Proposed Rules

Federal Register
Vol. 73, No. 13
Friday, January 18, 2008

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

OFFICE OF PERSONNEL MANAGEMENT

5 CFR Part 293

RIN 3260–AL24

Personnel Records

AGENCY: Office of Personnel Management.

ACTION: Proposed rule with request for comments.

SUMMARY: The Office of Personnel Management is issuing proposed regulations to achieve a consistent and effective policy for the use of Social Security Numbers by Federal agencies to combat fraud and identity theft. Federal agencies must reduce the threat of identity theft by eliminating the unnecessary use and collection of Social Security Numbers. This proposed regulation imposes significant restrictions on the use of Social Security Numbers throughout the Federal Government and is consistent with the recommendations made by the President's Identity Theft Task Force.

DATES: Comments must be received on or before March 18, 2008.

ADDRESSES: Send or deliver written comments to the Deputy Associate Director for Workforce Information and System Requirements, Strategic Human Resources Policy Division, Office of Personnel Management, Room 7439, 1900 E Street, NW., Washington, DC 20415–8200; by fax at (202) 606–4891.

FOR FURTHER INFORMATION CONTACT: Leroy McKnight, by telephone at (202) 606–4054; by fax at (202) 606–1719; or by e-mail at *Leroy.Mcknight@opm.gov*.

SUPPLEMENTARY INFORMATION: In an effort to better protect sensitive personal information, particularly Social Security Numbers (SSNs), Federal agencies must take immediate action to restrict the unnecessary use of this important personal identifier. Continued exposure of individuals' SSNs increases their vulnerability to identity theft and other harmful situations. While some Federal agencies have taken steps to reduce the use of SSNs in certain functions, inconsistencies in approaches and standards for protecting the SSN creates a risk that can lead to misuse. The Office of Personnel Management (OPM) has been working with the President's Identity Theft Task Force and the agencies on a number of identity theft protection initiatives, and was tasked with issuing formal guidance to the agencies on the appropriate ways to restrict the use, and conceal the SSNs in employee records and human resources information systems. OPM issued formal guidance to the Federal Chief Human Capital Officers on June 18, 2007, to help agencies achieve a consistent and effective policy for safeguarding the Social Security Numbers of Federal employees. A copy of the guidance package can be obtained by going to *http://www.chcoc.gov*. These proposed regulations are intended to update OPM's regulations governing personnel records so they are consistent with that guidance. These proposed regulations impose significant restrictions on the use of SSNs, leading to enhanced protection of sensitive personal information. Applying the guidance and regulations is a first step in protecting the personal identity of Federal employees.

Efforts are underway to develop requirements for a new Government-wide employee identifier which will replace the Social Security Number as the primary employee identifier. Once this new employee identifier is established, Federal agencies will have a viable alternative to the use of SSNs in their business activities. The use of this new employee identifier as a substitute for the SSN would diminish the risk of identity theft by eliminating the unnecessary use of the SSN as an employee identifier in many situations.

OPM is proposing the following specific changes, which we believe will assist Federal agencies in their efforts to combat fraud and identity theft:

In § 293.102 we are proposing to add definitions of *Exposure*, and *Primary Key*, which are new terms used in the proposed regulations.

In § 293.105, which addresses restrictions on collection and use of information, we propose to add paragraphs (b)(3) through (13). These new paragraphs provide agencies with specific information on the appropriate and inappropriate use of employee Social Security Numbers in employee records and human resources information systems.

OPM also proposes to add paragraphs (a)(8) through (10) to § 293.107, which requires special safeguards for automated records. The additional paragraphs will ensure that agencies know what they must do to improve their data security measures. These safeguards pertain specifically to improving the protection of employee Social Security Numbers.

E.O. 12866, Regulatory Review

This rule has been reviewed by the Office of Management and Budget in accordance with E.O. 12866.

Regulatory Flexibility Act

I certify that these regulations would not have a significant economic impact on a substantial number of small entities because they would apply only to Federal agencies and employees.

List of Subjects in 5 CFR Part 293

Government employees, Privacy, Records.

Office of Personnel Management.

Linda M. Springer,

Director.

Accordingly, OPM proposes to amend 5 CFR part 293 as follows:

PART 293—PERSONNEL RECORDS

1. The authority citation for part 293 is revised to read as follows:

Authority: 5 U.S.C. 552, 552a, 1103, 1104, 1302, 2951(2), 3301, and 4315; E.O. 12107 (December 28, 1978), 3 CFR 1954–1958 Comp.; 5 CFR 7.2; E.O. 9830; 3 CFR 1943–1948 Comp.

Subpart A—Basic Policies on Maintenance of Personnel Records

2. In § 293.102 the definitions of *Exposure* and *Primary Key* are added in alphabetical order as follows:

§ 293.102 Definitions.

* * * * *

Exposure means the unprotected display, storage, and transmission of personally identifiable information (PII), e.g., Social Security Numbers;

* * * * *

Primary Key means a particular item chosen to uniquely identify a specific individual or to associate information

with a specific individual in an automated environment;

* * * * *

3. In § 293.105, paragraphs (b)(3) through (13) are added to read as follows:

§ 293.105 Restrictions on collection and use of information.

