use it to administer our programs and serve over 60 million Social Security beneficiaries and 8 million SSI recipients. Historically, including the SSN on notices has ensured that our front line technicians can quickly identify notices and respond to beneficiary inquiries. In 2015, we mailed approximately 352 million notices (with nearly two-thirds containing an SSN).[1] On average, we sent just over three notices containing an SSN per beneficiary and recipient per year.

Of the 233 million notices containing SSNs, approximately 64 million are Annual Benefit Statements (Form SSA-1099/1042) required by statute (Internal Revenue Code section 6050F) for tax purposes. The remaining notices comprise over 1,000 different notice types, including but not limited to award and denial notices, appeals, claims development, and many kinds of post-entitlement notices. The latter make up the bulk of our small volume notices, and relate to changes in benefits, overpayments, and certain cost of living notices. Other categories of notices include Medicare and earnings notices.

Our notice infrastructure is complex, and we draft every notice we issue to respond to an individual's unique circumstances. There are approximately 60 programmatic applications that generate notices. A majority of these automated systems send their notices through our Target Notice Architecture for formatting. The Target Notice Architecture uses language snippets referred to as Universal Text Identifiers (UTIs) to build customized notices. These UTIs contain static language and dynamic place holders that allow for customized language, such as name, address and SSN, to be inserted into the notice for each individual.

Despite the complexities of our notices and related systems infrastructure, we continue to look proactively for opportunities to safeguard the SSN in our beneficiary notices.

Removing the SSN from Agency Notices

We take seriously public concerns related to mailing documents that include the SSN. Therefore, in 2015, we convened an intra-agency workgroup to analyze options for removing the SSN from all agency notices. Based on our review, we concluded the best option would be to replace the SSN with the BNC—the identifier we now use on the Social Security COLA notice. The BNC will allow us to identify the notice and respond to inquiries quickly—just as the SSN has. As part of our IT modernization efforts, we will begin to modernize communications (notices and mailings) in 2018. As we modify notices, or develop new ones, we will put only the BNC on such notices.

In concert with CMS' efforts to remove the SSN from Medicare Cards, next year we plan to replace the SSN with the BNC on benefit verifications letters, which account for approximately 11 million notices. We also plan to replace the SSN with the BNC on certain notices to

[1] We do not routinely capture information related to notices with SSNs. The agency's 2015 intra-agency workgroup developed these estimates.

appointed representatives and on Social Security post-entitlement notices, which account for approximately 2.6 million and 28 million notices, respectively.

Conclusion

We take great care to protect the integrity of the SSN and the PII of our beneficiaries. We have committed to removing the SSN from our notices on a flow basis. Thank you for the opportunity to describe our efforts regarding these very important issues. I will be happy to answer any questions.

Mr. RICE. Thank you, Ms. LaCanfora.

Mr. DeVries, welcome and thanks for being here. Please proceed.

**STATEMENT OF DAVID DEVRIES, CHIEF INFORMATION OFFICER, OFFICE OF PERSONNEL MANAGEMENT**

Mr. DEVRIES. Thank you, Chairman Rice, Chairman Hurd, Ranking Member Larson, Ranking Member Kelly, and Members of the Subcommittees, thank you for the opportunity to appear before you today to represent the Office of Personnel Management with respect to reducing the use of Social Security numbers as a personal identifier.

In 1962, the Civil Service Commission adopted the SSN to identify Federal employees. Over time, the SSN became universal to almost every piece of paper or its digital form in a Federal employee's official personnel file. It became a de facto personnel identifier. The SSN was used for routine personal actions to record training, to request health benefits, and for many other purposes.

In 2007, OPM issued guidance to Federal agencies to develop consistent and effective measures for use in safeguarding of Federal employees' SSNs. The intent of these measures was to minimize the risk of identity theft and fraud in two ways, one by eliminating the unnecessary use of SSN as an identifier and by strengthening the protection of personal information, including SSNs, from theft or loss. Examples of the measures that we recommended were eliminating the unnecessary printing display of the Social Security number on forms, reports, and your computer displays, and restricting access to only those individuals who had a need to know, and they were notified of their additional responsibilities to safeguard that. We also included privacy and confidentiality statements to go along with the—and, finally, we came up with how do you mask it or how do you take the Social Security numbers out of the forms itself there.

Internal to the OPM, we examined our internal policies with respect to the use of SSNs and, in 2012, issued an addendum to our information security and privacy policy. The updated policy identifies acceptable uses of the SSN, describes how the authorized use will be documented, and presented alternatives for SSN. This internal policy addendum notes that acceptable use of the SSN are only those that are provided for by law, executive order, require interoperability with organizations outside the OPM, or are required by operational necessities to achieve agency mission. For example, the SSN is a single identifier that is consistent across the security investigation process and may be necessary to complete an individual's background investigation. But it is now protected in both transit and in storage.

OPM has taken other efforts to reduce the use of SSNs since issuing the 2012 policy. OPM modified the USAJOBS and the USA Staffing Systems so that neither collect SSNs from applicants. We also undertook an effort in 2016 to understand which IT systems maintain SSNs and how they use those to communicate with other programs. The initial inventory was completed in September 2016, and we are now using it to validate the progress made and identify other opportunities. In addition, we are updating the internal 2012 policy this year.

It is difficult to completely eliminate the Federal use of SSNs without a governmentwide coordinated effort and dedicated funding. SSNs are generally the common element linking information among agencies, OPM shared service providers, and benefit providers. In the fall 2016, OMB and OPM proposed the program unique identifier, or PUID, initiative to reduce the use of SSNs in many government systems and programs. The PUID initiative sought to facilitate the exchange of information without SSNs. This would be accomplished by providing an alternative numbering scheme to uniquely identify records across various programs and agencies. An initial proof of concept shows potential for continued study.

Members of the subcommittee, thank you for having me here today to discuss OPM's rule in reducing the use of SSNs and for your interest and support in this important issue here. Safeguarding the PI of our Federal employees and others whose information we hold is of paramount importance to OPM. I would be happy to address any questions you may have. Thank you.

[The prepared statement of Mr. DeVries follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

**STATEMENT OF**
**DAVID DEVRIES**
**CHIEF INFORMATION OFFICER**
**U.S. OFFICE OF PERSONNEL MANAGEMENT**

**before the**

**SUBCOMMITTEE ON SOCIAL SECURITY**
**COMMITTEE ON WAYS AND MEANS**
**AND**
**SUBCOMMITTEE ON INFORMATION TECHNOLOGY**
**COMMITTEE ON OVERSIGHT AND GOVERNENT REFORM**
**UNITED STATES HOUSE OF REPRESENTATIVES**

**on**

**"Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers"**

**---**

**May 23, 2017**

---

Chairman Johnson, Ranking Member Larson, Chairman Hurd, Ranking Member Kelly, and members of the subcommittees:

I am pleased to have the opportunity to appear before you today to represent the Office of Personnel Management (OPM) with respect to reducing the use of Social Security numbers (SSNs) as a personal identifier. In 1962, the Civil Service Commission adopted the SSN to identify Federal employees. Over time, the SSN became ubiquitous to almost every piece of paper – or its digital form – in a Federal employee's official personnel file. It became a de facto personal identifier. Over time the SSN was used for routine personnel actions, to record training, to request health benefits, and for many other purposes.

**OPM's Efforts to Reduce the Use of SSNs as a Personal Identifier**

In 2007 OPM issued guidance[1] to help agencies achieve a consistent and effective policy for safeguarding the SSNs of Federal employees. The intent of this guidance was to minimize the

[1] https://www.chcoc.gov/sites/default/files/trans847.pdf

risk of identity theft and fraud in two ways: (1) by eliminating the unnecessary use of the SSN as an identifier, and (2) by strengthening the protection of personal information, including SSNs, from theft or loss. Examples of measures that agencies were recommended to implement include: Eliminating unnecessary printing and displaying of the SSN on forms, reports, and computer display screens; Restricting access to the SSN to only those individuals whose official duty requires such access; Making sure individuals authorized to access the SSN understand their responsibility to protect sensitive and personal information; Including privacy and confidentiality statements that describe accountability clearly and warn of possible disciplinary action for unauthorized release of the SSN and other personally identifiable information and having them signed by those who have access to the SSN; Avoiding the display of SSNs on the input screen when the SSN is required as a data entry parameter, except when establishing the initial human resources or payroll record; And masking the SSN with asterisks or other special characters in all other record retrieval and access authorization processes.

OPM continues to examine its internal policy with respect to the use of SSNs and, in 2012, issued an addendum to its Information Security and Privacy Policy to address this issue. The updated policy identifies the acceptable uses of the SSN, describes how authorized uses should be documented, and presents alternatives for SSN use. This internal policy addendum notes that acceptable uses of the SSN are those that are provided for by law, require interoperability with organizations outside of OPM, or are required by operational necessities. For example, the SSN is the single identifier that is consistent across the security investigation process and may be necessary to complete an individual's background investigation.

OPM has taken other efforts to reduce the use of SSNs since issuing the 2012 policy. OPM modified the USAJOBS and the USAStaffing systems so that neither collects SSNs from applicants; it is provided only when the Agency onboards their new employee. We also undertook an effort in 2016 to understand what IT systems maintain SSNs and how they use SSNs to communicate with other programs by inventorying its forms and IT systems that collect and process SSNs. The effort was completed in September 2016. OPM also started data masking the SSN, when possible. OPM intends to review and update as appropriate the 2012 policy this year.

It is difficult to completely eliminate the Federal use of SSNs without a governmentwide coordinated effort and dedicated funding. SSNs are generally the common element linking information among agencies, OPM, Shared Service Providers (human resources, payroll, and training), and benefit providers, some of which are legally required to use SSN. OPM proposed the Program Unique Identifier (PUID) initiative to reduce the use of SSNs governmentwide in the many government systems and programs in September 2016. The PUID initiative facilitates the exchange of information without a SSN and thus eliminates the need of storing SSNs by providing an alternative way to uniquely identify records. An initial use case proof of concept showed potential for applicability for a front-end single sign-on process with additional development and pilots.

**Conclusion**

**Statement of David DeVries, Chief Information Officer**
**U.S. Office of Personnel Management**
**---**
**May 23, 2017**

Members of the Subcommittees, thank you for having me here today to discuss OPM's role in reducing the use of SSNs. Safeguarding the personally identifiable information of our Federal employees and others whose information we hold is of paramount importance to OPM. I would be happy to address any questions you may have.

Mr. RICE. Thank you, Mr. DeVries.
Ms. Jackson, thank you for being here. You can proceed.

**STATEMENT OF KAREN JACKSON, DEPUTY CHIEF OPERATING OFFICER, CENTERS FOR MEDICARE & MEDICAID SERVICES**

Ms. JACKSON. Chairman Rice and Hurd, Ranking Members Larson and Kelly, and Members of the Subcommittees, thank you for this opportunity to discuss the Centers for Medicare and Medicaid Services' work to safeguard the personally identifiable information of the beneficiaries whom we serve, including our ongoing work to eliminate use of the Social Security number on Medicare cards.

This effort is an important step in protecting beneficiaries from becoming victims of identity theft, one of the fastest growing crimes in the country. As we all know, identity theft can disrupt lives, damage credit ratings, and result in inaccuracies in medical records. Thanks to congressional leadership and, in particular, Chairman Johnson, whom I am sorry is not here today, and members of the Ways and Means Committee, and based on the recommendations of our colleagues from the Government Accountability Office, CMS will eliminate the Social Security number-based identifier on Medicare cards by April 2019, as Congress directed us, as part of the Medicare Access and CHIP Reauthorization Act of 2015, known as MACRA. We very much appreciate Congress providing us with the resources necessary to undertake this important project.

Beginning in April 2018, all newly enrolled Medicare beneficiaries will receive a Medicare card with a new Medicare Beneficiary Identifier, known as the MBI. At the same time, CMS will begin distributing the new Medicare cards to our current beneficiaries. This new Medicare number will have the same number of characters as the current 11-digit Social Security number-based health insurance claim number, known as the HICN, but will be visibly different and distinguishable from the HICN. With the introduction of the MBI, for the first time, CMS will have the ability to terminate the Medicare number and issue a new number to a beneficiary in instances where they are a victim of identity theft or their Medicare number has been compromised in some way.

Transitioning to the MBI will help beneficiaries to better safeguard their personal information by reducing the exposure of their Social Security numbers. CMS has already removed the Social Security number from many types of our communications, including the Medicare summary notices that are mailed to beneficiaries on a quarterly basis. We have prohibited private Medicare Advantage Plans and Medicare Part D prescription drug plans from using Social Security numbers on their enrollees' insurance cards.

Many people wonder why CMS has used an identifier based on the Social Security number in the first place. When the Medicare program was established in 1965, it was actually the Social Security Administration who administered the program. While CMS is now responsible for management of Medicare, the Social Security Administration still enrolls beneficiaries and both CMS and the Social Security Administration rely on interrelated systems to coordi-

nate eligibility for Medicare benefits and for Social Security benefits.

Currently, healthcare providers use the HICN when they submit claims in order to receive payment for healthcare services and also for supplies. And CMS and its contractors use the HICN to process those claims, authorize payments, and to issue some beneficiary communications.

We're in the process of making changes to over 75 of our affected systems to replace those systems' indicators with the MBI over the HICN, and we have developed the software that will generate MBIs and assign them to beneficiaries. We are working with our key partners, such as SSA, Railroad Retirement Board, States and territories, the Indian Health Service, the Department of Defense, Department of Veterans Affairs, healthcare providers, and other key stakeholders—there are a lot of them—to ensure that beneficiaries continue to receive access to services and our partners will be able to process using the new MBI.

We are implementing an extensive and phased outreach and education program for the estimated 60 million beneficiaries who will be receiving new cards, as well as to providers, private health plans, other insurers, clearinghouses, and other stakeholders. This fall, we will tell Medicare beneficiaries they will be receiving a new card, instruct them on when they will be receiving it, and what to do with their old cards.

We are also working to make sure that physicians and other healthcare providers are prepared to serve patients throughout the transition by creating information for providers both for them to update their records with the new MBI and also for them to help remind beneficiaries that they need to bring their new cards with them when they see their doctors.

We know from other successful large-scale implementations that it helps to allow time for all stakeholders to adjust to the changes. And so, beginning in April of 2018, when we begin to mail out the cards, CMS will have a 21-month long transition period, during which our systems will accept transactions both containing the MBI and also the HICN.

Throughout our programs, we are committed to safeguarding personal information. Redesigning the Medicare card to remove the Social Security number-based identifier is a very important step for CMS in helping to combat identity theft and further protect our beneficiaries.

Thank you very much for your interest in our progress today, and I look forward to answering your questions.

[The prepared statement of Ms. Jackson follows:]

**STATEMENT OF**

**KAREN JACKSON**
**DEPUTY CHIEF OPERATING OFFICER,**

**CENTERS FOR MEDICARE & MEDICAID SERVICES**

**ON**

**PROTECTING AMERICANS' IDENTITIES:**

**EXAMING EFFORTS TO LIMIT THE USE OF SOCIAL SECURITY NUMBERS**

**BEFORE THE**
**U.S. HOUSE COMMITTEE ON WAYS & MEANS**
**SUBCOMMITTEE ON SOCIAL SECURITY**
**AND**
**U.S. HOUSE COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM**
**SUBCOMMITTEE ON INFORMATION TECHNOLOGY**

**MAY 23, 2017**

**Statement of Karen Jackson, Deputy Chief Operating Officer,**
**Centers for Medicare & Medicaid Services**
**"Protecting Americans' Identities:**
**Examining Efforts to Limit the Use of Social Security Numbers"**
**May 23, 2017**

Chairmen Johnson and Hurd, Ranking Members Larson and Kelly, and members of the subcommittees, thank you for this opportunity to discuss the Centers for Medicare & Medicaid Services' (CMS') work to safeguard the personally identifiable information (PII) of the beneficiaries we serve, including our ongoing work to eliminate use of the Social Security number (SSN) on Medicare cards and in Medicare transactions. This effort is an important step in protecting beneficiaries from becoming victims of identity theft, one of the fastest growing crimes in the country.[1] Identity theft can disrupt lives, damage credit ratings, and result in inaccuracies on medical records. CMS knows that we have an important role to play in protecting our beneficiaries, while maintaining their access to high quality health care.

