UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

FSIS DIRECTIVE

1306.21 | 5/24/17

PRIVACY CONTROLS FOR FSIS INFORMATION SYSTEMS

I. PURPOSE

This directive lists privacy control requirements as stated in the National Institute of Science and Technology (NIST) Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and NIST-SP, 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. It provides general information concerning how the Office of the Chief Information Officer (OCIO), Privacy Office, and other responsible parties implement the requirements within the Food Safety and Inspection Service (FSIS).

II. BACKGROUND

A. Privacy, with respect to personally identifiable information (PII), is a very important value for any Government organization. Government organizations maintain privacy by making sure that their policies and procedures address it. Protecting the privacy of individuals and their PII that is collected, used, maintained, shared, and disposed of by programs and information systems, is a fundamental responsibility of Federal organizations.

B. FSIS ensures information security controls are in place to protect FSIS program offices and information systems and data in compliance with Public Law 107-347, Title III, *E-Government Act of 2002*; Public Law 113-283, *The Federal Information Security Modernization Act (FISMA) of 2014;* Public Law 93-579, *Privacy Act of 1974*, as amended; and USDA Privacy regulations.

C. The goals of FISMA include development of a comprehensive framework to protect the Government's information, operations, and assets. FISMA assigns specific responsibilities to Federal agencies, NIST, and the Office of Management and Budget (OMB) to strengthen information technology (IT) system security. FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce information security risks to an acceptable level.

D. The privacy controls are based on the Fair Information Practice Principles (FIPPs) embodied in the *Privacy Act of 1974*, *Section 208 of the E-Government Act of 2002*, NIST SP 800-53, Revision 4, and OMB policies. The FIPPs are designed to build public trust in the privacy practices of organizations and to help agencies avoid tangible and intangible damages from privacy incidents. The privacy controls are implemented at the department, agency, program office, and information system level. The FSIS privacy controls are implemented under the leadership and oversight of the FSIS Privacy Office, and in coordination with FSIS OCIO, program officials, legal counsel, and others, as appropriate.

III. ROLES AND RESPONSIBILITIES FOR FSIS ADMINISTRATORS

A. **Agency Administrator.**

1. Ensures that information security and privacy policies, procedures, and practices are adequate and in place; and

2. Allocates sufficient resources (e.g., personnel and funds) to implement and operate the Privacy Program according to the NIST requirements.

B. **FSIS Assistant Administrators.**

1. Ensure that all privacy procedures are followed;

2. Ensure that employees follow privacy best practices; and

3. Ensure that employees have access to PII-specific training.

IV. ROLES AND RESPONSIBILITIES FOR THE FSIS PRIVACY OFFICE

1. Follows the guidelines set forth by the Senior Agency Officials for Privacy (SAOP) and the USDA Privacy Council;

2. Facilitates the Agency's efforts to comply with privacy requirements affecting the Agency's programs and systems that collect, use, maintain, share, or dispose of PII or other activities that raise privacy risks;

3. Ensures the development, implementation, and enforcement of FSIS privacy policies and procedures;

4. Defines roles and responsibilities for protecting PII;

5. Determines the level of information sensitivity with regard to PII holdings;

6. Identifies the laws, regulations, and internal policies that apply to PII;

7. Monitors privacy best practices;

8. Monitors and audits compliance with identified privacy controls;

9. Determines whether the proposed collection of PII, as well as the PII already collected, are authorized;

10. Documents the authority to collect PII in the Privacy Threshold Analysis (PTA), the Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other applicable documentation;

11. Describes the purpose(s) for which PII is collected, used, maintained, and shared in the system's privacy notices;

12. Describes the purpose in the related privacy compliance documentation, including the PTA, PIA, SORN, and other applicable documentation; and

13. Conducts privacy incident and breach investigations jointly with OCIO and documents the agreed upon mitigation and resolution.

V. ROLES AND RESPONSIBILITIES FOR FSIS SYSTEM OWNERS AND USERS

A. **System Owners**. System owners are FSIS employees who are designated by their specific program area and may be from program areas outside of OCIO. They are to:

1. Assist in the development of detailed operating procedures to satisfy appropriate privacy controls;

2. Assign to system users the appropriate level of role-based access;

3. Notify OCIO when use of the system is modified, including when new software is tested or installed; and

4. Identify the appropriate privacy training for system users that have significant information system security roles and responsibilities during the system development life cycle (SDLC):

    a. Before authorizing access to the system or performing assigned duties; and

    b. When required by system changes.

