Establishing a Federal Employee Personnel Number:

A Unique ID to Replace the SSN

May 23, 2016

By Lyn McGee

The Center for Organizational Excellence

QUESTION

1. How can OPM eliminate SSN from electronic records held by OPM?
2. How can OMB implement an alternate ID for Federal employees to replace the SSN as the employee ID?

RECOMMENDATION

Replace the SSN with an alternate employee ID number in all electronic records, and establish a secure correspondence file that associate every SSN with the new ID.

ALTERNATIVES

1. Implement digital certificates as the identification mechanism for Federal employees
2. Add an alternate ID to Federal employment records that becomes the primary identifier, but leave the SSN in the record for those systems that consume SSN
3. Encrypt the SSN reliably, but irreversibly into a unique “record linkage number” (RLN)

BACKGROUND

The social security number (SSN) was established in 1936 solely for the purpose of tracking the earnings histories of US workers for use in administering benefits under the new Social Security program including unemployment compensation, aid to the states for various health and welfare programs, and the Aid to Dependent Children program.

The expansion of SSN use began in 1943 with Executive Order (EO) 9397 requiring federal agencies to use the SSN for the purpose of identifying individuals in any new record systems. This didn't start to create big changes until the advent of the computer in the 1960s, when systems requiring the SSN proliferated throughout the government and private sector, including the IRS, who began using the SSN for federal tax reporting in 1962.

Subsequently, Congress enacted several laws that require the use of SSNs for purposes other than Social Security, such as food stamps, Temporary Assistance for Needy Families, and child support enforcement, as well as the Commercial Driver's License Information System. Laws then compelled banks to join in. Colleges and hospitals soon followed suit.

In 1961, the Civil Service Commission adopted the SSN as the official employee identification number for Federal employees, even though most are not eligible to collect Social Security.

The result is that the SSN is routinely used in thousands of transactions governing the lifecycle of the Federal employee, putting Federal employees at risk for identity theft.

The social security number and the card containing your name and number was never intended to be a way to verify identity. The card does not establish that the person presenting the card is actually the person whose name and SSN appear on the card. In 1946, the Social Security Administration (SSA) added the disclaimer "FOR SOCIAL SECURITY PURPOSES NOT FOR IDENTIFICATION" to the card and then removed it in 1972 during a redesign. Although SSA has made the card counterfeit-resistant, the card does not contain information that would allow it to be used as proof of identity. However, the simplicity and efficiency of using a unique number that most people already possess has encouraged widespread use of the SSN by both government agencies and private enterprises, especially

as they have adapted their recordkeeping and business systems to automated data processing.

Today the SSN may be the most commonly used numbering system in the United States. As of December 2008, the Social Security Administration (SSA) had issued over 450 million original SSNs, and nearly every legal resident of the United States had one. The SSN's very universality has led to its adoption throughout government and the private sector as a chief means of identifying and gathering information about an individual.

The result is that our SSN holds the key to our financial identities, which makes them appealing to identity thieves, who can use the numbers to open new bank accounts and credit cards. An SSN is also typically the first piece in building an identity profile that can be used for more elaborate crimes like insurance fraud. In addition to being unique and widely available, the vast majority of SSNs were assigned according to a publicly-available formula. Because it was never intended to be used for identification, the formula was never anticipated as being a problem.

PROBLEM STATEMENT

In 1962, The Civil Service Commission adopted the SSN to identify federal employees. The result is that the same number that is used on driver's licenses, tax returns, and bank statements is used on almost every piece of paper – or digital form – in a Federal employee's official personnel file. It is used for routine personnel actions, to record training, to request health benefits, and for many other purposes that do not require an SSN. This results in an unacceptable level of risk for Federal Employees that their SSN may become compromised.

This risk is especially high for records stored by the Office of Personnel Management (OPM). While the SSN is stored in hundreds of systems across the Federal government for subsets of Federal employees, only OPM stores files containing the SSN of every Federal employee.

RECOMMENDATION

Replace the SSN with an alternate employee ID number in all electronic records, and establish a secure correspondence file that associates every SSN with the new ID.