CMS has worked to eliminate the unnecessary use of SSNs, in accordance with OMB Circular A-130, including by minimizing its use on mailings. To build on this work, CMS appreciates Congress's leadership in providing the direction and resources to undertake the important work of removing SSNs from Medicare cards. As you know, as required by MACRA, by April 2019, CMS will eliminate the use of beneficiaries' SSNs as the source of the primary identifier on Medicare cards and replace it with a new, unique Medicare Beneficiary Identifier (MBI), or Medicare number.

CMS recognizes the trust that Congress and the American people have placed in us to complete this undertaking, and further protect Americans from identity theft. As we undertake this project, CMS seeks to minimize burdens for beneficiaries and providers, minimize disruption to Medicare operations, and effectively manage the cost, scope, and schedule for the project. In particular, we are preparing our communication channels to accommodate any questions beneficiaries may have as we make this change.

[1] https://www.bjs.gov/content/pub/press/vit14pr.cfm

Transitioning from the SSN-based Health Insurance Claim Number (HICN) to the MBI will help Medicare beneficiaries better safeguard their personal information by reducing the exposure of their SSNs. We are in the midst of a complex, multi-year effort that requires coordination between Federal, state, and private-sector stakeholders as well as an extensive outreach and education program for Medicare beneficiaries, providers, and other stakeholders.

Once we transition to the MBI, for the first time, CMS will have the ability to terminate a Medicare number and issue a new number to a beneficiary, for circumstances in which they are the victim of medical identity theft or their Medicare number has been compromised. This was not possible when the Medicare number was SSN-based. Being able to deactivate a compromised MBI will enable CMS to quickly respond and better prevent further misuse of a compromised number. CMS will be able to issue a beneficiary a new identifier without compromising access to care.

**History of Social Security Numbers in Medicare**

From the creation of the Medicare program under the Social Security Act in 1965 until 1977, the Medicare program was administered by the Social Security Administration (SSA). While CMS is now responsible for the management of Medicare, SSA and CMS continue to rely on interrelated systems to coordinate both Social Security and Medicare eligibility. Because of this shared history, SSNs, which are used in the SSA's systems, are a key component of the identification number CMS uses for beneficiaries. To identify beneficiaries, Medicare cards include a HICN, which is based upon a beneficiary's SSN, or in cases where a beneficiary's Medicare eligibility is based on the employment status and Medicare payroll tax contributions of another person, his or her spouse or parent's SSN.

SSA determines Medicare eligibility and transmits enrollment information to CMS; CMS then issues the Medicare card with the HICN to the beneficiary. Often, when receiving care, the beneficiary shows the provider or supplier their Medicare card with the HICN, just as an individual with private insurance uses their insurance card. The provider or supplier then uses

the Medicare card information to check eligibility and to bill Medicare, a process that involves multiple CMS systems.

Today, CMS uses the HICN to identify beneficiaries in more than 75 CMS systems, and in CMS communications with other Federal partners. Likewise, providers are required by CMS to use the HICN identifier when they submit claims in order to receive payment for treatments, services, and supplies. CMS and its contractors' systems use the HICN to check for duplicate claims, apply claims and medical policy edits, authorize or deny payment of claims, issue Medicare Summary Notices (MSNs), and conduct printing and mailing operations.

**Reduce the use of the SSN on Public Documents and Mailings**

CMS has already removed SSNs from many types of communications, including Medicare Summary Notices mailed to beneficiaries on a quarterly basis. We have prohibited private Medicare health (Medicare Advantage) and Prescription Drug (Part D) plans from using SSNs on enrollees' insurance cards (*e.g.*, insurance cards for Medicare Advantage, cost contract, and Part D enrollees). CMS has also looked for ways to minimize the need for mailings including beneficiary personally identifiable information (PII). For example, in November 2013, CMS introduced an automatic bank account withdrawal program called Medicare Easy Pay. This system allows beneficiaries to pay premiums by direct withdrawal from their bank accounts. Beneficiaries who use Easy Pay can opt out of receiving monthly mailings by calling 1-800-Medicare. Beneficiaries who choose to suppress their monthly billing statement receive one statement per year. Also in 2013, CMS instructed its Medicare Administrative Contractors (MACs) to partially redact HICNs on all Medicare Redetermination Notices[2], which are sent to beneficiaries during the claims appeal process.

**Replacing Health Insurance Claim Numbers with Medicare Beneficiary Identifiers**

The initiative to remove SSNs from Medicare cards, as called for by MACRA, and to replace HICNs with MBIs has been a substantial undertaking. MACRA provided a total of $320 million to CMS, SSA, and the Railroad Retirement Board (RRB) for this critical initiative. The replacement process requires coordinating with Federal, state, and private sector stakeholders;

[2] https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/Downloads/R1296OTN.pdf

updating and modifying numerous internal IT systems; and conducting an extensive outreach and education campaign for beneficiaries, providers, and other stakeholders. CMS is working to accomplish these tasks without disrupting payments to providers, business processes, or beneficiaries' access to care.

To date, we have analyzed and are in the process of making changes to over 75 CMS systems that are impacted by this initiative. Additionally, we have been actively working with our key partners such as the SSA, RRB, States and Territories, Indian Health Service (IHS), Department of Defense (Tricare), Department of Veterans Affairs as well as other key stakeholders on implementation to ensure that beneficiaries continue to receive access to services and partners will be able to process with the new MBI. CMS has developed the software in our Medicare Enrollment Database (EDB) that will be used to generate MBIs and assign them to beneficiaries. This assignment will be executed in mid-2017.

*The New Medicare Beneficiary Identifier*

The new Medicare number will be a unique and randomized number that will be placed on the new Medicare Card for each Medicare beneficiary. In order to move from current use of the SSN-based HICN to use of the MBI, CMS will randomly generate a new MBI for all Medicare beneficiaries, including all current and deceased beneficiaries. Assigning MBIs to deceased beneficiaries is critical for two reasons: it ensures that appropriate claims can continue to be processed smoothly after a beneficiary's death, and it facilitates researchers' ongoing work with Medicare datasets. CMS anticipates that it will use an MBI generator function to initially assign approximately 150 million MBIs, which includes 60 million active and 90 million deceased beneficiaries.

The new MBI will have the same number of characters as the current 11-digit HICN, but will be visibly different and distinguishable from the current HICN. It will also be easy to read and limit the possibility of letters being interpreted as numbers.

Beginning in April 2018, CMS will start the process of distributing new Medicare cards with the new MBI to current beneficiaries, and all newly enrolled beneficiaries eligible for Medicare will

receive the new Medicare card with a MBI. As of April 2018, CMS will be able to respond to requests to change MBIs for beneficiaries whose identity has been compromised.

**Coordination with Partners and Stakeholders**

Early on in the implementation process, CMS met with SSA and RRB to discuss the strategy, timeline, and assumptions for removing the SSN from Medicare cards. CMS also met with states and private health plans to coordinate new processes for crossover claims. In addition, CMS has procured a systems integrator to coordinate this multi-faceted project.

CMS will complete its system and process updates to be ready to accept and return the MBI on April 1, 2018. All stakeholders who submit or receive transactions containing the HICN must also modify their processes and systems to be ready to submit or exchange the MBI by April 1, 2018. CMS has held several key Open Door Forums with providers, billing agents, industry and other stakeholders to help them prepare their systems and business processes for this effort. To assist in the preparation, we have established a SSNRI website[3] that contains key operational information for providers, plans and other stakeholders.

To ensure a smooth implementation for states, CMS has formed a bi-weekly All-State SSNRI Forum call which includes representatives from the Center for Medicare (CM), Center for Medicaid and CHIP Services (CMCS), each CMS Regional Office, and every state, territory and the District of Columbia. These calls provide CMS the opportunity to promptly communicate important guidance and updates to the state Medicaid agencies (SMAs) and for SMAs and their invited key stakeholders to ask questions, share information and facilitate coordination. We have also identified the CMS and State IT systems that are affected with State implementation of MBI and are working with the States to make IT system and business changes. Similarly, we have instituted an All Federal Partners call, where we discuss key implementation issues that are common to our impacted Federal partners (e.g. SSA, RRB, VA, and DOD).

Testing of CMS IT systems is currently underway, and CMS is currently working on an integrated testing scope and schedule for State partners. Integration testing with States' IT

[3] https://www.cms.gov/medicare/ssnri/index.html

systems will begin in October 2017. States will test internally, with CMS and their external partners by the end of 2017.

Medicare beneficiaries often rely on their physicians and other providers for important information, so CMS is also working to make sure that these providers are prepared to serve their patients throughout the transition to MBIs. CMS has already begun communicating with providers and others to encourage them to look at their practice management IT systems and business processes and determine what changes they will need to make to use the new MBI. CMS is creating information for providers to give their patients to remind them to bring their new cards with them.

In addition, to ensure a smooth implementation, reduce burden on beneficiaries, providers, and other partners and, more importantly, to reduce the chance of care being interrupted, CMS will have a transition period during which our IT systems will need to accept and process transactions that have either a HICN or an MBI. We know from other successful large scale implementations that it is beneficial to allow time for beneficiaries, providers, and other stakeholders to adjust to changes and to address any problems that may arise. During this transition period, which will occur from April 1, 2018 through December 31, 2019, CMS will continue to process claims and other transactions without change, so that a provider will be able to submit a claim using either a valid and active HICN or a MBI and it will be processed as it is today. Beginning in October 2018, through the transition period, when a provider submits a claim using a patient's valid and active HICN, CMS will return both the HICN and the MBI on every remittance advice, which is a notice of payment sent to providers as a companion to Medicare claim payments. During this period, CMS will also monitor operational activities to ensure that the use of the MBI is increasing as the transition date approaches.

**Outreach and Education**

While we are modifying our IT systems, and before we issue new Medicare cards, we are implementing an extensive and phased outreach and education program for an estimated 60 million[4] Medicare beneficiaries, as well as providers, private health plans, other insurers,

[4] https://www.cbo.gov/sites/default/files/cbofiles/attachments/44205-2015-03-Medicare.pdf

clearinghouses, and other stakeholders. Since the fall of 2016, we have held numerous provider listening sessions, hosted Open Door Forums, presented at conferences, and created a SSN removal initiative webpage with provider-specific information[5] on how providers and vendors must change their own IT systems to accommodate the change to MBI from HICN. We shared the new MBI format so they could program edits around the new identifier, as well as information on how they will use the MBI. We will continue to reach out to providers with information on how to make the transition as smooth as possible. We are also communicating with Medicare Advantage and Part D plans, other insurers, and State Medicaid Agencies to ensure they know how to use MBIs so that they can continue their coordination of benefits activities.

Beginning in the fall of 2017, we will have a series of communications to inform beneficiaries that they will be receiving a new card, instruct them on when and how they should use their new card, and when and how to destroy their old card. In order to prevent bad actors from taking advantage of potential confusion and gaining access to personal information, we plan to clearly communicate with beneficiaries about when and how they will receive a new card, and how to get answers to their questions.

CMS plans to launch communication activities to support beneficiary education in the fall of 2017 by giving key partners and stakeholders information about the effort. During this timeframe, we will also be conducting outreach reminding beneficiaries of the steps they need to take to protect themselves from medical identity theft. Beneficiaries will see information about the new card in the 2018 Medicare & You handbook they will receive this October. Finally, a robust, broad based outreach and education campaign aimed at beneficiaries will begin in January 2018 and continue through April 2019. CMS is also working closely with the Social Security Administration to ensure that their communications to Medicare beneficiaries also include detailed information about the new card and new MBI.

[5] For more information visit: https://www.cms.gov/Medicare/SSNRI/Providers/Providers.html

**Other Beneficiary and Caregiver Outreach and Education**

Even as CMS is taking steps to eliminate the unnecessary use of SSNs and other PII to help safeguard beneficiaries from identity theft, alert and vigilant beneficiaries, family members, and caregivers are some of our most valuable partners in identifying and stopping misuse of personal information or other fraudulent activity. In 2013, CMS began sending redesigned Medicare Summary Notices (MSNs),[6] the explanation of benefits for people with Medicare fee-for-service, to make it easier for beneficiaries to spot fraud or errors. The new MSNs include clearer language, descriptions and definitions, and have a dedicated section that tells beneficiaries how to spot potential fraud, waste, and abuse. Beneficiaries are encouraged to report fraud, waste, and abuse to 1-800-MEDICARE, and this is promoted in the re-designed MSN.

CMS engages in a variety of outreach efforts to inform beneficiaries about the risk of medical identity theft and to educate them on steps they can take to protect their personally identifiable information. A robust outreach campaign has been executed every fall since 2010, prior to Medicare Open Enrollment, when we know there is a higher prevalence of fraud. Information is available online and in The Medicare & You handbook, which is distributed to all Medicare households each fall. These resources explain the importance of personal information and how it is used by Medicare; they also include instructions on contacting the appropriate authorities when Medicare fraud, including medical identity theft, is suspected. In these publications, Medicare beneficiaries are advised to take preventive action against identity theft, including:

- Guarding personal information such as Medicare identifiers and SSNs, and only share personal information with providers, plans, and suppliers approved by Medicare (a list of approved suppliers is available on Medicare.gov). Importantly, do not give personal information to anyone who calls or comes to the door uninvited, including individuals claiming to be conducting a health survey. Medicare and Medicaid do not send representatives to homes to sell products or services.
- Checking medical bills, MSNs, explanations of benefits, and credit reports for accuracy; using a calendar to record the receipt of services and comparing this to Medicare statements.

[6] http://blog.medicare.gov/2013/06/06/redesigned-with-you-in-mind-your-medicare-summary-notice/

- Do not accept offers of money or gifts for free medical care.
- Not letting anyone borrow or use a Medicare ID card or identity in exchange for goods or services; this is illegal.

CMS has been partnering with the Administration for Community Living to support the Senior Medicare Patrol (SMP) program, a volunteer-based national program that educates Medicare beneficiaries, their families, and caregivers to prevent, detect, and report Medicare fraud, waste and abuse. The SMP program empowers Medicare beneficiaries through increased awareness and understanding of health care programs and educates them on how to recognize and report fraud. In 2015, the SMP projects reported $2.5 million in expected Medicare recoveries that were attributable to their projects,[7] an increase of 282 percent from 2014.[8] SMP projects also work to resolve beneficiary complaints of potential fraud in partnership with state and national fraud control and consumer protection entities, including Medicare contractors, State Medicaid fraud control units, State attorneys general, the Department of Health and Human Services Office of Inspector General (HHS OIG), and the Federal Trade Commission (FTC).

