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. DAVID DEVRIES

As the Chief Information Officer, David DeVries serves as the senior digital and information technology advisor to the OPM Director. In this role, in coordination with OPM senior leadership and other stakeholders, he is responsible for defining and implementing a technology strategic vision that aligns with the organization's mission, objectives, and goals. The CIO leads OPM in the adoption of modern, innovative, business and digital solutions, and is the accountable official for all IT and information security operations across the OPM enterprise. Mr. DeVries joined OPM after serving as the Principal Deputy Chief Information Officer at the Department of Defense.

Mr. DeVries joined the DoD CIO in May 2009 as the Deputy CIO for Information Enterprise, where he was responsible for integrating DoD policies and guidance to create information advantages for department personnel and organizations, and DoD mission partners. Since August 2010, his work has included moving the department towards adopting a Joint Information Enterprise (JIE) based on a single, secure, reliable DoD-wide IT architecture; realizing Secretary of Defense IT efficiencies; creating the way ahead for improved DoD - Veterans Affairs electronic health record exchange capability; expanding cloud adoption and mobile communications capabilities; and establishing key enabling capabilities to achieve the DoD Information Enterprise.

Mr. DeVries has a bachelor of science degree from the United States Military Academy, and a master of science degree in electrical engineering from the University of Washington in Seattle, Washington. He is also a graduate of the Army Senior Service College and served as a Corporate Fellow with IBM Business Consulting Services while participating in the Secretary of Defense Corporate Fellowship Program.