IMPLEMENTATION IN OPM SYSTEMS

Step 1: Identify all OPM systems that store SSN data

The first step is to identify all instances of SSNs in OPM systems. Because of the Privacy Act of 1974, this will be easier to do for systems of record, which are reported to the Office of the Federal Register (http://www.ofr.gov/Privacy/2011/opm.aspx), and which list 45 systems, 23 of which list SSN as part of the data captured. Other systems may have SSNs, but don't list the data captured. And many of the 45 systems listed have multiple sub-systems. See Appendix A for a list of identified systems of record and their use of SSN data.

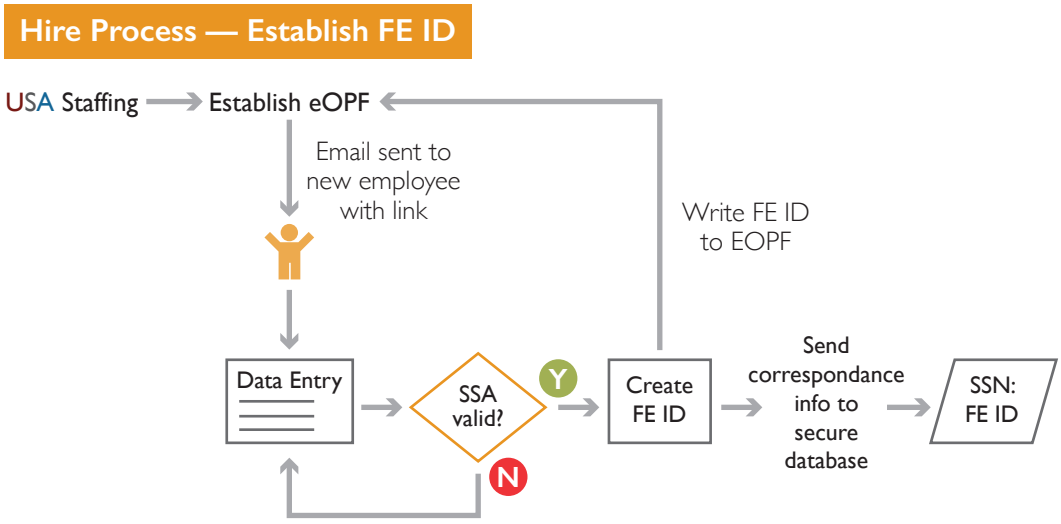
Because of a weakness in the privacy act that only requires disclosure of PII captured and the uses to which it will be put for systems maintained to accomplish agency functions, there are many other systems maintained by OPM and OPM contractors likely contain SSN information that may be difficult to capture.

Once the systems that capture SSN have been identified, OPM will need to identify which systems are required by law to capture the SSN and which systems are using SSN as an identification number. Training records, for example do not need to store SSN. Payroll records would require SSN to submit tax information to the IRS. Even then, it may be possible to eliminate SSN from the system, replacing it with an alternate ID, and only doing the translation to SSN for reporting out to trusted systems that require the SSN.

Step 2: Create Alternate ID

Create a randomized system for assigning a 12-digit number to every current, active Federal employee called a Federal Employee Personnel Identification Number (FEPIN). The number should be completely random, having no relationship to SSN, agency, age, date of hire, or any other identifiable characteristics.

There should only be one database that correlates SSN with FEPIN and only two systems that can access the correspondence database: eOPF and the FEPIN number generator. See below for a high-level system architecture:



First, we address how an employee is assigned an FEPIN, then discuss how the conversion of all SSNs to FEPINs is accomplished in OPM systems.

When a decision is made to hire, USA Staffing sends information to eOPF to establish the OPF. The only change would be that USA Jobs and USA Staffing would no longer capture SSN. When a new personnel record is established, an email is generated and sent to the new employee with a link to the FEPIN generator.

The new employee will follow the link to the FEPIN generator, enter the required information (name, address, SSN). The FEPIN generator calls the Social Security Administration (SSA) to verify the SSN:

Step 3: Verify SSN

There are two Internet verification options you can use to verify that your employee names and Social Security numbers (SSN) match Social Security's records. You can:

- Verify up to 10 names and SSNs (per screen) online and receive immediate results. This option is ideal to verify new hires.