**Moving Forward**

Throughout our programs, CMS is committed to safeguarding the personal information of the beneficiaries and consumers we serve. Redesigning the Medicare card to remove the SSN-based identifier is just the latest initiative in a long line of efforts to safeguard our beneficiaries and the Medicare Trust Funds. This is an important step in helping to combat identity theft and further protect our beneficiaries. Given how much is at stake, CMS' objectives are to complete the transition to the new cards in a timely fashion that not only improves security, but also minimizes beneficiary confusion and disruption from denied claims or access to services. CMS is doing all that it can to make this a successful transition for beneficiaries, their families, providers, and our partners. Thank you for your interest in our progress towards removing the SSN from Medicare cards and protecting the personal information of beneficiaries. I look forward to working with the Committees on these important issues.

---

[7] https://oig.hhs.gov/oei/reports/oei-02-16-00190.asp Note: The vast majority of these recoveries resulted from one project's efforts, which led to the conviction of a hospice company owner for Medicare fraud.
[8] http://www.smpresource.org/Handler.ashx?Item_ID=3A7D6D74-1D4F-4FA6-A8AE-2979022F185F

Mr. RICE. Thank you, Ms. Jackson.

Mr. Oswalt, thank you for being here. You can proceed.

**STATEMENT OF JOHN OSWALT, EXECUTIVE DIRECTOR FOR PRIVACY, OFFICE OF INFORMATION TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS**

Mr. OSWALT. Good afternoon, Chairman Rice, Chairman Hurd, Ranking Member Larson, Ranking Member Kelly, and distinguished Members of the Subcommittees. Thank you for this opportunity to participate in your joint hearing on government use of Social Security numbers across the government and VA, and the steps that VA has taken to find ways to reduce, eliminate Social Security numbers from VA's systems.

VA's mission is to serve with dignity and compassion America's veterans and their families. This mission is contingent upon accurate and timely information being readily available. If we are to advocate for veterans, ensure they receive the medical care, benefits, social support, and lasting memorials they have rightfully earned in service to our Nation, VA most properly identify, verify, and coordinate this protected information entrusted to us.

The Department interfaces with many other Federal agencies, including but not limited to, the Department of Defense, the Social Security Administration, the Internal Revenue Service, and the Department of Education.

VA's primary uses of SSNs are threefold: One, locate veterans and their dependents to ensure correct identification associated with the delivery of healthcare and services; second identify employees for employment related recordkeeping; and, three, ensure 100 percent accuracy in patient identification. Mistaken identity in the delivery of healthcare can result in catastrophic and tragic outcomes. Until such time when the comprehensive and equally accurate means to do so is established and implemented, the use of SSNs remains the best means of ensuring patient identification.

In addition, SSNs must be used if required by law or regulation for purposes such as background investigations, income verification, and the matching of computer records between government agencies.

Elimination of the SSN use is not solely a function of information technology, IT. The business processes used by the Veterans Health Administration, VHA; the Veterans Benefit Administration, VBA; and VA offices require a complete overhaul in how they establish absolute identity verification inside VA and, equally important, outside VA.

IT solutions to eliminate SSN use can only occur after our integrated and comprehensive review of SSN's use and its interconnectedness is complete. VA recognizes the growing threat posed by identity theft and the impact on veterans, dependents, and employees. In 2009, VA created and implemented the enterprisewide Social Security reduction effort—Social Security Number Reduction Effort. The goal of an SSNR is to gather and catalog SSN use, leading to the reduction and/or elimination of the SSN as the VA's primary identifier, all while maintaining the 100 percent requirement for proper veteran patient identification.

For example, VHA has eliminated the full SSN use on appointment letters, routine correspondence, and the veteran's health identification card. VA mailout pharmacy has eliminated the SSN from prescription bottles and mailing labels. As a whole, VA has removed SSNs from several forms where such use was deemed not necessary. VBA is modifying an existing contract to replace SSNs with barcode labels on all outgoing correspondence. Completion of that effort is expected in November of this year.

As VA migrates away from SSN use, the Office of Information Technology is collaborating with stakeholders to continue expanding the use of the Master Veteran Index, MVI, a registry of veterans, their beneficiaries and other eligible persons. MVI serves as the authoritative identity source within VA and generates an assigned and integrated control number, or ICN, for each veteran. The use of MVI as a unique identifier continues to expand with the ultimate goal being replacement of the SSN as a primary identifier.

There are many challenges facing VA regarding the elimination of the unnecessary collection and use of the SSN. This includes an enterprisewide system analysis that needs to be conducted to find and identify the large volume of interface systems that VA needs for clinical care and administrative functions, undertaking a robust education and retraining program for employees to implement any now unique identifier—this has already begun, but it will take time to integrate fully into our work processes—and acceptance by the veteran committee community. A change of this magnitude across the entire VA system will require substantial outreach and education.

VA has made considerable progress toward eliminating unnecessary use of SSNs and continues to reduce the use of SSNs with the goal to replace it with an alternative primary identifier. This concludes my testimony, and I'm prepared to answer any questions you or other Members of the Subcommittee may have. Thank you.

[The prepared statement of Mr. Oswalt follows:]

**STATEMENT OF**

**MR. JOHN OSWALT,**

**EXECUTIVE DIRECTOR FOR PRIVACY**

**OFFICE OF INFORMATION TECHNOLOGY**

**DEPARTMENT OF VETERANS AFFAIRS (VA)**

**BEFORE THE**

**HOUSE WAYS AND MEANS COMMITTEE,**

**SUBCOMMITTEE ON SOCIAL SECURITY**

**AND**

**HOUSE OVERSIGHT AND GOVERNMENT REFORM,**

**SUBCOMMITTEE ON INFORMATION TECHNOLOGY**

**MAY 23, 2017**

Good afternoon, Chairman Johnson, Chairman Hurd, Ranking Member Larson, Ranking Member Kelly, and distinguished members of the Subcommittees. Thank you for providing me with this opportunity to participate in your joint hearing on "Government Use of Social Security Numbers," and to discuss the actions that VA is taking to find ways to eliminate or reduce the use of Social Security Numbers (SSN) from VA's information systems.

***Overview***

VA's revised SSN Reduction Plan clarified many of the activities that must take place over the next few years to reduce the unnecessary collection and use of the SSN within VA.

VA's mission is to serve America's Veterans and their families with dignity and compassion, to be their principal advocate, and to ensure that they receive the medical care, benefits, social support, and lasting memorials for which they are eligible because of their service to our Nation. VA is the second largest Federal Department and as advocates for Veterans and their families, VA employees are committed to providing world-class services in the provision of benefits.

VA is composed of a Central Office, located in Washington, DC, and field facilities throughout the United States, American Samoa, Guam, Puerto Rico, the Philippines, and the Virgin Islands. VA has three major line organizations: the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA).

VA's Administrations have very different missions – health, benefits, and memorial affairs. To complete these missions, VA needs to collect and maintain a tremendous store of personal information about Veterans and their beneficiaries. The Department interfaces with many other Federal agencies including, but not limited to, the Department of Defense (DoD), the Social Security Administration (SSA), the Internal Revenue Service (IRS) under the Department of the Treasury, and the Department of Education (DOE).

VA's primary uses of Social Security numbers (SSNs) are threefold:

(1) Locate Veterans and their dependents to ensure correct identification associated with the delivery of benefits and services;

(2) Identify employees for employment-related record keeping; and

(3) Ensure 100 percent accuracy in patient identification.

Mistaken identity in the delivery of health care can result in catastrophic and tragic outcomes. Until such time when a comprehensive and equally accurate means to do this is established and implemented, the use of SSNs remains the best means of ensuring patient identification within our records.

In addition, SSNs must be used if required by law or regulation, for purposes such as: Background investigations; security checks for validation purposes, such as computer matching of records between government agencies; and support of unique identification.

***Reliance on SSNs***

VA currently relies on the SSN to ensure that the correct records are obtained and utilized to determine eligibility for VA benefits such as compensation, disability, education, and rehabilitation. VA is required by 38 U.S.C. § 5103A, to request evidence from third parties on behalf of Veterans to support their claims. In these requests, VA must sufficiently identify the party for whom it is seeking information. Many entities holding Veterans' records, including DoD, other government agencies, and private parties, continue to utilize SSNs as a primary identifier. As such, VA will face substantial challenges in obtaining records from these entities on behalf of Veterans if precluded from using the SSN. This will negatively impact Veterans by delaying the

time required to process their claims and possibly even preventing VA from obtaining the records needed to establish Veterans' eligibility to benefits.

VA's success rate in matching records with other Federal and non-Federal organizations is over 85 percent when the SSN is available compared to 20 percent when the SSN is not used. VA providers will not have access to important outside care information and could order redundant tests, slow decision making, or make incorrect and even harmful decisions when such data is unavailable. VA also participates in Health Information Exchanges with DoD, Walgreens, Kaiser Permanente, etc., and without the use of the SSN to help match the Veteran within these exchanges, critical health information will not be available leading to poor health care decisions and slower treatment.

Elimination of SSN use is not solely a function of information technology (IT). The business processes used by VHA, VBA and other VA offices require a complete overhaul in how they establish absolute identity verification inside VA and most importantly outside of VA. IT solutions to eliminate SSN use can only occur after the integrated and comprehensive review of the prevalence and inter-connectedness of SSN use is complete.

***Efforts to reduce the use of SSNs***

VA recognizes the growing threat posed by identity theft and the impact on Veterans, dependents and employees. In 2009, VA created and implemented the enterprise-wide Social Security Number Reduction (SSNR) effort, in response to the Office of Management and Budget Memorandum M-07-16, "Safeguarding Against and

Responding to the Breach of Personally Identifiable Information (May 2007)." The key goal of the SSNR is to reduce or eliminate the unnecessary collection and use of SSNs as the Department's primary identifier, while maintaining the 100 percent requirement for proper Veteran-Patient identification. For example:

- VHA eliminated the use of SSNs on appointment letter correspondence and the Veterans Health Identification card.
- VA Pharmacy mail out eliminated the SSN from prescription bottles & mailing labels.
- VA removed the SSN from several forms where it was not deemed necessary.
- VA is currently evaluating the elimination of SSNs from correspondence.
- VA set defaults in some software to eliminate printing SSNs, e.g. Document Storage System/Release of Information (DSS/ROI).
- NCA has reviewed and reevaluated all of its forms requiring SSNs.
- VA/DoD Health Information Exchange Joint Legacy Viewer is using the Integration Control Number (ICN), Electronic Data Interchange Personal Identifier (EDIPI) and other demographics for trait matching while phasing out use of the SSN.
- VHA is utilizing a SSNR tool to collect VHA's SSN holdings data but it has limitations due to outdated technology. The Office of Information & Technology (OIT) is currently developing a new SSNR tool for VA-wide use which is expected to be completed by September 2017.

***Master Veteran Index System***

As VA works to migrate away from the use of SSNs as the sole means of Veteran identification in our records, OIT is collaborating with the Veterans Relationship Management Initiative to create the Master Veteran Index (MVI) system and require MVI integration for every VA system. MVI serves as the authoritative identity service within VA. MVI assigns an ICN, a unique identifier, for Veterans, dependents and beneficiaries. The ICN is a sequentially assigned, non-intelligent number that, in itself, does not provide any protected sensitive information about the Veteran-patient. The ICN is a means to accurately and securely track the individual and confirm their identification. ICNs conform to the American Society for Testing and Materials International standard for a universal health care identifier. MVI now has information on over 26 million Veterans, dependents, and beneficiaries who have applied for health care. While additional work remains to fully extricate SSNs from Veteran records, including re-engineered business processes and legacy system upgrades, programs like MVI have made significant progress towards the goal of SSN reduction.

***Challenges***

There are several major challenges facing VA regarding the elimination of the unnecessary collection and use of the SSN:

- An organization wide analysis of VA IT systems needs to be conducted due to the volume of interfaced IT systems VA uses for clinical care and administrative functions. VA anticipates that many IT system changes need to be made before VA can implement new unique identifiers that will replace the SSN as the primary identifier.

- Culture change among employees is required since long time employees are accustomed to using the SSN to authentication purposes. VA will need to implement education and retraining programs for employees to break the habit of using the SSN as the primary way to identify Veterans in its records. This has already begun, but it will take time to instill in the workforce and processes across the Department. After the MVI correlation is complete, it will still take several years to change IT system look up tables to search for Veterans and beneficiaries with the ICN or EDIPI instead of the SSN.
- Culture change is necessary for Veterans as well. Resistance to change will need to be balanced against the continued threat to identity theft if the old card is lost or stolen.

***Conclusion***

VA has made considerable progress towards implementing the SSN reduction initiative. VA continues to reduce the use of SSNs with the goal to replace the SSN with an alternative primary identifier. The timeframe to implement an alternate primary identifier would be contingent upon an organization-wide information system analysis, business needs, technology upgrades and funding.

This concludes my testimony, and I am prepared to answer any questions you or other Members of the Subcommittees may have. Thank you.

Mr. RICE. Thank you, Mr. Oswalt.

We now turn to questions. As is customary for each round of questions, I will limit my time to 5 minutes, and I will ask my colleagues to also limit their questioning time to 5 minutes as well.

Mr. Oswalt, I want to start with you. You were just speaking of the hurdles that the VA has to cross to eliminate the Social Security number and, of course, how critical it is that we make sure that we identify each patient, as their lives are in the balance, right, and make sure they get the right medication and so forth.

So you were saying that, as a replacement for the Social Security number, you started implementing an ICN. What you didn't tell us is how long it's going to take to get that done. What would be your best estimate for when you can get that done?

Mr. OSWALT. Well, the MVI, which is the registry of all certain types of identifiers, has been in place in various incarnations since 1999.

Mr. RICE. So you don't use Social Security numbers anymore?

Mr. OSWALT. We do use Social Security, but its use as a primary identifier is still in the VA processes. The ICN is generated by all the information that the MVI collects. So using that ICN as a means to identify a veteran as their information traverses the system or a machine talking to a machine; that has happened to a large extent already. It's primarily the SSN use is when there's a human-to-human interface between the clinician and the patient.

Mr. RICE. Do you still have their Social Security numbers on their little wristbands?

Mr. OSWALT. Yes, we do. There is an effort underway, I believe, on a pilot level. Right now, we are seeking to eliminate the full SSN with the goal of being a complete elimination, and there's also a barcode——

Mr. RICE. Do you have any kind of timetable for that?

Mr. OSWALT. Sir, I would have to take that and provide that for the record because I'm not aware of the project status.

Mr. RICE. Thank you, Mr. Oswalt.

Ms. Jackson, your testimony was very interesting and exciting to me. You said, by 2018, you will eliminate Social Security numbers from the Medicare cards. You are moving at lightning speed for the Federal Government. Thank you for your efforts.

Mr. DeVries, you said something that was very interesting to me. You have stopped collecting Social Security numbers for applicants for employment for the Federal Government?

Mr. DEVRIES. Correct, sir. When an applicant is going to enter into or wants to come into the Federal Government and they go to the USAJOB site, we no longer collect their Social Security number from them at that time, correct.

Mr. RICE. When do you collect their Social Security numbers?

Mr. DEVRIES. So we don't collect it. The agency—once we match up the job applicants against the job posting, to what we call U.S. Staffing, and the agency takes that referral list and the list of applicants and they narrow it down and they make the selection, when they bring that person on to make them employment offer, that's when the agency that's hiring them collects that from them then.

Mr. RICE. I know they would use their Social Security number for tax withholdings and such. What else would they use the Social Security number for when they were looking to hire somebody?

Mr. DEVRIES. So it is mostly that. It is your status of employment and then the benefits that come with it, whether it be the pay and then reporting back to the IRS and the Social Security side of the house.

Mr. RICE. Do you do criminal background checks in any agency of the government?

Mr. DEVRIES. So, once you become an employee and if your position requires that, then, when you submit for the background investigation, that would also be the primary use. And similar to what we do in the VA, though, once it gets into the background investigation system, then it is a different number that becomes the controlling number for it.

