OFFICE OF

INSPECTOR GENERAL

Inspection Report

Elimination of Unnecessary Use of Social Security Numbers at the Farm Credit Administraon
I-16-02

Inspector
Ava Bell

Issued August 31, 2016

FARM CREDIT ADMINISTRATION

Farm Credit Administration

Office of Inspector General
1501 Farm Credit Drive
McLean, Virginia 22102-5090

August 31, 2016

The Honorable Kenneth A. Spearman, Board Chairman
The Honorable Dallas P. Tonsager, Board Member
The Honorable Jeffery S. Hall, Board Member
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Board Chairman Spearman and FCA Board Members Tonsager and Hall:

The Office of Inspector General (OIG) completed an inspection of the Farm Credit Administration's (FCA or Agency) use of Social Security Numbers (SSN) within the Agency. The objective of this inspection was to determine whether FCA has eliminated unnecessary use of SSNs and is safeguarding SSN information in Agency processes and systems.

We found the Agency is not storing or using employee SSNs unnecessarily. When SSN information is used within FCA systems and processes, there are administrative, technical and physical safeguards.

Our inspection report contains no recommendations.

We appreciate the courtesies and professionalism extended by FCA personnel to the OIG staff. If you have any questions about this inspection, Ava Bell and I would be pleased to meet with you at your convenience.

Respectfully,

Elizabeth M. Dean
Inspector General

Enclosure

EXECUTIVE SUMMARY

I-16-02

RESULTS:

The Farm Credit Administration (FCA or Agency) has eliminated unnecessary use of Social Security Numbers (SSN) and is safeguarding SSN information and other personally identifiable information (PII) in its processes and systems.

This report contains no recommendations.

INSPECTION OF ELIMINATION OF UNNECESSARY USE OF SOCIAL SECURITY NUMBERS AT FCA

The objective of the inspection was to determine whether the Farm Credit Administration (FCA or Agency) has eliminated unnecessary use of Social Security Numbers (SSN) and is safeguarding SSN information in Agency processes and systems.

We found the Agency is not storing or using Social Security Numbers unnecessarily and there are safeguards in place when SSN information is used in Agency processes and systems. The Agency:

- Eliminated requests for SSNs from current FCA forms, with the exception of a few for which SSN use accomplishes an agency function;
- Does not unnecessarily collect and store SSNs in its processes and systems; and
- Protects SSN information with administrative, technical and physical safeguards.

This report contains no recommendations or agreed upon actions.

TABLE OF CONTENTS

BACKGROUND

The Farm Credit Administration (FCA or Agency) is an independent federal agency responsible for regulating, examining, and supervising the Farm Credit System (FCS) and the Federal Agricultural Mortgage Corporation. The core mission of FCA is to ensure a safe, sound, and dependable source of credit and related services for agriculture and rural America.

With this mission comes a responsibility to safeguard sensitive FCS and loan information, as well as sensitive, personal information within the Agency itself, including personally identifiable information (PII). PII is any information that 1) distinguishes an individual's identity, such as name, date of birth, and social security number, and 2) is linked to an individual, such as medical, financial, and employment information.[1]

We limited our inspection to a review of employee Social Security Numbers (SSN) within the Agency. Agency processes and systems change over time. Given the recent data breaches in several federal agencies, the Office of Inspector General (OIG) considered it prudent to review SSN use in forms and systems within FCA to ensure there is no unnecessary collection of SSNs, or when necessary to collect, the information is being safeguarded.

Legislation and Guidance

The Privacy Act of 1974, as amended, requires each agency that maintains a system of records to maintain only the information about individuals that is relevant and necessary to accomplish a purpose of the agency required by statute or Presidential executive order.[2] The Privacy Act also requires agencies to establish appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of records when they maintain a system of records.[3]

The Office of Management and Budget (OMB) has issued several memoranda requiring agencies to eliminate the unnecessary use of SSNs and safeguard PII and other sensitive agency information. These memoranda and their requirements are summarized as follows:

---

[1] National Institute of Standards and Technology's Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122 (April 2010).

[2] 5 USC § 552a(e)(1).

[3] The Privacy Act defines "system of records" as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 USC § 552a(a)(5). See also 5 USC § 552a(e)(10).