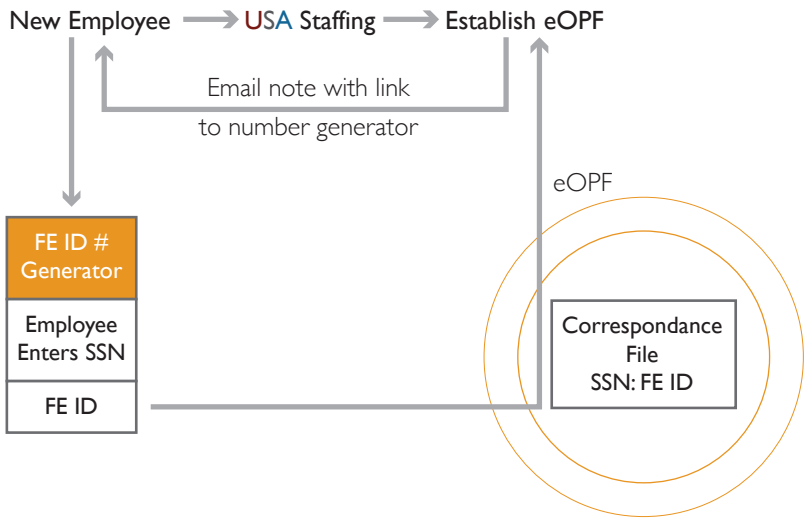
- Upload overnight files of up to 250,000 names and SSNs and usually receive results the next government business day. This option is ideal if you want to verify an entire payroll database or if you hire a large number of workers at a time.

If the SSN is valid, a FEPIN is assigned and the information is sent to eOPF and to the correspondence database.

Step 4: Convert SSN in existing OPM systems to FEPIN

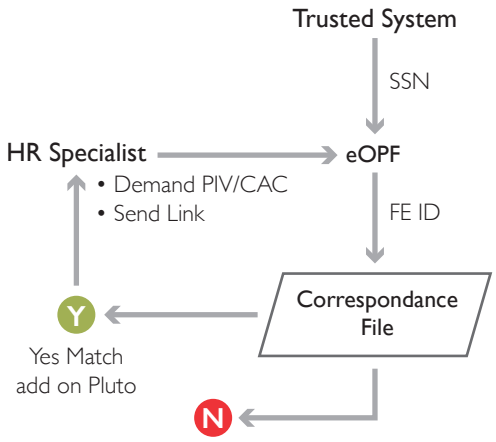
The challenge for OPM is that multiple data providers, agencies and shared service centers send files with SSN data to OPM every week. Converting all of those agency files will take years. Our recommendation is to put a conversion capability in place behind the OPM firewall for all inbound files, converting the SSN to the new FEPIN before the data is stored in OPM systems.

Because the correspondence file, which keeps a record of the SSN:FEPIN data is the single point of weakness, it would be critical to limit access to this file. To do that, we suggest a defense in depth security posture, which isolates the correspondence file from almost all files. The only systems that should be able to access the correspondence file are eOPF (or the DW) and the FEPIN number generator:



Populate other systems with FEPIN. To protect the correspondence file, all HR systems should consume the FEPIN from eOPF. In the unlikely event that there is a need to conduct a reverse validation (input FEPIN and confirm associated SSN), we still recommend that there is a two part process that ensures the person or system requesting the information is trusted:

Verify Employee SSN Using FE ID



The initial solution would allow an HR specialist to enter FEPIN and SSN and get back either a green “yes” they match or red “danger” they don’t match. An enhancement could offer a return of the photo of the person associated with the FEPIN and SSN.

OTHER ALTERNATIVES

1. Do nothing.

The SSN is becoming less and less valuable as a starting point for identity theft for two reasons. One is that it is so easy to get in today's environment. The other is that technology is enabling the development of new on-line, certificate-based validation methods that will make the SSN obsolete as the basis of identification.

Social security numbers are the most common starting point for identity thieves, said Angel Grant, a senior manager at the information security firm RSA, which monitors the black markets where identity thieves traffic. In the last five years, SSNs have become so easy to obtain that thieves now usually bundle the number with extra identifying information like birth dates and even medical records in order to get the price up. "A Social Security number is good, and it's very easy for a fraudster to obtain," she said. "Social Security numbers are a commodity in the underground right now."