Mr. RICE. And since this massive hacking that occurred several years ago, I assume you've implemented a lot more protections to prevent that from happening again.

Mr. DEVRIES. Yes, sir.

Mr. RICE. Ms. LaCanfora, gosh, amazing statistics. Did I hear you correctly that you respond, that you verify 2 billion requests per year? Is that right?

Ms. LACANFORA. Two billion verifications, yes.

Mr. RICE. Wow. So that would be like six for every single living person in the country.

Ms. LACANFORA. Yes. It is worth noting that more than half of those are Federal and State agencies that are verifying numbers with us, and that can happen multiple times throughout a year if they are processing, for example, an application for benefits.

Mr. RICE. All right.

OMB has required agencies to eliminate the unnecessary use of Social Security numbers, but they never defined what necessary use is. How does each of your agencies define necessary use? I'll start with you, Mr. Wilshusen.

Mr. WILSHUSEN. Actually, I don't know how my agency has defined unnecessary use. What we did in terms of our audit of the other agencies is determine to what extent that they have defined unnecessary use. We found that of the 24 CFO Act agencies, a number of them, four I believe, did not define what "unnecessary use" is and another eight didn't have it documented or did not have a formal definition. Rather the agencies, based it on the judgment of the individuals who are making the particular assessment on Social Security use.

Mr. RICE. Thank you, sir.

Mr. Larson.

Mr. LARSON. Thank you, Mr. Chairman.

And I want to thank the witnesses again.

What a credit to government service you are, and I thank you for being here today.

Just a couple of questions. First, it has got to be incredibly hard to operate an agency that is the largest insurer in the Nation and to do so with a 99-percent loss ratio, the envy of any private sector insurance company. Kudos to you. Not without its problems and complexities, one of which we are exploring here today in terms of

making sure we get after fraud and abuse. And as we said many times on the committee, anyone who abuses this system, a sacred trust, ought to get the ultimate penalty. And I'm all for strengthening anything that we can do to further crack down on this.

What we've heard in your testimony today is a couple of things that strike me. Number one, we have a 13-percent increase overall with the baby boomers coming through the system, and yet you have had a 10-percent overall cut in your budget. One has to ask, how are you able to manage with these increases and the complexity of the problems that you face, including hacking?

Now, listen I am one of those people that would also concur that, hey, listen, some—you don't always—you know, cuts in service, if they are replaced by technology that is current, can overcome those things. But it seems to me like you're also saddled with legacy IT that needs to be updated and improved, and yet there aren't the resources that we funneled you to do that. Is that a fair assessment?

Ms. LACANFORA. You have cited some of our challenges, yes. I think I will mention, though, that we are embarking on a very ambitious IT modernization plan. We know that we cannot continue to operate the way that we are operating.

Mr. LARSON. When you say you are embarking on it, do you have the money for it? And where are we going? It seems like a lot of the problems and concerns that we are confronted with, especially in the area of veterans, et cetera—and I noticed the wristband concerns that were brought up in terms of identification—that if we have the resources, and certainly we have the technological capability, why wouldn't we protect what is the government's leading program to protect and assist its citizens? Could you—do you need more money?

Ms. LACANFORA. I think our budget folks are coming up to brief your staff on the 2018 budget, but I will say that the 2018 budget attempts to balance service and stewardship, as well as improving the efficiency with which we operate—the IT modernization plan that I mentioned is something that we are looking forward to advancing, and we're considering that to be an agency priority. So we are going to dedicate the funding to support that. Part of that will help us to modernize our communications infrastructure and remove the SSN from the remaining notices.

Mr. LARSON. What it is very alarming to us—and I know that my colleagues on the other side of the aisle share this as well—is that we know how vital this program is to all of our citizens. We know and everyone can attest to the long waits on disability in terms of processing claims. It seems the country, as gifted as we are with IT, this ought to be something that we ought to be able to solve rather easily. So it is further frustrating when we continue to see cuts in the budget and quite alarming today when we have the President's budget is revealed with about a $70 billion cut in Social Security, which, to me, is unconscionable, especially given the President's previous statements about preserving and saving, if not expanding, these benefits to keep pace actuarially where they should be from where we were in 1983, when we actually last looked at this from in a business actuarially sound position. I really believe that we can close a lot of these gaps with appropriate tech-

nology and assistance from the rank and file, who I would also note, according to testimony in previous hearings, that frontline members in Social Security offices are our best line of defense against fraud and abuse and waste. And they don't get enough credit. And continuing to cut the budget, instead of looking at investments in both IT and where we can be more efficient and successful, I think is where we need to go. Thank you.

Mr. RICE. Just to clarify, the President is not talking about cutting benefits. He's talking about cutting administrative costs.

Mr. Schweikert.

Mr. SCHWEIKERT. Thank you, Mr. Chairman.

Forgive me, who would be the most technical of all of you. All right. I need you to work through something with me and correct me if I'm not hearing something correctly. I have a BNC. I have a PUID. I have an MBI. I have an ICN. Are these all on a common registry that, a derivation table, that you tag in technology and you pull back and tag?

Mr. DEVRIES. No, sir

Mr. SCHWEIKERT. In that case, forgive me, and look, I've only been reading the testimony and the things here, but what I see is absurd technologywise. Without a common central token system—and forgive me, but if you use Apple Pay here, Apple Pay does not hold your credit card number. What it does is it creates a one-time-use token. The token hands off, matches, is handed back a number, reflects back. You all have IT budgets. You're trying to solve a problem, but in many ways—I need you to walk me through—it's my fear that the problem may have just gotten worse because I have the VA now with one set of numbers. I have Medicare with a different set of numbers. I have OPM with a different set. I'm now going to have Social Security with another blind identifier. Have we just made the problems much worse at least for the customer service aspect?

Mr. DEVRIES. Sir, if I could, let me address that to a limited degree here. What you just heard here was exactly the case. We took the one common field—it is called 9-digit Social Security number—that grew up for decades. It became ubiquitous in every form that we filled out. And then we said we can't show that, we can't display it out, we have to cut the use of that to where it is not publicly used——

Mr. SCHWEIKERT [continuing]. Blind it.

Mr. DEVRIES. We created a scheme for each of these things. I came from several years inside DOD. And so when I become a DOD member, I become a veteran at the end of that thing, yet I get a different number. Now I am a civil servant; I get a different number yet. How do we unite that thing? That's where we need the unification at the top there to help drive the standardization of these things and then how do you link them back, because, at the end of day, I still need to tie the different benefits that come at it from the various employment opportunities and——

Mr. SCHWEIKERT. Does everyone see what I'm observing is we may be actually, in our attempt to blind these numbers, creating another cascade effect that's going to create a whole new level of complication, and that is when my veteran happens to also be working on his Medicare, who also is dealing with a Social Security

dispute, that may be wanting to go back to work for the Federal Government at the Park Service, and now I have a handful of different numbers.

Off just the top of my head—and I'm on the edge of my technical expertise—I could come to you right now and, whether it be in a distributed ledger model, but some sort of common tokenization, where I hand this number, I get the hand off, and I would get a constant match. It wouldn't stop you all from doing what you're doing, but we would have to actually build a common unified clearinghouse data system that would reflect all the numbers and then hand back the one-time-use token. But that may be a unifying solution to solve actually a number of our problems, which is I can actually take you all the way to Social Security earned income tax credit fraud and a whole number of other things that could actually help on. Am I way out of my league here from your area of expertise? Am I seeing a unifying problem here?

Mr. DEVRIES. You are correct, sir. In my opening remarks, I talked about the program unique identifier. The concept there was to keep the Social Security number as the gold place. You protect that. You surround it, but you don't bring it out. And then you have programs, and so each of these could be a unique program. And they would have structures to their numbering schemes, and they own the numbering schemes, just like we talked about today here, but then it gets associated back to it, and that's what gets shared out. If his Medicare card gets confiscated or lost, we cut him a new one; it does not start the whole process.

Mr. SCHWEIKERT. Obviously, it would be easier if every time someone used a Medicare benefit, they had a chip card that handed off a new token, but the fact of the matter is you are not going to design the same thing where I type in this time the unique number; it hands off. It may be worth a conversation for those who are interested in this type of technology. Maybe as the committee here, we need to sort of—it is going to take some resources, but there has to be a unified theory we could get to make this simpler.

I yield back Mr. Chairman.

Mr. RICE. Thank you.

Ms. Kelly.

Ms. KELLY. Thank you, Mr. Chairman.

Social Security numbers have become used as a principal method of identity verification in and across agencies. However, that very fact makes them lucrative targets for identity thieves.

Mr. Wilshusen——

Mr. WILSHUSEN. Wilshusen.

Ms. KELLY. You testified that SSNs are particularly risky because they can, quote, "connect an individual's PII across many agencies' information systems and databases." Can you explain how the widespread use of Social Security numbers increases the risk of identity theft?

Mr. WILSHUSEN. Certainly. And thank you for the question. One of the reasons is that they are available, and if the numbers are not properly secured, they are vulnerable to theft. In our work on information security at Federal agencies, we looked at the examination of—or examined the security controls over the agency's information. We have often found that the security controls are not

effective to the extent to where they can adequately protect the confidentiality, integrity, and availability of the information and systems at those agencies. So, by having stores of Social Security numbers in a particular agency and they are not adequately protected, then that information can be stolen and used not only at that agency but can be used as an identifier for that individual at other agencies and indeed in the private sector as well.

Just last year, in fiscal year 2016, agencies reported about 8,300 incidents involving PII to the US–CERT for fiscal year 2016. So it's a present problem.

Ms. KELLY. How could the use of such an alternate identifier reduce the risk of identity theft?

Mr. WILSHUSEN. Well, for one, it may limit the extent to which an alternative ID may be used to identify that individual with other databases at other entities. So it's an opportunity to limit the extent that that identifier can be used across various different organizations.

Ms. KELLY. And you talked about in your testimony no such identifier was available. Can you expound on that?

Mr. WILSHUSEN. Well, there are other identifiers but none that's universally as accepted and applicable as the Social Security number. We did report that, in certain instances and at certain organizations, including DOD and VA or VHA, they've started to use an alternate identifier other than Social Security numbers to provide their members and require one.

Ms. KELLY. Despite OPM's failure to implement an alternate in 2008, the agency proposed a program unique identifier initiative in 2015 to provide an alternative way for identifying records in government systems.

Mr. DeVries, is that correct? And can you elaborate on that?

Mr. DEVRIES. Ma'am, could I get the last part of your question there?

Ms. KELLY. I asked about the proposed program unique identifier initiative in 2015 to provide an alternate way for identifying records in government systems. And can you elaborate on that?

Mr. DEVRIES. Yes, ma'am.

So, again, going back to, from a program perspective, if you define a program as being a functional area of interest, so like say CMS, VA, DOD and some other ones, there are benefits and other things that must get reported and attributed back to the individual. When I was born, I got a Social Security number. I went up and I worked as a teenager. I went to college. I started in the work force. Along the way, I accrued these different benefits. But each one gets recorded in their own way. So, by uniting—and kind of going with what we talked about before with a ledger that says here's the program owner for this numbering scheme and we standardize the numbering, then you can reuse those things. And, again, just as he pointed out, we would not—if you lose your Medicare card, you lose the connectivity of what that thing represented in the Medicare business but not across the whole financial institutions and all the other ones.

The challenge is, how do I work that thing not only at the Federal level at the agencies here but then down to the agencies that report into us and also to the State and local government things.

Because everything is coded into these various programs, the Social Security Administration talked about the number system she has. They keep on exploding when you go down to the State and local government side of the house too. And all those have to be linked together there at some point in time. But I think we can take it one phase at a time.

Ms. KELLY. I worked for the State of Illinois, and it was the same issue there. And I wonder, do States change it on their own one by one or how does that—do they decide to make changes? Because I think, before I left, they did can make some changes because they had Social Security numbers on everything.

Mr. DEVRIES. I'll let my esteemed colleagues talk here, but within the Department of Defense, where we have moved from moving away from Social Security numbers on all of our ID cards and so forth, that did not happen overnight. It came with putting out a standard, coming up with a schema, as we talked about, and then enforcing it.

Mr. RICE. Thank you Ms. Kelly.

Mr. Mitchell.

Mr. MITCHELL. Thank you, Mr. Chair.

Mr. Wilshusen, let me start with you. One of the things that I haven't seen referenced here is the use of Social Security numbers and the hacking that goes on with the IRS. It probably won't surprise you to know that I—among how many million others of Americans have had their Security number hacked for IRS purposes.

The solution to that was we'll issue a PIN number. So you get a PIN number mailed to you so you can file your taxes.

Do you know what happened this year on that?

Mr. WILSHUSEN. I understand that those PIN numbers were also compromised to some extent.

Mr. MITCHELL. They were. So I didn't get a PIN number.

I can only begin to describe to you the entertainment of trying to file my taxes, as well as I don't know how many other million of Americans, when in fact they don't have PIN numbers that will work either and they can't file electronically or any other way with their Social Security number.

The reason I raise it is the point that Mr. Schweikert raised, which is, if, in fact, rather than independent agencies creating their own identifiers, a PIN number, all of the acronyms—I don't know if anybody is watching this or will watch this tape, but most Americans, their eyes will glaze over with acronyms—the private sector has a variety of approaches to creating an identifier, a token system. I'm shocked, at this point, there hasn't been substantial conversations as to why we don't set a centralized process so someone can trigger that and create a token for not only benefits but when they pay their taxes. Why is that not a more active effort at this point in time rather than individual efforts?

Mr. WILSHUSEN. I think that's definitely a possibility. But I think you also touch upon the fact that these numbers, regardless of their provenance, if you will, need to be adequately protected by agencies in their information systems. And we have found traditionally that the security controls over agency systems need to be improved.

Mr. MITCHELL. Oh, I wouldn't disagree with you one bit.

You've got two issues. One is the user using their number and the agency securing it. And those are two separate dilemmas in the problem. But we seem to be making one harder by issuing all kinds of different identifiers, which in the case of the IRS, that was compromised as well.

So what's to prevent being compromised, this additional effort we've made and all the money we've put into it, rather than have an encrypted token-based system that allows you to do that? And that technology has existed in the private sector for a fair amount of time. So I would encourage the agencies to begin actively, and we should talk about it further, Mr. Chair, about how it is we actually encourage doing something that is integrated that secures it to a token system that's encrypted. At least protects that end, the user end.

If I can real quick, Mr. Oswalt, before my time runs out, I was looking through your testimony and listening to you—I returned a little late from the floor to hear everyone, and I apologize. There's some notations here that I guess troubled me a bit. VA is currently evaluating the elimination of Social Security numbers from correspondence.

I'm trying to find a polite way to word my response on that. It's nice that they're evaluating that. How long does it take VA to evaluate that?

Mr. OSWALT. Sir, since we began the SSN reduction effort, I mean, a number of correspondence and forms generally have been scrubbed. If there's a compelling business need for it, we would—it would remain. We have an SSN number review board that reviews things from a departmentwide standpoint. I can't attest right now—I can submit it for the record—what forms and letters, correspondence still has that. But as I said in my oral testimony——

Mr. MITCHELL. I've only got a couple minutes. Let me ask for the record that you do submit the number of forms, correspondence, and what their purpose is and what their justification is for the record.

Because I don't understand why it is on correspondence we are sending out, that we still put the Social Security number on there. And in fact, if we are putting the Social Security number, are we putting the whole Social Security number? My goodness gracious, guys.