- OMB M-06-15, Safeguarding Personally Identifiable Information, May 2006: Required agencies to conduct a review of administrative, technical, and physical controls, and take corrective action as necessary, to safeguard PII.
- OMB M-06-16, Protection of Sensitive Agency Information, June 2006: Required agencies to use the National Institute of Standards and Technology (NIST) checklist for protection of remote information, and outlined additional technical safeguards to compensate for the lack of physical security controls when agency information is accessed remotely.
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 2007: Required agencies to: review current PII holdings and reduce such holdings to the minimum necessary for the proper performance of a documented agency function; identify and eliminate instances in which collection or use of SSNs is superfluous; explore alternatives to agency use of SSNs as a personal identifier; and develop an implementation plan to eliminate unnecessary use of SSNs.
- OMB M-07-19, FY 2007 Reporting Instructions for FISMA and Agency Privacy Management, July 2007: Required agencies to provide the implementation plan developed under M-07-16 with their annual Federal Information Security Modernization Act (FISMA) evaluation.

Prior Review

In 2002, prior to the issuance of the OMB memoranda identified above, the FCA OIG conducted a review of the Agency's use of SSNs. The objectives of the review were to determine: how FCA uses SSNs, whether the use of SSNs is mandatory, and whether procedures and safeguards were in place to protect SSN information. The OIG reviewed existing policies and procedures, and all forms published in the FCA forms database. The OIG also surveyed office directors about departmental use and safeguarding SSNs. The OIG concluded that FCA staff were taking reasonable measures to safeguard SSNs, and managers were exercising due diligence in protecting SSNs.

INSPECTION RESULTS

The objective of this inspection was to determine whether FCA has eliminated unnecessary use of Social Security Numbers (SSN) and is safeguarding SSN information in Agency processes and systems. Based on our review, the Agency is not collecting and using SSNs unnecessarily in its processes and systems. When SSNs are collected, that information is protected through administrative, technical and physical safeguards.

Eliminating Unnecessary Use of Social Security Numbers

To evaluate FCA processes and systems for unnecessary use of SSNs, we reviewed current FCA forms. We identified electronic systems and paper records that use or store SSNs and determined whether the use was for an agency function. We also tested selected data collections for unnecessary use of SSNs.

FCA Forms

We reviewed current FCA forms found in the Forms Library and other internal sources to determine whether the Agency has eliminated the unnecessary use of SSNs in its forms. We excluded Federal forms (standard forms, optional forms, etc.) from our review, as the Agency has no discretion to revise these forms. We found that FCA has eliminated the request for the SSN on most Agency forms. Only a few forms still request the SSN, and we determined each use to be required or necessary for various reasons. The following FCA forms still include SSNs:

- Flexible Spending Account (FSA) forms (Health Care FSA Claim Form and Dependent Day Care FSA Claim Form) – require a full SSN for tax reporting purposes.
- Child Care Provider Information Form – requires the Federal Tax Identification Number for child care providers for tax reporting purposes.
- Government Purchase Card Setup Form – requires a partial SSN (last four digits) for card activation.
- Government Travel Card Application – requires a full SSN for a credit check.

We determined SSN use is necessary because these forms are either tax-related documents as required by the Internal Revenue Service, or the SSN is a required use to accomplish an agency function (i.e., issuance of government credit cards).

SSNs in Paper and Electronic Systems

FCA has very few paper records that contain SSNs. These documents are payroll and personnel security records, which are maintained to accomplish agency functions (e.g., payroll administration and employee background investigations).

However, the Agency uses several electronic systems that store and use SSNs:

- National Finance Center (NFC) (payroll system)
- eOPF (OPM-mandated electronic official personnel files)
- FedHR Navigator (hiring, onboarding, retirement)
- Personnel Retrieval System (personnel management)
- USAStaffing (OPM's hiring management system)
- Executive & Schedule C System (secure database on SES, Schedule C appointees, etc.)
- GSA-USA Access (employee and contractor ID card issuance)
- e-Verify (citizenship/eligibility to work verification)
- Electronic Questionnaires for Investigations Processing and Central Verification System (personnel security)
- MyEnroll (FCA flexible spending plan administration)
- Wells Fargo (FCA 401k plan administration)
- Citibank (government travel and purchase cards)

The OIG reviewed the electronic systems identified as storing and using SSNs to determine if current SSN use is necessary for the performance of an agency function. We determined each of the systems accomplish an agency function, e.g., payroll and benefits administration, maintenance of official personnel files, or personnel security. For example, the NFC payroll system is designed to use the SSN as a personal identifier for employee record retrieval.

The Agency has also created internal electronic data collections for various purposes, and the OIG tested a judgmental sample of these data collections to determine whether SSNs are being used unnecessarily. We selected and reviewed the following data collections to confirm discussions with staff who stated that there are no SSNs in these collections:

- Personnel Action Report
- Retirement Eligibility Report
- Voluntary Leave Bank Enrollments

We confirmed that neither the reports nor the leave bank enrollments contain SSNs.

Safeguarding Social Security Numbers

We researched Agency policies and procedures, reviewed the 2015 FCA FISMA Evaluation, and conducted interviews with FCA staff to determine whether the Agency has administrative, technical and physical safeguards in place to protect SSNs in its processes and systems.