Obama's 2009 Cyberspace Policy Review (CPR) led to the establishment of a National Strategy for Trusted Identities in Cyberspace (NSTIC), which is exploring ways to create secure, efficient, easy-to-use and interoperable identity credentials for accessing online services in a manner that promotes confidence, privacy, choice and innovation.

The projects will test solutions that rely on mobile phones, biometrics, encryption, and other cutting-edge security technology that lets consumers browse anonymously but also validate their identities when needed. If one or more of the privately-developed online identity systems commissioned by the Obama administration proves effective, it may end up creeping into daily use the same way the SSN did — that is, through common practice instead of federal mandate. Unlike the SSN system, these systems are being designed for use as an identifier. If implemented, one of these systems could easily substitute for many less secure verification methods in place today, including typing in your mother's maiden name or reciting the last four digits of your SSN.

The use of SSN as ID Number for Federal Employees

Several federal agencies have already taken steps to replace the use of the SSN as an identifier.

In June 2007, OPM issued a policy on protecting Federal employee SSNs. When the SSN is required as a data entry parameter, it must not be displayed on the input screen except when establishing the initial human resources or payroll record. In all other record retrieval and access authorization processes, the SSN must be masked with asterisks or other special characters, similar to the technique used when handling passwords and PINs.

Beginning in the fall of 2007, beneficiaries of the Federal Thrift Savings Plan received randomly assigned account numbers in place of their SSN, which had previously served as the account number.

In 2010, the Department of Veterans Affairs (VA) and the Department of Defense (DoD) agree on a single lifetime personal identifier that will follow military personnel from active duty through retirement. The DoD identification number, formerly referred to as the Electronic Data Interchange Personal Identifier (EDIPI), is a unique 10-digit number that is associated with personnel and their Common Access Card (CAC). The DoD ID is assigned to each person registered in the Defense Enrollment and Eligibility Reporting System (DEERS). This includes government civilians, active duty military, dependents, reservists, retirees and contractors. In time, the DoD ID number will replace the SSN in many Department of the Navy and DoD business processes. The Pentagon stopped printing Social Security numbers on all DoD ID cards by June 2011, substituting the new identifier. And the VA rolled out new VA health ID cards in 2014 that do not store SSNs in card magnetic strips or barcodes.

APPENDIX A: OPM SYSTEMS OF RECORD

System Designation	System Name	SSN?	Purpose?
OPM/INTERNAL–2	Negotiated Grievance Procedure Records.	**Y**	These records are used to process an employee's grievance filed under a negotiated grievance procedure.
OPM/INTERNAL–3	Security Officer Control Files.	**Y**	These records are used to control position sensitivity and personnel clearances.
OPM/INTERNAL–4	Health Program Records.	**Y**	These records document utilization of health services provided by OPM's Health Unit.
OPM/INTERNAL-5	Leave, and Travel Record.	**Y**	These records are used to administer the pay, leave, and travel requirements of OPM and in the administration of the fare subsidy program.
OPM/INTERNAL-6	Appeal and Administrative Review Records	**N**	These records are used to process the various appeals or administrative reviews available to OPM employees.
OPM/INTERNAL-7	Complaints and Inquiries Records	**N**	These records are used to take action on or respond to a complaint or inquiry concerning an OPM employee or to counsel the employee.
OPM/INTERNAL-8	Employee Counseling Services Program Record	**N**	These records are used to document the nature of the individual's problem and to record participation in and the results of treatment or rehabilitation.
OPM/INTERNAL-9	Employee Locator Card Files	**N**	This information is used to capture emergency contact information should an emergency occur while the employee is on the job.
OPM/INTERNAL-10	Moter Vehicle Operator and Accident Report Records	**N**	These records document verification of employee's license to operate a Government motor vehicle; and information regarding motor vehicle accidents.