Question number two for you, you made a comment about the Social Security numbers still being on their wristbands. Now, my guess is everybody in the room has been in the hospital for one purpose or another or been to a lab, and you get a wristband. I haven't seen a Social Security number on a wristband in a medical institution in close to a decade, maybe 7 years. Why in the world would you still put it on when they're hospitalized?

Mr. OSWALT. There is a barcoded SSN that allows the clinician to talk to a machine to the barcode. So that's used as a form of patient identification and verification. As I think I mentioned in my oral testimony, there's a pilot at a number of VA sites underway where we're using the last four. Eventually, we'll move away from the full human-readable SSN, and the integration control number, the ICN, will replace that.

Mr. MITCHELL. Thank you, Mr. Chair. I yield back.

Thank you, sir.

Mr. RICE. Thank you, Mr. Mitchell.

Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman. Thank you for having this hearing.

Ms. Jackson, I sat on the Ways and Means Health Subcommittee. We had extensive conversations with the Social Security agency about the process for removing Social Security numbers from Medicare cards. Hearing again about this process is enough to make your head spin. At the time we had this dialogue, it was quite clear that Social Security, quote-unquote, "did not have the funding to do this." That's what you said to us.

Now, can you explain how what seems like a pretty simple task of removing of Social Security numbers from Medicare cards can be such a challenge that CMS'—to the system that you use in terms of information technology? Tell me what's going on.

Ms. JACKSON. Thank you very much for the opportunity to speak to that.

We have, at CMS, been looking into the removal of the Social Security number from the Medicare card for a number of years. But it was not until Congress gave us the resources to be able to implement the system changes both in our internal systems and also in the data exchanges and the updates that we must do with the Social Security Administration, with the Railroad Retirement Board, who also use a HICN-based identification card, updating information in our internal systems as well as informing providers, healthcare providers, and Medicare beneficiaries about their need to use a new card when they both provide care on the healthcare provider side and for billing purposes and also when a beneficiary goes to receive care from their doctor or from their hospital.

To move forward with implementation of the Medicare beneficiary identifier, we have made system changes over the past couple of years. We hit a major milestone this past weekend in assigning new Medicare beneficiary identifiers to all Medicare beneficiaries, which now will allow us to begin the testing process with all of our systems and our data exchange partners to then be able to mail the card and begin the transition period.

We expect to have this completely implemented by April of 2019, with the beginning of mailing of cards in April of 2018.

The transition period for us is very important so that all stakeholders are able to receive the new MBI, submit bills and claims using the new MBI, and to assure that healthcare is still available and provided to Medicare beneficiaries.

Mr. PASCRELL. The new identifiers will be the same number as the past?

Ms. JACKSON. No. The new identifier, it's an 11-digit code. But it is an alphanumeric code that is randomly assigned—was randomly assigned when we did the enumeration over the weekend, and does not look anything like the current health insurance claim number.

Mr. PASCRELL. So we've done it with some resources, and you proved it could be done, and the system will be complete in 2019?

Ms. JACKSON. That's correct.

Mr. PASCRELL. Am I correct in saying that?

Ms. JACKSON. Yes.

Mr. PASCRELL. That's pretty big. And you're standing by that?

Ms. JACKSON. I am standing by that.

Mr. PASCRELL. Good.

Ms. JACKSON. We actually will be ready to receive the MBI on claim submissions by April of 2018.

Mr. PASCRELL. Thank you.

Mr. DeVries, in your testimony—where are you? Oh, there you are. Am I pronouncing that correctly, sir?

Mr. DEVRIES. Yes, sir.

Mr. PASCRELL. You stated that it was difficult to completely eliminate the Federal use of Social Security numbers without a governmentwide, coordinated effort and dedicated—you said—dedicated funding. That's what you said, right?

Mr. DEVRIES. Yes, sir.

Mr. PASCRELL. Okay. Can you explain how OPM would use additional funding to try to achieve the goal of limiting the Federal Government's use of Social Security numbers?

Mr. DEVRIES. In the case of OPM, where we exchange the important data between a Federal retiree with the Social Security and the IRS for tax purposes there, that underlying thing would still be coded and still be exchanging through the Social Security number. But, again, the communication that goes out to the Federal retiree benefit is a different number. We do in fact do that today for the retirement services, where you get a different control number when you become a Federal retiree. And that's how all action is tracked back to you.

In terms of the money to change the systems, it is—we're operating systems today, and, just as CMS probably experienced, you need an infusion of money to do coding and other changes and testing, as you prepare this parallel highway, if you will, of how we're doing it there.

Mr. PASCRELL. Thank you.

Mr. Chairman, may I just add this into the record? I heard from one of our members—and I need to correct the record—said that the President's budget does not cut Social Security benefits. But it does. In the budget, it cuts Social Security disability by up to $64 billion. I think the record needs to be corrected. And maybe the Congressman who said it needs to be corrected.

Mr. RICE. Thank you, sir.

Mr. Hurd.

Mr. PASCRELL. You're welcome. Thank you.

Mr. HURD. Thank you, Chairman.

Mr. Oswalt, I was confused by an earlier exchange. Do we know how many documents within the VA have the Social Security number printed on it?

Mr. OSWALT. We know what we know right now. It's an ongoing, expanding effort. There is a Social Security number reduction tool.

Mr. HURD. I get that. So, correct me if I'm wrong, there's a bunch of forms that the VA sends out. We should know how many those are. One of the data elements on that form is Social Security. Why does it take years to go through each form and delete that data element or not show it on the underlying form?

Mr. OSWALT. Sir, I would have to submit for the record the history of why it's taken so long. But there are a number of instances where it's in the——

Mr. HURD. Ms. Jackson, how many forms does your organization have that print the Social Security number on it?

Ms. JACKSON. With the implementation of the Medicare Beneficiary Identifier, we won't have any forms that will issue the Social Security number. Over the past couple of years, we——

Mr. HURD. So you're saying 2019 is when we're going to be successful in achieving that. Again, we currently, right now, there is X number of forms that produce, when they're printed out, on that form, it includes the Social Security number, correct?

Ms. JACKSON. No, sir. I'm sorry. I should have been clearer. Our correspondence with Medicare beneficiaries, we have truncated the Social Security number on all of that correspondence, with the exception of one document, which is our Medicare premium billing form. That still does include the health insurance claim number. I'm sorry. I can't remember if it is truncated. That will be the document that will be replaced with the MBI when we implement.

Mr. HURD. Great.

Ms. LaCanfora, how many forms does your organization produce that has the full Social Security number on it?

Ms. LACANFORA. Currently, we send out about 233 million notices or forms of correspondence each year that still have the Social Security number.

Mr. HURD. Is it that many unique, or is it five different kinds of correspondence?

Ms. LACANFORA. There's over a thousand separate types of notices.

Mr. HURD. So we have a thousand documents, and one of those elements, when it gets printed out, is Social Security number. Why can you not just delete that when you run a batch?

Ms. LACANFORA. So we have deleted the number or removed the number and replaced it with a beneficiary notice code on over a hundred million notices and we have another 42 million that we're doing in fiscal year 2018. The challenge that we have is twofold. One is that there are 60 separate disparate systems that produce those 1,000-plus notices. So the resources needed to make the changes are significant.

Beyond that, the other significant issue or challenge that we have is that the Social Security number was created to do business with our agency. And so, when we mail out a notice to someone and they, for example, are being told that they have an overpayment, they might pick up the phone and call us. And we have got to be able to quickly identify who they are and what their issues are.

Mr. HURD. Mr. DeVries, Estonia has done this. Estonia has moved to a system where it is a tokenization. Now, they're 1.3 million people, so the size of my hometown of San Antonio. A little bit different. But they've achieved the ability to have this interoperable number across all of their government agencies. We've talked about tokenization here. In your role with OPM, what do you need—ultimately, it's a shared service. And how do we implement a shared service at OPM when it comes to an identifier across all the Federal Government?

Mr. DEVRIES. Chairman Hurd, that's a great question. I'm not sure the exact answer, because what you're talking about is through the token and the bitchain type technology and so forth. That's the one I think that we need to work with industry closer on and bring that to the Federal Government side of the house, because it's not the same thing as it is on the industry side of the house. I'm desperately trying to reach out there for it. We're still stymied by how do you bring that technology in and infuse it into—it's really our application systems. It's not our hardware systems. It's the applications that are writing it and changing that.

Mr. HURD. Mr. Wilshusen, in the last 30 minutes of my time, you reference legacy IT being a barrier. What do we need to do in order to prevent that from being a barrier?

Mr. WILSHUSEN. Well, that's one of the problems in terms of with legacy systems. Often they may not be able to handle newer numbers. And so, in order to be able to do that, it requires significant system change or modification.

Mr. HURD. I yield back, Chairman.

Mr. RICE. Thank you, sir.

Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

I thank the witnesses for your help with the committee's work.

Mr. DeVries, back in 2015, I think it was July, OPM disclosed that its information technology systems had experienced a massive data breach, compromising the Social Security numbers, names, addresses, background information, birth dates, and the background investigation records for about 22 million people who had applied for sensitive positions with the FBI, CIA, NSA. And we had a hearing subsequent to that breach. And I actually asked your predecessor, Ms. Archuleta, I asked her if she was even taking the most rudimentary steps to protect Social Security numbers; are we even encrypting them within the system at OPM? And I was very sad to hear her testify that, no, at that time, in 2015, we were not encrypting. And I urged them to do that.

Then, a year later, we had a followup hearing with Ms. Cobert. I think she had some operational responsibility there. I asked her the same question a year later if that job was complete. She testified that, no, it was not complete.

And so we come full cycle here, and you're here. And I got to ask you: Now, Ms. Cobert said our system did not allow encryption of Social Security numbers. And I just want you to tell me something good. Tell me that we've encrypted these Social Security numbers. You know, it would be laughable if it wasn't so serious.

Mr. DEVRIES. It is serious.

Mr. LYNCH. I read an article last Sunday in The New York Times where a bunch of our sources in China are being killed off, either killed or imprisoned, U.S. sources, foreign intelligence sources. And, you know, I gotta think that—well, that hack was attributed to the Chinese Government. The hack actually came after—at least we found out about it after many of these people were executed in China for cooperating with the United States Government. They were shot as spies or imprisoned as spies. But you see, especially with sensitive information like this for secure positions, we're really exposing our personnel, our intelligence offi-

cers, and anyone who cooperates with them to grave, mortal threat. And so we've really got to step up our game here.

So let me go back to my question. Are we encrypting these Social Security numbers?

Mr. DEVRIES. Representative Lynch, yes, we are. Regarding the background investigations records incident, I have all the databases that contained the Social Security numbers and other PIs encrypted, with the exception of one database that resides in the mainframe, which is now sitting behind other security controls and detection systems. And that is scheduled for completion, which is a little bit more of a challenge because it's on the mainframe, to be completed this calendar year.

Mr. LYNCH. Okay. So we had this hack about 10 days ago, this ransomware attack. It was basically not stealing our information, but preventing people from utilizing that. Most of the impact was overseas. They tell me that that was because many of the—much of that software was bootlegged software, that Microsoft Windows—well, they bought it bootleg so that the fixes and all that were not available for those people. But are we—do you feel that we have major vulnerability from that type of hack as far as our user population goes?

Mr. DEVRIES. Sir, I would say yes. And I think that's the lowest common denominator that we all got to take steps to keep on educating, both the families at home as well as the workforce itself. Within OPM, there was no choice. Their systems are patched. That's a call that the Director supports, and I make it as the CIO, and I think that is the right approach to take, just as you would in any kind of corporation there.

Mr. LYNCH. All right.

Mr. Chairman, thank you for your courtesy. I yield back the balance of my time.

Mr. RICE. Thank you, sir.

Ms. Sánchez.

Ms. SANCHEZ. Thank you, Mr. Chairman.

And I want to thank the witnesses for being here with us today to talk about this important issue.

Identity theft affects over 12 million Americans per year, and it costs the victims just over $350 on average. That's on average. You hear cases of it taking people years and a lot more money to sort of get it straightened out. And I've been one of those people that have, unfortunately, been a victim of identity theft.

Social Security numbers and other personal information, like dates of birth, are—that information is very coveted by hackers who steal that personally identifiable information from breaches of the Office of Personnel Management, from health insurance companies, the United States Postal Service, and even retailers like Target. And while I'm encouraged with the Office of Management and Budget's initiative when they issued the 2007 memo calling for agencies to reduce collected and retained information and to strengthen the security of sensitive information, these recent hacks show that OPM and other agencies are still fundamentally very ill-prepared, and many Americans' sensitive information is still very vulnerable to attack.

That's why, you know, reducing the superfluous collection and retention of Social Security numbers is so important. It's troubling to see that, after 10 years, Government Accountability Office reports show that only 2 of 24 agencies examined met the requirements for a complete plan to reduce unnecessary usage of Social Security numbers. And it's even more troubling that the Office of Management and Budget has provided very little guidance to agencies to help with the transition. In addition, to exacerbate matters, the President's budget proposal guts agency personnel and operating budgets, further limiting their capacity to protect information and to improve their systems.

Whether it's a lack of funding or a lack of guidance, 10 years after the issuance of the memo, we should be in a better position to safeguard Americans' personal information.

And I know—I recognize that there are clear barriers that agencies face in reducing the collection of Social Security numbers. For example, in many cases, States mandate the collection of that information. I just wanted to note, before I delve into questions, that I think it's interesting that today we're discussing the progress of agencies to reduce the collection of Social Security numbers when tomorrow this same committee will be marking up a bill to add a new requirement on an agency to collect and verify Social Security numbers. So, on the one hand, we are saying, "Don't collect them and don't collect them superfluously," and then, on the other hand, we are going to be mandating the collection of that information. And I think it's both ironic and hypocritical of us on this dais to be doing both things.

But aside from that comment, Mr. DeVries, in the GAO's report, it mentions that OPM proposed using an alternate Federal employee identifier but withdrew that regulation because the identifier wasn't available. What are the barriers to creating a new identifier for Federal employees or for agencies to use in their administration of benefits?

Mr. DEVRIES. Representative Sánchez, thank you for that question. Again, I think the complexity or the barriers to overcome here is the size and complexity of the government. Just as the witnesses here at the table represent a few of the agencies, every agency really has a collection thing that kind of ties back to an individual and the benefits that get tied to it, whether it be their pay, their benefits, medical and so forth. How do you then create that architecture—and again, going back to what Chairman Hurd talked about, you would have to have that architecture in hand as you begin to even talk about the token to use or the other bitchain type stuff. How do you then promulgate that down? My colleague to my left here talked about how they rolled out the whole Medicare new number there. It is not done overnight. It's a process. It's based upon the architecture there.

Ms. SANCHEZ. And cuts in funding, how does that affect the ability to protect sensitive information effectively?

Mr. DEVRIES. So, in every agency, there is probably just enough dollars to make that go. When I am going to try and do something else, I have got to have that infusion to create something that goes alongside what I am currently operating and bring in something new. And I must turn off what I just got rid of.

Ms. SÁNCHEZ. Would you say that right now you are operating with the very best equipment that money can buy?

Mr. DEVRIES. No, ma'am.

Ms. SÁNCHEZ. Would you say that the equipment that you have to work with, on a scale of 1 to 10 in terms of modern and efficient, where would it lie on that scale?

Mr. DEVRIES. Ma'am, I would say, from an overall architecture and operating perspective, I would say it would be about a 0.3 or a 0.4.

Ms. SÁNCHEZ. So further budget cuts not necessarily helpful to rectifying that?

Mr. DEVRIES. No.

Ms. SÁNCHEZ. Thank you. No more questions.

Mr. RICE. Thank you, Ms. Sánchez.