Administrative Safeguards

FCA has an information technology (IT) security policy published in PPM 902, *Computer Security Program*, and PPM 906, *Limited Personal Use of Farm Credit Administration Assets*. Compliance with these policies is mandatory. Employees and contractors are required to read and sign the Employee Certification Form for these policies when they come on board. The Agency also has a number of IT security related documents that define sensitive information and PII and provide guidance on how to protect such information. Two examples are: 1) guidance requiring personnel to encrypt email containing sensitive or privacy information, and 2) a PII breach notification policy requiring the Chief Information Officer to notify FCA management and comply with breach incident reporting requirements to the Department of Homeland Security's US-Cert website.

The Agency also provides mandatory, annual information security awareness training to all employees and contractors, which includes guidance on protecting PII. Additionally, the performance standards for all human resources staff include confidentiality language to ensure PII controls are observed.

Technical Safeguards

Annually, the OIG conducts an independent evaluation of FCA's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and an assessment of the Agency's information security program. The 2015 FCA FISMA evaluation contained no recommendations.[4] The FISMA report stated that the FCA has established an information security program consistent with National Institute of Standards and Technology, Department of Homeland Security, and OMB guidelines, in the following reportable areas:

- Continuous Monitoring Management
- Configuration Management
- Identity and Access Management
- Incident Response and Reporting
- Risk Management
- Security Training

[4] See OIG 2015 Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Modernization Act, E-15-01, Nov. 13, 2015.

- Plans of Action & Milestones
- Remote Access Management
- Contingency Planning
- Contractor Systems

Although the 2015 FISMA evaluation did not specifically review technical safeguards in place to protect SSNs, the OIG determined the FCA has an information security program that continues to mature.

Physical Safeguards

We interviewed several FCA staff who regularly handle electronic and paper records containing SSNs to determine whether physical safeguards are in place to protect this information. Through interviews in the staff offices, we determined these personnel are keeping paper records in locked cabinets, safes, closets and offices. Staff stated they keep documentation with SSNs secure in the locked areas when not using the records. Additionally, information provided by FCA managers indicated that SSNs found to be unnecessary are redacted from paper records originating from another agency. FCA staff who regularly use or access SSNs and other PII stated they are sensitive to safeguarding this information in their daily work routines.

INSPECTION CONCLUSIONS

This report contains no recommendations or agreed upon actions. We encourage the Agency to continue its vigilance in safeguarding SSNs and other sensitive Agency information.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the inspection was to determine whether the Farm Credit Administration has eliminated unnecessary use of Social Security Numbers (SSN) and is safeguarding SSN information in Agency processes and systems. We conducted fieldwork at FCA's headquarters in McLean, Virginia from May to August 2016. We limited our scope to review of current FCA forms, processes and systems.

We completed the following steps to accomplish the inspection objective:

- Reviewed applicable laws, OMB policy and other guidance related to the inspection objective.
- Considered prior reviews related to the inspection objective.
- Conducted interviews with key personnel who use or store employee SSNs.
- Reviewed applicable FCA policies and procedures.
- Researched and reviewed all FCA forms for SSN use.
- Selected and tested a judgmental sample of internal data collections to determine whether FCA is unnecessarily collecting or using employee SSNs in its data collection efforts.
- To avoid duplication of evaluative work, this inspection referenced the 2015 FCA FISMA Evaluation report, which stated FCA has an IT security program that includes all key areas identified in FISMA, and contained no findings or recommendations.

This inspection was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. Those standards require that we plan and perform the inspection to obtain sufficient, competent and relevant evidence that supports a reasonable basis for our findings, conclusions and recommendations. We assessed internal controls and compliance with laws and regulations to the extent necessary to satisfy the objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our inspection. We assessed the information and data collected during the inspection and determined it was sufficiently reliable and valid for use in meeting the inspection objectives. We assessed the risk of fraud related to our inspection objective in the course of evaluating evidence. Overall, we believe the evidence obtained is sufficient to provide a reasonable basis for our findings and conclusions based on the inspection objective.

ACRONYMS

FCA	Farm Credit Administration
FCS	Farm Credit System
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PPM	Policies and Procedures Manual
SSN	Social Security Number
PII	Personally Identifiable Information

R E P O R T

Fraud | Waste | Abuse | Mismanagement

FARM CREDIT ADMINISTRATION

OFFICE OF INSPECTOR GENERAL

Phone: Toll Free (800) 437-7322; (703) 883-4316

Fax: (703) 883-4059

E-mail: fca-ig-hotline@rcn.com

Mail: Farm Credit Administration
Office of Inspector General
1501 Farm Credit Drive
McLean, VA 22102-5090