System Designation	System Name	SSN?	Purpose?
OPM/INTERNAL-11	Administrative Grievance Records	**N**	These records are used to process grievances submitted by OPM employees in a matter subject to the control of agency management.
OPM/INTERNAL-12	Telephone Call Detail Records.	**N**	The call detail records verify telephone usage to resolve billing discrepancies; to allocate the costs; to identify unofficial telephone calls; and as a basis for taking action.
OPM/INTERNAL-13	Parking Program Records.	**Y**	The records are used to administer parking at TRB to collect information for tax purposes, and compare records with other Federal agencies to ensure parking privileges are not abused.
OPM/INTERNAL-14	Photo Identification and Visitor Access Control Records.	**N**	OPM will use the records to issue official U.S. Government Identification cards to OPM employees and contract employees requiring access to OPM building and offices.
OPM/INTERNAL-15	OPM Child Care Tuition Assistance Records.	**Y**	To establish and verify OPM employees' eligibility for child care subsidies in order for OPM to provide monetary assistance to its employees.
OPM/INTERNAL-16	Adjudications Officer Control Files.	**Y**	These records help make suitability or security determinations, granting security clearances for access to classified information, and documenting an individual's performance on an OPM—IS contract.
OPM/INTERNAL-17	Web-Enabled Voting Rights System (WEVRS).	**N**	In accordance with the Voting Rights Act of 1965, as amended, OPM maintains the List, keeping it as up-to-date as possible.
OPM/INTRENAL-18	Federal Cyber Service: Scholarship For Service (SFS).	**N**	The information is used by OPM's Center for Talent Services to register scholarship recipient's education and experience and to provide this information to potential Federal employers.

System Designation	System Name	SSN?	Purpose?
OPM/CENTRAL-1	Civil Service Retirement and Insurance Records.	**Y**	These records provide information and verification on which to base entitlement and computation of CSRS and FERS benefits, CSRS and FERS and survivors' benefits, FEHBP and enrollments, and FEGLI benefits, and to withhold State income taxes from annuitant payments. These records may also be used to compute CSRS and FERS benefit estimates.
OPM/CENTRAL-2	Complaints and Inquiries Records.	**N**	The principal purpose for which these records are established is to retain a record of correspondence with an individual, over a complaint or inquiry, as a reference should that individual again contact OPM.
OPM/CENTRAL-3	RESERVED		
OPM/CENTRAL-4	Inspector General Investigations Case Files.	**Y**	Information in case files serves to document the outcome of investigations, reporting the results of investigations to other OPM components or agencies for their use in evaluating their programs and imposition of any civil or administrative sanctions.
OPM/CENTRAL-5	Intergovernmental Personnel Act Assignment Records.	**?**	These records document and track mobility assignments made under the Intergovernmental Personnel Act.
OPM/CENTRAL-6	Administrative Law Judge Application Records.	**Y**	These records serve as a basis for rating and ranking applicants for Administrative Law Judge positions in the Federal service.
OPM/CENTRAL-7	Litigation and Claims Records.	**?**	These records are maintained to defend OPM against lawsuits and to settle administrative claims brought against OPM or OPM employees..
OPM/CENTRAL-8	Privacy Act/ Freedom of Information Act (PA/ FOIA) Case Records	**N**	These records are maintained to process an individual's request made under the provisions of the Freedom of Information and Privacy Acts.

System Designation	System Name	SSN?	Purpose?
OPM/CENTRAL-9	Personnel Investigations Records.	**Y**	The records in this system may be used to provide investigatory information for determinations concerning whether an individual is suitable or fit for Government employment;
OPM/CENTRAL-10	Federal Executive Institute Program Participant Records	**Y**	The records are used by FEI staff to administer the program, to promote program participant interaction, and by FEI program participants to maintain contact with other participants.
OPM/CENTRAL-11	Presidential Management Fellows (PMF) Program Records	**Y**	These records are used by program personnel to assess eligibility; to make a final determination for finalists to become Fellows and to track PMF appointments, certifications, conversions, reappointments, withdrawals, resignations, extensions, waivers and deferrals; to track agency reimbursements
OPM/CENTRAL-12	**RESERVED**		
OPM/CENTRAL-13	Executive Personnel Records.	**Y**	The records are used to assist OPM in carrying out its responsibilities under title 5, U.S. Code, and OPM rules and regulations promulgated thereunder to manage the lifecycle of the SES employee.
OPM/CENTRAL-14	Debarment or Suspension Records for Federal Employees Health Benefits Program (FEHPB).	**Y**	This system of records documents OPMs actions to reduce fraud and abuse in Federal nonprocurement programs and actions taken to exclude participants in Federally authorized nonprocurement programs administered by OPM.
OPM/CENTRAL-15	Health Claims Data Warehouse (HCDW).	**Y**	The primary purpose of this system of records is to provide a central database from which OPM may analyze the FEHBP to support the management of the program to ensure the best value for the enrollees and taxpayers.