The Federal Government needs to ensure it is doing all it can to protect Americans' identities and that Social Security numbers are not being used unnecessarily. While progress has been made, based on what we have heard today, there is still a long way to go.

Thank you to our witnesses for their testimony.

Thank you also to our members for being here.

With that, the subcommittee stands adjourned.

[Whereupon, at 3:35 p.m., the subcommittees were adjourned.]

[Questions for the Record follow:]

**House Ways and Means Committee,**
**Subcommittee on Social Security**
**and**
**HOUSE Oversight and Government Reform,**
**Subcommittee on Information Technology**
**Protecting Americans' identities: Examining Efforts to Limit the Use of Social Security Numbers**
**May 23, 2017**
**Hearing Deliverables**

Rep. Rice

**Question:**

What is VA's timeline for eliminating SSN from patient wristbands?

**Response:**

VA is aware of this requirement and is prioritizing this work in the development backlog. This plan to remove Social Security Numbers (SSNs) from patient wristbands is highly dependent upon the specific components of the new EHRM solution which still needs to be determined.

Rep. Mitchell

**Question:**

What is the current number of VA forms/correspondence with SSN?

**Response:**

VA currently has a total of 698 forms that require social security numbers. However, there is no distinction between the collection of full SSN and a truncated SSN, such as last 4. Use of the last 4 is important to help us uniquely identify the appropriate Veteran. In addition, VA decision notification letters include the Veteran's claim number which in many instances is the Veteran's social security number.

**Question:**

What is the justification for the continued use of Veteran SSN on VA forms/correspondence?

Response:

VA does not have a common, non-SSN identifier to match a Veteran or other claimant with his or her Federal or State agency records. In order to determine eligibility for benefits and healthcare, VA uses the Veteran's SSN to validate his or her military service with the Department of Defense as well as obtain copies of their records (i.e., service treatment records, personnel records, investigative reports, etc.) SSNs are

**House Ways and Means Committee,**
**Subcommittee on Social Security**
**and**
**HOUSE Oversight and Government Reform,**
**Subcommittee on Information Technology**
**Protecting Americans' identities: Examining Efforts to Limit the Use of Social Security Numbers**
**May 23, 2017**
**Hearing Deliverables**

required for locating a Veteran's Army or Air National Guard records with State Adjutant General Offices, confirming fugitive felon status with the Office of Inspector General, verifying a claimant's income with SSA and IRS for VA's pension and health care eligibility, etc. Other federal agencies also use SSNs for electronic data sharing with VA such as Department of Education data match to identify totally disabled Veterans eligible for waivers of school loans.

There are instances where the collection and use of SSNs are required to address a compelling business need. NCA's mission critical information systems require and retain personally identifiable information, including SSNs, to determine eligibility and document/track the provision of burial and memorial benefits. VA Forms request SSNs to identify an individual in order to ensure an accurate decision is made when determining eligibility for burial benefits. NCA considers the protection of SSNs and all personally identifiable information as critical. The VA systems from NCA have their records enumerated to the Master Veteran Index (MVI), establishing unique identifiers for NCA's Veterans, beneficiaries, and clients.

VHA must initially collect the SSN when a Veteran presents in order to uniquely identify the Veteran and link the Veteran's record to other VA, DoD and private health care records. Once a Veteran's record is established, a VA-specific unique patient identifier is established (the Integration Control Number or ICN). VA software applications continue to be updated to replace the use of SSN with ICN. Because the SSN is generally known by the patient and other identifiers are not, the SSN must continue to be used to ensure correct patient matching. In addition, SSN is needed when exchanging patient information with other Federal agencies and private health care providers that provide benefits and care to our patients to ensure patient records are appropriately matched for safe patient care. Our Master Veteran Index keeps the Veteran's SSN along with a link to the ICN and any unique identifiers from other care providers (Department of Defense and private health care sharing partners).

**House Ways and Means Committee,**
**Subcommittee on Social Security**
**and**
**HOUSE Oversight and Government Reform,**
**Subcommittee on Information Technology**
**Protecting Americans' identities: Examining Efforts to Limit the Use of Social Security Numbers**
**May 23, 2017**
**Hearing Deliverables**

Rep. Hurd

**Question:**

Why is VA taking so long to remove SSN from its forms/correspondence?

**Response:**

VA is currently seeking where appropriate to reduce the use of SSNs on forms/correspondence. VA must collect SSN when initially setting up services for Veterans. Without it, it is not possible to uniquely identify the Veteran and ensure that the patient's records are linked across all VA, DoD and private health care systems. Once in our system, we give each Veteran a unique identifier which is used to communicate within VA systems. There are still reasons why the SSN must be utilized. For example, VA uses SSN when connecting with private health care facilities as they do not know our internal unique identifier. In addition, some forms still include the last 4 of the SSN as that is a number Veteran knows readily and it ensures appropriate identification and record linkage. Further, services such as the VA Life Insurance assign their own file/policy numbers, which would be impossible without knowing the Veteran's SSN. When a Veteran is applying for life insurance, a SSN is the only way we may access their disability compensation file to ensure the qualification requirements for a new insurance policy are met. SSNs are also used for deceased Veterans to match with the Social Security Death Index, to locate next of kin and beneficiaries when policies of deceased Veterans have not been claimed. VA continues to reduce usage of full SSN within our information technology (IT) systems where possible.

# Congress of the United States

## U.S. House of Representatives

COMMITTEE ON WAYS AND MEANS
1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625
Washington, DC 20515-6348
http://waysandmeans.house.gov



June 21, 2017

David DeVries
Chief Information Officer
Office of Personnel Management
1900 E Street, NW
Washington, DC 20415

Dear Mr. DeVries:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security and the Committee on Oversight and Government Reform Subcommittee on Information Technology at the May 23, 2017 hearing entitled "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers." In order to complete our hearing record, I would appreciate your responses to the following:

1. How does the Office of Personnel Management (OPM) define necessary Social Security number (SSN) use?

2. Does the OPM maintain an inventory of its SSN use?

3. In 2006, the President's ID Theft Task Force charged OPM with developing methods for the reduction of SSN use and alternatives to the SSN for personnel purposes. What has OPM done to meet this responsibility?

4. In 2007, OPM issued guidance to federal agencies on how to minimize identity theft and protect SSNs. What is the status of this guidance, and when was it last updated?

5. What's the current status of the Program Unique Identifier initiative to reduce government-wide SSN use?

I would appreciate your responses to these questions by **July 5, 2017**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson

Sam Johnson
Chairman
Subcommittee on Social Security

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

**Questions for Mr. David DeVries**
Chief Information Officer
U.S. Office of Personnel Management

**Questions from Representative Sam Johnson**
Committee on Ways and Means
May 23, 2017, Hearing: "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers"

1. How does the Office of Personnel Management (OPM) define necessary Social Security number (SSN) use?

**Response:**

OPM's 2012 Information Security and Privacy Policy Addendum sets forth acceptable uses of the SSN and notes that any use for which the Addendum does not provide is considered unnecessary. Per the OPM policy, acceptable uses of the SSN are those that are authorized by law, are required for interoperability with organizations outside of OPM, or are required by operational necessity. Operational necessity refers to the inability to alter systems, processes, or forms due to costs or an unacceptable level of risk.

2. Does the OPM maintain an inventory of its SSN use?

**Response:**

OPM conducted a baseline inventory of SSN use by OPM in 2016, prior to my arrival. We are reviewing and updating the forms that request the SSN, in accordance with the applicable policies.

3. In 2006, the President's ID Theft Task Force charged OPM with developing methods for the reduction of SSN use and alternatives to the SSN for personnel purposes. What has OPM done to meet this responsibility?

**Response:**

In response to the ID Theft Task Force recommendations, OPM reviewed OPM-approved forms that are used across government in order to change, eliminate, or mask the use of SSNs. In addition, OPM issued guidance to other Federal agencies regarding SSN use in Federal employee records and explored options to establish a new employee identifier to replace SSNs in Federal

government human resource and payroll systems. In January 2008, OPM issued a notice of proposed rulemaking (NPRM) regarding the collection, use, and display of SSNs but subsequently withdrew that NPRM after evaluating comments received and determining that it would be impractical to issue the rule without an alternate government-wide employee identifier in place. More recently, OPM has been exploring the concept of developing and using program unique identifiers (PUID), which would be linked to the SSN but would protect the SSN by limiting its access and visibility.

4. In 2007, OPM issued guidance to federal agencies on how to minimize identity theft and protect SSNs. What is the status of this guidance, and when was it last updated?

**Response:** OPM's 2007 *Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft* (June 18, 2007) remains in effect.

5. What's the current status of the Program Unique Identifier initiative to reduce government-wide SSN use?

**Response:** OPM developed a proof of concept for the PUID initiative, which might reduce the Federal government's reliance on SSNs. In concept, the PUID would facilitate the collection and exchange of information across Federal government IT systems without continually duplicating and exposing the SSN, but still permit the unique identification of an individual. This is far more complex than the current practice of utilizing SSN's to link records, but bears further exploration. The project is currently inactive due to resource constraints. OPM cannot move from the proof of concept to conducting a pilot to review viability without additional resources and support.

Congress of the United States
U.S. House of Representatives
COMMITTEE ON WAYS AND MEANS
1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625
Washington, DC 20515-0518
http://waysandmeans.house.gov



June 21, 2017

Karen Jackson
Deputy Chief Operating Officer
Centers for Medicare and Medicaid Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Ms. Jackson:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security and the Committee on Oversight and Government Reform Subcommittee on Information Technology at the May 23, 2017 hearing entitled "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers." In order to complete our hearing record, I would appreciate your responses to the following:

1. How do the Centers for Medicare and Medicaid Services (CMS) define necessary Social Security number (SSN) use?

2. Does CMS maintain an inventory of its SSN use?

3. The new Medicare Beneficiary Identifier (MBI), unlike the Health Insurance Claim Number (HICN), will no longer be associated with the SSN. What flexibility does that allow CMS in issuing or reissuing MBIs? How does that compare to the flexibility CMS had with HICNs?

I would appreciate your responses to these questions by **July 5, 2017**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson

Sam Johnson
Chairman
Subcommittee on Social Security

**Karen Jackson's Hearing on**
**"SSN Removal"**
**W&M Social Security Subcommittee &**
**House OGR Information Technology Subcommittee**

**Chairman Sam Johnson**

1. **How do the Centers for Medicare and Medicaid Services (CMS) define necessary Social Security number (SSN) use?**

**Answer:** When the Medicare program was created in 1965, it was administered by the Social Security Administration. While CMS is now responsible for the management of Medicare, the Social Security Administration still enrolls beneficiaries, and both agencies rely on interrelated systems to coordinate Social Security and Medicare eligibility. Other than the use of SSNs in coordination with the Social Security Administration, CMS only collects and/or uses SSNs when a statute, regulation or an Executive Order provides legal authority to do so.

CMS is working to eliminate the unnecessary use of SSNs, in accordance with OMB Circular A-130, including by minimizing its use on mailings. To build on this work, CMS appreciates Congress's leadership in providing the direction and resources to undertake the important work of removing SSNs from Medicare cards. As you know, as required by MACRA, by April 2019, CMS will eliminate the use of beneficiaries' SSNs as the source of the primary identifier on Medicare cards and replace it with a new, unique Medicare Beneficiary Identifier (MBI), or Medicare number.

2. **Does CMS maintain an inventory of its SSN use?**

**Answer:** As required by OMB Circular A-130, CMS maintains an inventory of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII), and the SSN is PII.

3. **The new Medicare Beneficiary Identifier (MBI), unlike the Health Insurance Claim Number (HICN), will no longer be associated with the SSN. What flexibility does that allow CMS in issuing or reissuing MBIs? How does that compare to the flexibility CMS had with HICNs?**

**Answer:** Beginning in April 2018, all newly enrolled Medicare beneficiaries will receive a Medicare Card with the new Medicare Beneficiary Identifier, known as the MBI. At the same time CMS will begin distributing the new Medicare cards to current beneficiaries. This new Medicare number will have the same number of characters as the current 11-digit SSN-based Health Insurance Claim Number, known as the HICN, but will be visibly different and distinguishable from the HICN. With the introduction of the MBI, for the first time, CMS will have the ability to terminate a Medicare number and issue a new number to a beneficiary, in instances in which they are the victim of medical identity theft or their Medicare number has been compromised.

Transitioning to the MBI will help beneficiaries better safeguard their personal information by reducing the exposure of their Social Security numbers. CMS has already removed

Social Security Numbers from many types of communications, including Medicare Summary Notices mailed to beneficiaries on a quarterly basis. We have prohibited private Medicare Advantage and Medicare Part D prescription drug plans from using SSNs on enrollees' insurance cards.

Congress of the United States
U.S. House of Representatives
COMMITTEE ON WAYS AND MEANS
1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625
Washington, DC 20515-6348
http://waysandmeans.house.gov



June 21, 2017

Marianna LaCanfora
Acting Deputy Commissioner
Office of Retirement and Disability Policy
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235

Dear Ms. LaCanfora:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security and the Committee on Oversight and Government Reform Subcommittee on Information Technology at the May 23, 2017 hearing entitled "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers." In order to complete our hearing record, I would appreciate your responses to the following:

1. How does the Social Security Administration (SSA) define necessary Social Security number (SSN) use?

2. Aside from the Social Security card, please provide examples of when it would be necessary to include a full SSN in correspondence.

3. Does the SSA maintain an inventory of its SSN use?

4. In 2014, the SSA created a clearinghouse for best practices in SSN reduction. While 25 agencies were registered users of this site at the time, the site is no longer available. Please provide additional details about this clearinghouse including its history, the identified best practices, and why the SSA no longer provides this resource.

5. Last year, the SSA mailed approximately 230 million documents with a full SSN. How many now include a Beneficiary Notice Code (BNC) instead? When will the BNC finally replace the SSN for most mailed documents?

I would appreciate your responses to these questions by **July 5, 2017**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson

Sam Johnson
Chairman
Subcommittee on Social Security

**Committee of Ways and Means, Subcommittee on Social Security**
**Hearing on Efforts to Limit the Use of the Social Security Numbers – May 23, 2017**
**Questions for the Record**

**1. How does the Social Security Administration (SSA) define necessary Social Security number (SSN) use?**

To determine if SSN use is necessary, we follow our obligations under the Privacy Act (5 U.S.C. § 552a(e)(1)), which are reiterated in our privacy regulations (20 C.F.R. § 401.30(b)(1)) promulgated in accordance with the Social Security Act (42 U.S.C. § 1306). Specifically, the Privacy Act and our privacy regulations provide that we will only maintain records that are "relevant and necessary to accomplish a purpose…required to be accomplished by statute or by executive order."

As authorized by law, we developed the SSN specifically to allow employers to uniquely identify, and accurately report, an individual's earnings covered under the Social Security program. Accordingly, the SSN is essential to how we maintain records to support these programs. The SSN allows us to post over 275 million earnings items to individuals records each year in order to administer current and future program benefits. In fiscal year 2017 alone, we expect to pay more than $940 billion to Social Security beneficiaries to approximately 62 million beneficiaries and nearly $55 billion in Federal benefits to a monthly average of approximately 8 million SSI recipients. Without the SSN, we could not administer these vital benefits.

**2. Aside from the Social Security card, please provide examples of when it would be necessary to include a full SSN in correspondence.**

Other than on the SSN card, the full SSN is not necessary on correspondence, and we will be removing the SSN from our remaining notices as we modify existing notices or develop new ones.

However, the SSN is critical to the operation of our programs. Accordingly, we must continue to collect and use the SSN on certain documents and forms, such as benefit and representative payee applications, remittances, and, as you noted, SSN cards. Removing the number from these documents would disrupt automated scanning processes that allow us to handle large workloads efficiently, and would result in us reverting to manual, labor-intensive data entry processes.