* * * * *

(b) * * *

(3) If Social Security Numbers are collected, they will be collected only at the time of the employee's appointment to be entered into the human resources and payroll systems. The collection tool (if paper-based) will be stored in a protected location to guard against exposure until it is no longer required. The Guide to Personnel Recordkeeping will be used to determine retention requirements for certain paper-based collection tools. Disposal of all paper-based collection tools (i.e., forms, letters, and other correspondence) will be in accordance with the General Record Schedule issued by the National Archives and Records Administration.

(4) Agencies may not use the Social Security Number as an employee's primary key, i.e., unique identifier, in internal or external data processing activities.

(5) Agencies must ensure that Social Security Numbers are not printed, e.g., on forms, or reports, or displayed on computer display screens.

(6) Access to Social Security Numbers must be restricted to those individuals whose official duties require such access. A listing of all individuals with access authorization based on legitimate business needs must be maintained and reviewed for continued applicability.

(7) Agencies must ensure, through appropriate annual training and educational programs, including training on Privacy Act and Freedom of Information Act requirements, that those individuals who are authorized to access Social Security Numbers understand their responsibility to protect sensitive and personal information. This responsibility includes securing this information when working from home or another remote location.

(8) Agencies must use privacy and confidentiality statements that describe accountability clearly and warn of possible disciplinary action for unauthorized release of the Social Security Number and other personally identifiable information. These statements must be signed by all individuals who have access to Social Security Numbers.

(9) Agencies must ensure their telework policies and written agreements are in compliance with Federal privacy protection policies, including policies governing protection of personally identifiable information, e.g., Social Security Numbers.

(10) Agencies must require supervisory approval before authorized individuals may access, transport, or transmit information containing a Social Security Number outside of the agencies' facilities. Electronic records containing Social Security Numbers must be transported or transmitted in an encrypted or protected format as prescribed in all established guidance regarding the protection of sensitive agency information. Paper-based records containing Social Security Numbers must be transported in wheeled containers, portfolios, briefcases, or similar devices that can be locked when not in use. In addition, these containers must be identifiable by tag or decal with contact and mailing address information.

(11) Agencies must ensure access to Social Security Numbers, including access involving data entry, printing, and screen displays, occurs in a protected location to guard against exposure.

(12) Agencies must ensure all security incidents involving personally identifiable information, especially Social Security Numbers, are reported in accordance with all established guidance regarding the reporting of incidents involving personally identifiable information. In addition, agencies must inform all employees of all established incident reporting requirements annually.

(13) Agencies must ensure all authorized disclosures of information containing Social Security Numbers and other personally identifiable data are made in accordance with established regulations and procedures.

4. In § 293.107, paragraphs (a)(8) through (10) are added to read as follows:

§ 293.107 Special safeguards for automated records.

(a) * * *

(8) Minimize the risk of unauthorized disclosure of Social Security Numbers during data entry activities by concealing the Social Security Number on the screens.

(9) Assure adequate internal control procedures to properly monitor authorized and unauthorized access to Social Security Numbers and other personally identifiable data.

(10) Assure all Social Security Number safeguards and protection rules are enforced in both test and production environments.

* * * * *

[FR Doc. E8–858 Filed 1–17–08; 8:45 am]

BILLING CODE 6325–39–P

DEPARTMENT OF AGRICULTURE

Federal Crop Insurance Corporation

7 CFR Part 457

RIN 0563–AC14

Common Crop Insurance Regulations; Dry Pea Crop Provisions

AGENCY: Federal Crop Insurance Corporation, USDA.

ACTION: Proposed rule.

SUMMARY: The Federal Crop Insurance Corporation (FCIC) proposes to amend the Common Crop Insurance Regulations; Dry Pea Crop Insurance Provisions to include the insurability of additional types of dry peas, to offer winter coverage, to allow replanting payments, and to make chickpeas insurable under the Dry Pea Crop Provisions rather than the Dry Bean Crop Provisions. The intended effect of this action is to provide policy changes, to clarify existing policy provisions to better meet the needs of the producers, and to reduce vulnerability to program fraud, waste, and abuse. The changes will apply for the 2009 and succeeding crop years.

DATES: Written comments and opinions on this proposed rule will be accepted until close of business March 18, 2008 and will be considered when the rule is to be made final.

ADDRESSES: Interested persons are invited to submit written comments, titled ''Dry Pea Crop Provisions'', by any of the following methods:

- *By Mail to:* Director, Product Administration and Standards Division, Risk Management Agency, United States Department of Agriculture, Beacon Facility, Stop 0812, Room 421, PO Box 419205, Kansas City, MO 64141–6205.
- *By Express Mail to:* Director, Product Administration and Standards Division, Risk Management Agency, United States Department of Agriculture, Beacon Facility, Stop 0812, 9240 Troost Avenue, Kansas City, MO 64131–3055.
- *E-mail: DirectorPDD@rma.usda.gov.*
- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

A copy of each response will be available for public inspection and copying from 7 a.m. to 4:30 p.m., CST,