System Designation	System Name	SSN?	Purpose?
	Health Claims Disputes External Review Services	**Y**	The primary purpose of this system of records is to aid in the administration of external review of adverse benefit determinations and final internal adverse benefit determinations.
OPM/CENTRAL-X	Federal Competency Assessment Tool	**N**	The Federal Competency Assessment Tool is a web-based instrument for assessing the proficiency levels of Federal employees in key competencies.
OPM/Central–18	Federal Employees Health Benefits Program Claims Data Warehouse	**N**	The primary purpose of this system of records is to provide a central database from which the OIG may use claims data from carriers for audit and investigative purposes to meet its oversight obligations under the Inspector General Act of 1978.
OPM/GOVT–1	General Personnel Records.	**Y**	The OPF is the official repository of the records, reports of personnel actions, and the documentation required in connection with these actions affected during an employee's Federal service.
OPM/GOVT–2	Employee Performance File System Records.	**Y**	These records are ensure that all appropriate records on an employee's performance are retained and are available.
OPM/GOVT–3	Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers.	**Y**	These records result from the proposal, processing, and documentation of these actions taken either by the OPM or by agencies against employees in accordance with regulations.
OPM/GOVT–4	**RESERVED**		
OPM/GOVT–5	Recruiting, Examining, and Placement Records.	**Y**	The records are used in considering individuals who have applied for positions in the Federal service by making determinations of qualifications including medical qualifications.

System Designation	System Name	SSN?	Purpose?
OPM/GOVT–6	Personnel Research and Test Validation Records.	**N**	These records are used for the construction, analysis, and validation of written tests and other assessment instruments used in personnel selection and appraisal and for research on and evaluation of personnel/organizational management and staffing methods, including workforce effectiveness studies.
OPM/GOVT–7	Applicant Race, Sex, National Origin, and Disability Status Records	**Y**	These records are used by OPM and agencies to evaluate measurement and selection methods; to Implement and evaluate agency affirmative employment programs; and enable OPM to meet its responsibility to assess an agency's implementation of the Federal Equal Opportunity Recruitment Program. e. Determine adverse impact in the selection process as required by the Uniform Guidelines cited in the Authority section above. (See also "Questions and Answers," on those Guidelines published at 44 FR 11996, March 2, 1979.) f. Enable reports to be prepared regarding breakdowns by race, sex, and national origin of applicants (by exams taken, and on the selection of such applicants for employment). g. To locate individuals for personnel research. Note 1: These data are maintained under conditions that ensure that the individual's identification as to race, sex, national origin, or disability status does not accompany that individual's application nor is otherwise made known when the individual is under consideration by a selecting official.
OPM/GOVT–8	**RESERVED**		

System Designation	System Name	SSN?	Purpose?
OPM/GOVT–9	File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints.	**N**	These records are primarily used to document the processing and adjudication of a position classification appeal, job grading appeal, retained grade or pay appeal, or FLSA claim or complaint.
OPM/GOVT–10	Employee Medical File System Records.	**Y**	Records are maintained for a variety of purposes including: a. To ensure that records required to be retained on a long-term basis, b. To provide data necessary for proper medical evaluations and diagnoses, to ensure that proper treatment is administered, and to maintain continuity of medical care.

ABOUT COE

For over 30 years, COE has been a trusted partner in helping organizations and programs transform to more efficiently and effectively accomplish their mission. We help our clients achieve meaningful and measurable outcomes by designing and delivering strategy and development consulting solutions in the areas of organizational effectiveness, human capital, information technology and data management. For more information, visit us at www.center4oe.com.