**3. Does the SSA maintain an inventory of its SSN use?**

We maintain an inventory of all personally identifiable information (PII), which includes the SSN, in our systems. Additionally, our Systems of Record Notice, which is publicly available, documents the systems that use SSNs.

**4. In 2014, the SSA created a clearinghouse for best practices in SSN reduction. While 25 agencies were registered users of this site at the time, the site no longer is available. Please provide additional details about this clearinghouse including its history, the identified best practices, and why the SSA no longer provides this resource.**

We implemented the clearinghouse for best practices in SSN reduction in two steps:

- First, we formed the SSN Best Practices Collaborative, which included representatives from 36 Federal departments and agencies and met regularly in 2007 to explore, develop, and share best practices for reducing reliance on SSNs. Upon implementation of the online clearinghouse, it was determined the Collaborative no longer needed to meet. However, the Collaborative formed a subcommittee chaired by the Internal Revenue Service (IRS) and comprising agencies that handle high volumes of SSNs and personally identifiable information (PII), such as the Department of Defense, Department of Veterans Affairs, Department of Homeland Security, Centers for Medicare and Medicaid Services (CMS), and us.

- The online clearinghouse was established in July 2007 on a bulletin board website. As you mentioned, at that time, over 25 agencies were registered to use the site. The clearinghouse provided a forum for agencies to share materials regarding SSN use and display by Federal agencies. It highlighted best practices as well as contacts for specific programs and initiatives.

As you know, the clearinghouse website is no longer available. Unfortunately, our current records do not shed light on exactly when the clearinghouse became inactive, or what became of the identified best practices.

However, we appreciate the momentum created by this hearing and plan to use it as a springboard for renewed inter-agency discussion and collaboration. Moving forward, we believe an ideal way for us to assist other agencies in reducing SSN use would be through the Communities of Practice (COPs) we lead on Data Exchange and Improper Payments. These COPs provide, among other things, a forum to share best practices. We will include safeguarding data, including the SSN, and reducing the unnecessary use of the SSN as topics for discussion and collaboration. Currently, 45 Federal agencies are represented in these COPs. In addition, we will continue to support CMS and IRS in their respective efforts to remove the SSN from Medicare cards and to allow truncated SSNs on Forms W-2 issued to employees.

**5. Last year, the SSA mailed approximately 230 million documents with the full SSN. How many include Beneficiary Notice Code (BNC) instead? When will the BNC finally replace the SSN for most mailed documents?**

We removed the full SSN from two of our largest annual workloads—the S*ocial Security Statement* and the Social Security Cost of Living Adjustment (COLA) notice. These notices typically account for about one-third of our notices. The *Statement* only displays the last four digits of the SSN. The Social Security COLA notice only displays the BNC.

The remaining two-thirds—approximately 230 million notices—still contain the SSN. In 2018, we plan to replace the SSN with the BNC on benefit verification letters, as well as appointed representative and Social Security post-entitlement notices. Together, these mailings account for approximately 42 million annual notices, or nearly 20 percent of the remaining notices with an SSN. Additionally, as part of our Information Technology (IT) modernization efforts, we will modernize our complex notice infrastructure, comprising over 1,000 different notice types. While we do not have a set timeframe for completion, we are committed to leveraging our modernization effort to replace the full SSN with the BNC on a flow basis on our remaining notices.

# Congress of the United States

## U.S. House of Representatives

COMMITTEE ON WAYS AND MEANS

1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625

Washington, DC 20515-0518

http://waysandmeans.house.gov



June 21, 2017

John Oswalt
Executive Director for Privacy
Office of Information and Technology
Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Mr. Oswalt:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security and the Committee on Oversight and Government Reform Subcommittee on Information Technology at the May 23, 2017 hearing entitled "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers." In order to complete our hearing record, I would appreciate your responses to the following:

1. How does the Department of Veterans Affairs (VA) define necessary Social Security number (SSN) use?

2. Please provide examples of when it would be necessary to include a full SSN in correspondence.

3. Does the VA maintain an inventory of its SSN use?

4. In your written testimony, you noted that IT solutions to eliminate SSN use can only occur after conducting an "integrated and comprehensive review of SSN use." Has the VA undertaken such a review? If not, why not?

5. The VA has developed the Integrated Control Number (ICN) as a unique identifier for patients. In what ways can the ICN be used as an SSN replacement?

6. Why does the VA use the SSN for patient identification purposes? In what instances does the VA use a full SSN and how does the VA ensure that these SSNs are protected?

7. When the Veterans Health Administration (VHA) uses SSNs, for instance on patient wristbands and IV bag labels, how does the VHA track these instances to ensure that the SSNs are properly disposed of following use?

I would appreciate your responses to these questions by **July 5, 2017**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson

Sam Johnson
Chairman
Subcommittee on Social Security

**Department of Veterans Affairs (VA) Response to Questions for the Record House Oversight and Government Reform, Subcommittee on Information Technology Hearing: Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers**

**May 23, 2017**

1. **How does the Department of Veterans Affairs (VA) define necessary Social Security number (SSN) use?**

   **VA Response:** The SSN is used to identify employees for employment-related record keeping. It is used for Veterans and their dependents to ensure accurate identification for VA healthcare and benefits. Positive identification of Veterans is necessary in order to avoid mistaken identity, which can be catastrophic in healthcare delivery.

2. **Please provide examples when it would be necessary to include a full SSN in correspondence.**

   **VA Response:** The full SSN is used for Veterans Benefits Administration (VBA) correspondence since a large amount of mail is returned due to incorrect addresses. The full SSN is needed so that VBA staff can accurately look up and positively identify the Veteran in their system. It is not possible to establish identity using only name and date of birth (DOB) since there are many Veterans with similar names and matching DOBs.

3. **Does the VA maintain an inventory of its SSN use?**

   **VA Response:** Veterans Health Administration (VHA) maintains an inventory of its SSN use. The Veterans Administration Systems Inventory (VASI) office also maintains an inventory of Personally Identifiable Information (PII) which includes SSN use.

4. **In your written testimony, you noted that IT solutions to eliminate SSN use can only occur after conducting an "integrated and comprehensive review of SSN use." Has the VA undertaken such a review? If not, why not?**

   **VA Response:** VHA already collects and maintains an SSN use inventory database. VA is developing a new SSN Reduction tool to inventory SSN use and full deployment is expected throughout VA by September 2017.

5. **The VA has developed the Integrated Control Number (ICN) as a unique identifier for patients. In what ways can the ICN be used as an SSN replacement?**

**Department of Veterans Affairs (VA) Response to Questions for the Record House Oversight and Government Reform, Subcommittee on Information Technology Hearing: Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers**

**May 23, 2017**

**VA Response:** The VA's Master Veteran Index Integration Control Number (ICN) is an enterprise level unique person identifier assigned to every person of interest to the VA and was developed in accordance with the ASTM 1714 standard for Unique Healthcare IDs (UHIDs). As such, the ICN can be used within VA electronic systems, as well as externally, such as on correspondence, to uniquely identify a patient. The ICN is, on rare occasion, changed for a person, in the event that a duplicate or other anomaly is found. Thus, it is generally not recommended that the ICN is used externally on more permanent formats, such as ID cards. However, although the ICN is not used directly on cards for this reason, it is correlated to other unique identifiers (such as the ID card number) used within VA and external agencies to ensure appropriate linkage and patient identification.

The Master Veteran Index (MVI) Technical team recommends that the ICN not be used on more permanent formats including ID cards as there is a small chance the ICN can change over time under certain conditions. For example, if duplicate identity records are found for a person, one of those records will be deprecated and all information on that identity combined into the retained ICN, leaving references to the "old" deprecated ICN invalid. The Card ID is used to manage the issuance and tracking of the cards themselves, and is unique to the specific card, not unique to the patient identity.

6. **Why does the VA use the SSN for patient identification purposes? In what instances does the VA use a full SSN and how does the VA ensure that these SSNs are protected?**

**VA Response:** According to The Joint Commission (TJC), two patient identifiers are required to reliably identify individuals for whom services and treatment are intended, and to reliably ensure the services and treatment match the person for which they are intended. In addition, patient medical records must have a unique medical record number for identification of the patient within the record system. Historically, VHA policies have required the SSN as part of the patient's identifying traits as well as the medical record number. For example, in October of 2013, the National Center for Patient Safety published guidance on information required on VA wristbands: 1) Patient's Full Name, 2) Full SSN, and 3) Bar Code of SSN. Also, VHA Chief Business Office (now Office of Community Care) policy change dated November 2013 required full name, SSN, and a bar code of the SSN be printed on the patient wristband to ensure appropriate patient identification in a human readable format. However, VHA SSN Reduction and

**Department of Veterans Affairs (VA) Response to Questions for the Record House Oversight and Government Reform, Subcommittee on Information Technology Hearing: Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers**

**May 23, 2017**

Elimination Initiative seeks to reduce or eliminate the use of SSNs as the forward-facing unique identifier in VHA systems, processes, and forms as part of the government-wide effort to reduce the exposure of PII.

Below are examples (not exhaustive) of how VHA uses the full SSN:

a. Enrollment for healthcare
b. Positive patient identification
c. Computer matching agreements with other federal agencies (e.g., IRS and SSA)
d. Health information exchange with community partners (e.g., Virtual Lifetime Electronic Health Record)
e. Collection of co-pay claims

All VA workforce members are required to take annual privacy and security training. Staff is reminded to safeguard protected health information and personally-identifiable information (e.g., the SSN).

7. **When the Veterans Health Administration (VHA) uses SSNs, for instance on patient wristbands and IV bag labels, how does the VA track these instances to ensure that the SSNs are properly disposed of following use?**

**VA Response:** VHA does not have a tracking system to know when patient wristbands and IV bags labels are destroyed. Each respective VA Medical Center (VAMC) is responsible for developing a local policy for destruction of sensitive material to include paper and biohazardous waste materials. The common practice at VAMCs is for the IV bag labels and patient wristbands, unless kept by the patient, to be placed in the incinerator or biohazardous bags and autoclaved.

Congress of the United States
U.S. House of Representatives
COMMITTEE ON WAYS AND MEANS
1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625
Washington, DC 20515-0518
http://waysandmeans.house.gov



June 21, 2017

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security and the Committee on Oversight and Government Reform Subcommittee on Information Technology at the May 23, 2017 hearing entitled "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers." In order to complete our hearing record, I would appreciate your responses to the following:

1. The Government Accountability Office (GAO) found that some agencies had inventories of Social Security number (SSN) use while others did not. Why are these inventories so important for SSN reduction efforts and what information do these inventories need to capture?

2. GAO found the implementation of the OMB SSN reduction and reporting mandate was inconsistent across the government. Did GAO identify the cause of this inconsistency, and if so, how can consistency be improved?

3. What best practices was the GAO able to identify for reducing the use of SSNs and which agencies, if any, employed them?

I would appreciate your responses to these questions by **July 5, 2017**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to mm.russell@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

Sam Johnson
Chairman
Subcommittee on Social Security

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 5, 2017

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

**Subject: GAO Response to Post-Hearing Questions on Reducing Social Security Number Use**

Dear Mr. Chairman:

It was a pleasure to appear before your Subcommittee on May 23, 2017 to discuss federal efforts to reduce the use of Social Security numbers.[1] This letter responds to a request that I provide answers to post-hearing questions for the record. The questions, along with my responses, follow.

1. **The Government Accountability Office (GAO) found that some agencies had inventories of Social Security number (SSN) use while others did not. Why are these inventories so important for SSN reduction efforts and what information do these inventories need to capture?**

Developing a baseline inventory of systems that collect, use, and display SSNs, and ensuring that the inventory is periodically updated, are important for SSN reduction efforts because such an inventory can assist agencies in maintaining an awareness of the extent of their collections, and progress in eliminating unnecessary use of the numbers. Without such an inventory, agency managers might not be aware of systems they operate that continue to unnecessarily collect, use, or display SSNs. Further, maintaining such an inventory would enable agencies to report to the Office of Management and Budget (OMB) on the numbers of systems they maintain that contain SSNs. This, in turn, would enable OMB to better measure progress in eliminating the unnecessary collection and use of these numbers across the government.

The baseline inventory should capture information identifying the name of each of the agency's systems and, for each system, the approximate number of individual records containing SSNs. This information would be useful for measuring the extent to which SSNs are collected, stored, and displayed by the agency's systems, and for enabling agencies to prioritize their plans for possible reduction efforts by identifying which systems affect the greatest numbers of individuals.

[1]GAO, *Social Security Numbers: OMB and Federal Efforts to Reduce Collection, Use, and Display*, GAO-17-655T (Washington, D.C.: May 23, 2017).

**2. GAO found the implementation of the OMB SSN reduction and reporting mandate was inconsistent across the government. Did GAO identify the cause of this inconsistency, and if so, how can consistency be improved?**

Our review found that a lack of clear direction and ineffective monitoring by OMB contributed to the inconsistent SSN reduction efforts and incomplete status reporting on those efforts across the federal government. When OMB directed agencies to develop plans for the elimination of unnecessary collection and use of SSNs in May 2007, it did not set requirements for how agencies were to create effective plans or what elements the plans should contain. For example, OMB did not specify that agencies should identify in their plans, performance goals and indicators, measurable activities, timelines for completion, or specific roles and responsibilities. Due to the lack of guidance from OMB, many agencies' SSN reduction plans did not include these key elements, calling into question their usefulness in determining the overall progress agencies had achieved.

Further, regarding the annual progress updates that agencies were required to submit, OMB's guidance did not establish the specific performance measures on which agencies were to report. Without such performance measures, OMB had little basis to monitor the implementation of agencies' reduction efforts or determine whether agencies had achieved their goals in eliminating the unnecessary collection and use of SSNs. Our review determined that 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. Without such information, determining whether additional actions could be taken to minimize the risk of unnecessarily exposing SSNs to identity theft is difficult.

Based on our assessment of these issues, we are making recommendations to OMB in our draft report. Specifically, OMB could better ensure the consistency and effectiveness of SSN reduction efforts by:

- specifying elements that agency plans for reducing the unnecessary collection, use, and display of SSNs should contain and requiring all agencies to develop and maintain complete plans;
- requiring agencies to modify their inventories of systems containing personally identifiable information to indicate which systems contain SSNs and use the inventories to monitor their reduction of unnecessary collection and use of SSNs;
- providing criteria to agencies on how to determine unnecessary use of SSNs to facilitate consistent application across the federal government;
- taking 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 Federal Information Security Modernization Act of 2014 reports; and
- establishing performance measures to monitor agency progress in consistently and effectively implementing planned reduction efforts.

**3. What best practices was the GAO able to identify for reducing the use of SSNs and which agencies, if any, employed them?**

We identified several effective SSN reduction practices based on information obtained from the 24 Chief Financial Officer Act agencies' responses to our questionnaire about the steps they had taken to reduce the unnecessary collection, use, and display of SSNs. These practices and the agencies that employed them include:

- **Developing and using alternate identifiers**. Officials from the Departments of Defense, Veterans Affairs, Health and Human Services, and Education 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.
- **Removing SSNs from printed forms and other physical displays**. Even when SSNs continue to be used as identifiers within internal information systems, three agencies reported taking steps to mask, truncate, or block the display of these numbers on paper forms, correspondence, and computer screens. The Social Security Administration, the Internal Revenue Service, and the Department of Veterans Affairs provided examples of instances in which they had successfully taken these actions.
- **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 email traffic for the numbers and blocking the numbers' transmittal. Specifically, the Bureau of Economic Analysis within the Department of Commerce reported that it implemented a filter on its email system to block both incoming and outgoing emails containing SSNs. In addition, the Department of Justice reported that it upgraded its data loss prevention capabilities to automatically block email traffic to external, nongovernment users when an SSN is detected either in the body of an email or in an email attachment.

In addition to these specific practices, agencies also reported reviewing their ongoing collection, use, and display of SSNs and setting restrictions on access to SSNs and other personally identifiable information. All of these practices can contribute to limiting the exposure of SSNs to potential compromise.

---

In preparing this correspondence, we relied primarily on our draft report on OMB's and federal agencies' efforts to reduce the collection, use, and display of SSNs. The draft report is currently undergoing internal review, and we anticipate issuing the final report this month. Should you or your staff have any questions on matters discussed in this letter, please contact me at (202) 512-6244, or John de Ferrari, Assistant Director, at (202) 512-6335. We can also be reached by e-mail at wilshuseng@gao.gov and deferrarij@gao.gov, respectively.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues



[Submissions for the Record follow:]

AJRR American Joint Replacement Registry
Improving Orthopaedic Care Through Data

9400 West Higgins Road, Suite 210
Rosemont, IL 60018-4975

847-292-0530 | fax 847-292-0531 | www.ajrr.net

June 5, 2017

Chairman Sam Johnson
House Ways and Means Social Security Subcommittee

Ranking Member John Larson
House Ways and Means Social Security Subcommittee

Chairman Will Hurd
House Oversight and Government Reform Information Technology Subcommittee

Ranking Member Robin Kelly
House Oversight and Government Reform Information Technology Subcommittee

Dear Chairmen Johnson and Hurd and Ranking Members Larson and Kelly,

The American Joint Replacement Registry (AJRR) is an independent national total joint replacement registry with over one million hip and knee replacement and revision procedures in its database. AJRR's mission is to improve orthopaedic care through the collection, analysis, and reporting of actionable data. Undisrupted access to patient data is necessary for AJRR to help providers improve patient outcomes and quality of care. AJRR is writing to express concern over the planned enactment of the Center for Medicare and Medicaid's Social Security Number Removal Initiative (SSNRI). While we recognize that identity theft is a serious threat, efforts to reduce or restrict the use of social security numbers by patients present unique obstacles to the operations of a registry such as AJRR.

Under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), the Centers for Medicare and Medicaid Services (CMS) must remove all social security numbers from Medicare beneficiary cards by April 2019. A new Medicare Beneficiary Identifier number (MBI) will replace the current social security-based Health Insurance Claim Numbers (HICNs). With a transition period lasting from April 1, 2018 through December 31, 2019, the SSNRI requires CMS to have completely mailed out all replacement cards to enrollees by April 2019. All stakeholders submitting transactions based on the patient's HICN must modify their systems and processes by April 2018.

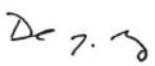
The SSNRI poses a challenge to a registry's data validation processes by potentially disrupting the development of crucial longitudinal data. While AJRR appreciates that CMS will be developing a "lookup tool" for providers, we believe it is critical that this tool be available as early as possible. It is important to ensure uninterrupted access to this data for other stakeholders as registries' access to patients' social security numbers play a vital role in their operations. Any disruption in our data validation methods would jeopardize the Registry's ability to keep track of outcomes.

Conversion to a system which operates on MBI rather than HICN will require providers to devote resources and time to adjusting their workflow. Interruptions caused by unforeseen factors, as well as those mentioned above, could impede effective tracking of procedure outcomes.

Although AJRR understands and shares Congress's concerns about the risks of identity theft, the solution should not jeopardize patient safety and care.

Please feel free to contact Jeffrey Knezovich, Executive Director, AJRR at 847-292-0530 or knezovich@ajrr.net should you have any questions or comments.

Sincerely,



Daniel J. Berry, MD
Chair
American Joint Replacement Registry

cc:
Jeffrey P. Knezovich, CAE, Executive Director
David G. Lewallen, MD, Medical Director

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 22, 2017

The Honorable Sam Johnson, Chairman
The Honorable John Larson, Ranking Member
House Committee on Ways & Means
Social Security Subcommittee

The Honorable William Hurd, Chairman
The Honorable Robin Kelly, Ranking Member
House Committee on Oversight and Government Reform
Subcommittee on Information Technology

Dear Chairman Johnson, Chairman Hurd, Ranking Member Larson, and Ranking Member Kelly:

We write to you regarding the hearing "Joint Oversight Hearing on Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers."[1] EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has participated in the leading cases involving the privacy of the Social Security Number ("SSN") and has frequently testified in Congress about the need to establish privacy safeguards for the SSN to prevent the misuse of personal information.[2] EPIC also maintains an archive of information about the SSN online.[3]

---

[1] *Joint Oversight Hearing on Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers*, 115th Cong. (2017), H. Comm. on Ways and Means, Subcomm. on Social Security and H. Comm. on Oversight and Gov't Reform, Subcomm. on Information Tech., https://waysandmeans.house.gov/event/joint-oversight-hearing-protecting-americans-identities-examining-efforts-limit-use-social-security-numbers/ (May 23, 2017).

[2] *See, e.g., Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993) ("Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling"); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994) ("the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs"); Marc Rotenberg, EPIC, *Testimony at a Hearing on Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough", Before the S. Special Comm. on Aging*, 114th Cong. (Oct. 7, 2015), *available at* https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf; Marc Rotenberg, EPIC, *Testimony at a Hearing on Protecting the Privacy of the Social Security Number from Identity Theft, Before the H. Ways & Means Subcom. on Social Security*, 110th Cong. (June 21, 2007), *available at* https://epic.org/privacy/ssn/idtheft_test_062107.pdf; Marc Rotenberg, *Testimony at a Joint Hearing on Social Security Numbers & Identity Theft, Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001), *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Chris Jay Hoofnagle, EPIC, *Testimony at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the H. Ways & Means Subcom. on Social Security*

We appreciate your Subcommittees' interest in SSN privacy issues. It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater risk to personal privacy. The use of the number for identification poses an ongoing risk of identity theft, financial fraud, and other forms of crime.

**Social Security Number History and the Importance of Limiting SSN Collection**

The Social Security Number is the classic example of "mission creep," a program designed for a specific, limited purpose has been transformed for additional, unintended purposes, often with disastrous results. The pervasiveness of the SSN and its use to both identify and authenticate individuals threatens privacy and financial security.

These risks associated with the expanded use of the SSN underscore the importance of the hearing today. But this problem has been well known to Congress for many years.

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the SSN that show a striking resemblance to the problems we face today. Although the term "identify theft" was not yet in use, a detailed report, prepared by Willis Ware and technical experts and legal scholars, made clear the risks from the expanded use of the SSN.[4]

The Report of the Ware Commission provided the cornerstone of the landmark Privacy Act of 1974. In enacting the Privacy Act, Congress recognized the dangers of widespread use of SSNs as universal identifiers, and included provisions to limit the uses of the SSN. The Act makes it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN. Section 7 of the Privacy Act specifically provides that any agency requesting that an individual disclose his or her SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it."[5] This section reflects a presumption that the SSN should not be used for recordkeeping purposes unrelated to Social Security and taxation. In its report supporting adoption of Section 7, the Senate Committee stated that the widespread use of the SSN as a universal identifier in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation."[6]

Since passage of the Privacy Act, concern about SSN confidentiality and misuse has become even more compelling. The SSN is central to identity theft in the United States. In 2016,

---

*& the H. Judiciary Subcom. on Immigration, Border Sec. & Claims*, 105th Cong. (Sept. 19, 2002), *available at* http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[3] Social Security Numbers, EPIC, https://epic.org/privacy/ssn/.

[4] Department of Health, Education, and Welfare (HEW), *Records Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973) (Ware Commission report), available at https://www.epic.org/privacy/hew1973report/.

[5] Privacy Act of 1974, 5 U.S.C. § 552 (a) (2006).

[6] S.Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6943.

almost 30% of identity theft complaints received by the FTC were incidents of tax fraud.[7] In 2015, it was announced that the Office of Personnel Management was the target of one of the worst data breaches in US history. The breach compromised the personal information of over 21.5 million individuals, including social security numbers and fingerprints.[8] Also in 2015, taxpayer data for over 610,000 Americans, including SSNs, was stolen from the Internal Revenue Service.[9]

**Solutions to Prevent the Misuse of SSNs and Identity Theft Risks**

EPIC favors technological innovation that enables the development of context-dependent identifiers. Such a decentralized approach to identification is consistent with our commonsense understanding of identification. If you're going to do banking, you should have a bank account number. If you're going to the library, you should have a library card number. If you are enrolled in a university, you should have a student ID number. Utility bills, telephone bills, insurance, the list goes on. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number gets compromised, all the numbers are not spoiled and identity thieves cannot access all your accounts. All your accounts can become compartmentalized, enhancing their security.

**Conclusion**

The reality is that today the SSN is the key to some of our most sensitive and personal information, and it is more vulnerable than ever. Given the growing risk of identity theft coupled to the SSN and the ease of alternative systems, there is simply no excuse for the use of SSNs in either the public or private sector. *The need to find a solution to the problem of the widespread use of the SSN is critical.*

We ask that this statement be entered in the hearing record. EPIC looks forward to working with the Subcommittees on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

---

[7] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY – DECEMBER 2016 12 (2017), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf.

[8] Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," NY Times (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

[9] Lisa Rein, "IRS says breach of taxpayer data far more widespread than it first thought: 610,000 taxpayers at risk," Wash. Post (August 17, 2015), http://www.washingtonpost.com/blogs/federal-eye/wp/2015/08/17/irs-says-breach-of-taxpayer-data-far-more-widespread-than-it-first-thought-610000-taxpayers-at-risk/.

NATIONAL COUNCIL OF NONPROFITS
National voice. State focus. Local impact.

Statement of the
National Council of Nonprofits

Before the
House Ways and Means Social Security Subcommittee and
House Oversight and Government Reform Information Technology Subcommittee

Hearing on
Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers

May 23, 2017

Chairmen Johnson and Hurd, Ranking Members Larson and Kelly, and members of the Subcommittees, I write on behalf of the National Council of Nonprofits to share background materials relevant to the subject of today's hearing, "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers."

We understand that the hearing is focusing on efforts by federal agencies to reduce the use of Social Security numbers (SSNs) and the security challenges facing these agencies. The thousands of charitable nonprofits that my organization represents wholeheartedly support the reduction in the use of SSNs, both in their own operations and by government. As the Members of the Subcommittee hear testimony today on progress within the departments and agencies represented by the witnesses, we ask that you also recognize that the need for vigilance is not limited to reducing existing usage of SSNs, but can arise in new and unexpected ways. The brief story of the Gift Substantiation Proposed Regulation from the Internal Revenue Service is one such "out of the blue" proposal that shows that all of us inside and outside of government must remain vigilant to protect American's identities.

The IRS Gift Substantiation Proposed Rule
in September 2015, the Treasury Department and Internal Revenue Service published proposed regulations (IRS REG-138344-13) to permit, but not require, charitable nonprofits to file a new, separate information return with the IRS (in addition to the IRS Form 990) by February 28 every year to substantiate contributions of more than $250 in value. The new informational tax return ("Donee Report") would have required the nonprofit to collect the donor's name, address, and Social Security number or other taxpayer identification number. Nonprofits taking this option would also have been required by that date to provide a copy to each donor listed (but only the portion that contains "information related to that donor").

Opposition to the proposed rule was broad-based and consistent. A set of joint comments submitted by 215 nonprofits expressed concern that the collection of SSNs would "expose the public to increased risk from identity theft, impose significant costs and burdens on nonprofit organizations, and create public confusion and disincentives for donors to support the work of nonprofits."

In separate detailed comments, the National Council of Nonprofits demonstrated that the proposal to collect SSNs runs counter to IRS' own advice, the policies of law enforcement agencies across the country, and clear directives from the federal government and Congress. It is notable for the purposes of this hearing that we expressly pointed to the divergence of IRS policy from OMB

Statement of the National Council of Nonprofits
Protecting Americans' Identities Hearing
May 23, 2017

Memorandum M-07-16 that instructs federal agencies to "review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous."[1]

The good news is that Treasury and the IRS responded to the nearly 37,000 public comments by withdrawing the Gift Substantiation Proposed Rule in early January 2016. Sadly, a great deal of energy had to be diverted from nonprofit missions and program services in order to respond to a bad proposal – the collection and reporting of SSNs – when federal policy is so abundantly clear.

That being said, clear messages were delivered to Treasury and the IRS that are relevant to the issues before the Subcommittees at this hearing. The following points are paraphrased from the comments from the National Council of Nonprofits and the Community Comments signed by 215 national nonprofit organizations:

- **"Never" is the better answer**: The Treasury and IRS proposal would have opened the door for scam artists, even if not a single nonprofit in the country adopted the "voluntary" reporting system. Although the IRS argued that the proposed regulation wouldn't *require* nonprofits to collect the Social Security numbers, the mere existence of the rule opens the door for bad actors. The IRS shouldn't help them by creating confusion. A charitable nonprofit should never be asking a donor for her or his Social Security Number when soliciting donations; if someone is asking in relation to a donation, that should be considered a sign of a scam or fraudulent solicitation. That is the consistent message being promoted by law enforcement now. Rather than create a regime in which some nonprofits occasionally require donors to provide their SSNs, Treasury and the IRS would better serve the public by getting behind one consistent message that donors should never be asked to provide their SSNs for gift substantiation purposes.[2]
- **Administrative Burdens and Fiduciary Duties**: Collection, storage, and reporting of Social Security numbers to the IRS is a costly additional endeavor that would have imposed significant risks on entities that could be hacked. To protect sensitive donor information, nonprofits would have to divert resources from mission to purchase expensive data security systems that have no guarantee of protecting the public. Nonprofits that collect Social Security numbers and improperly protect the data could be subjecting themselves and their board members to lawsuits asserting a breach of fiduciary duty.
- **Disincentive for Donor Support**: In 2009, the Government Accountability Office reviewed a proposal similar to the September 2015 draft regulation and found that "[t]axpayers may reduce giving because they are reluctant to provide Social Security numbers to charities given concerns over identity theft."

We present the foregoing information as a cautionary tale. It isn't enough to have a directive that all departments and agencies are expected to follow. The issue of information security, and particularly

---

[1] Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16, May 22, 2007.
https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

[2] We recognize that Social Security numbers are required in different contexts, such as when an individual steps forward to donate a vehicle (see IRS Publication 4302) or volunteers to work with certain populations that the law protects by requiring detailed background tests. Those circumstances are different because they do not lend themselves to scam artists calling people randomly asking for their Social Security numbers.

the security of Social Security numbers, is one that requires constant and vigorous defense. The charitable nonprofit community has shown its willingness to join in that defense, and will continue to work with, and in this example, against, government officials at all levels to ensure that Social Security numbers are safe.

Respectfully submitted,
National Council of Nonprofits

Contact Information

David L. Thompson
Vice President of Public Policy
National Council of Nonprofits
1001 G Street NW Suite 700E
Washington, DC 20001
(202) 962-0322
dthompson@councilofnonprofits.org

National Council of Nonprofits

The National Council of Nonprofits (Council of Nonprofits) is a trusted resource and advocate for America's charitable nonprofits. Through our powerful network of State Associations and 25,000-plus members – the nation's largest network of nonprofits – we serve as a central coordinator and mobilizer to help nonprofits achieve greater collective impact in local communities across the country. We identify emerging trends, share proven practices, and promote solutions that benefit charitable nonprofits and the communities they serve.