B. **FSIS System Users.** All employees, contractors, and authorized individuals who use FSIS IT resources are to:

1. Be knowledgeable of the contents in this directive;

2. Follow procedures in this directive, as well as those stated in all privacy-related directives, including those listed on the FSIS Privacy Program web page at: https://www.fsis.usda.gov/wps/portal/informational/aboutfsis/privacy/privacy-program;

3. Password protect or encrypt all documents and data storage devices containing sensitive PII. "Sensitive PII" is personally identifiable information which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Such information includes, but is not limited to: Social Security Numbers, employee identification numbers, health or medical information or condition, employee performance, allegations of misconduct made by or against the employee, and non-business contact information;

4. Cooperate with the Privacy Officer and OCIO in their investigation and documentation of a privacy breach or incident, including their investigation of the employees' failure to password protect sensitive PII in records they transmitted by email or sent by mail; and

5. Complete PII and security training, as required.

VI. ROLES AND RESPONSIBILITIES FOR FSIS OCIO

A. **OCIO.** Supports and promotes the privacy controls for information systems throughout FSIS.

B. **OCIO Information Systems Security Program Manager (ISSPM).**

1. Ensures collaboration among organizational entities;

2. Incorporates effective privacy protections and practices (i.e., privacy controls) within FSIS programs and information systems and the environments in which they operate;

3. Assists system owners in identifying appropriate privacy procedures or personnel;

4. Documents and provides appropriate privacy training to personnel (including system managers, system and network administrators) as identified by the Information System Security Officer;

5. Establishes, maintains, and updates annually an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, sharing, or disposing of PII;

6. Provides each update of the PII inventory to the Chief Information Officer (CIO) or information security official annually to support the establishment of information security requirements for all new or modified information systems containing PII;

7. Develops and implements a Privacy Incident Response Plan (PIRP);

8. Establishes a cross-functional Privacy Incident Response Team (PIRT) that reviews, approves, and participates in the execution of the PIRP;

9. Develops a process to determine whether notice to oversight organizations or an affected individual is appropriate and to provide that notice accordingly;

10. Develops a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and takes steps to mitigate any such risks, where appropriate;

11. Develops an internal procedure to ensure prompt reporting by employees and contractors of any privacy incident to information security officials;

12. Develops an internal procedure for reporting noncompliance with privacy policy by employees or contractors to appropriate management or oversight officials; and

13. Provides an organized and effective response to privacy incidents in accordance with the PIRP.

VII. NIST SP 800-53, REVISION 4 REQUIREMENTS

A. Authority and Purpose.

1. Determine whether the contemplated collection of PII is authorized;

2. Document the authority to collect PII in the PTA, PIA, or SORN;

3. Describe the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices; and

4. Clearly describe the purpose in the related privacy compliance documentation, including the PTA, PIA, SORN, and other applicable documentation.

B. Accountability, Audit, and Risk Management.

1. Appoint an FSIS Privacy Officer who is accountable for developing, implementing, and maintaining a governance and privacy program to ensure compliance with all applicable laws and regulations

regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;

2. Monitor federal privacy laws and policy for changes that affect the privacy program;

3. Allocate sufficient resources to implement and operate the privacy program;

4. Develop a strategic privacy plan for implementing applicable privacy controls, policies, and procedures;

5. Update the privacy plan, policies, and procedures at least biennially;

6. Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;

7. Conduct PTAs and PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing policies and procedures;

8. Perform a PTA and PIA before developing or procuring information systems, or initiating programs of projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks;

9. Establish privacy roles, responsibilities, and access requirements for contractors and service providers;

10. Include privacy requirements in contracts and other acquisition-related documents;

11. Monitor and audit privacy controls and internal privacy policy annually to ensure effective implementation;

12. Implement a process to embed privacy considerations into the life cycle of PII, programs, information systems, mission or business processes, and technology;

13. Track programs, information systems, and applications that collect and maintain PII to ensure compliance;

14. Ensure that access to PII is only on a need-to-know basis;

15. Ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s);

16. Implement technology to audit for security, appropriate use, and loss of PII;

17. Perform reviews to ensure physical security of documents containing PII;

18. Assess contractor compliance with privacy requirements;

19. Ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected;

20. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

21. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements annually;

22. Develop, disseminate, and update reports to the Department, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance;

23. Design information systems to support privacy by automating privacy controls;

24. To the extent feasible, employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII when designing information systems;

25. Conduct periodic reviews of systems to determine the need for updates to maintain compliance with the privacy regulations;

26. Keep an accurate accounting of disclosures of information held in each system of records under its control, including:

    a. Date, nature, and purpose of each disclosure of a record; and

    b. Name and address of the person or agency to which the disclosure was made.

27. Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

28. Make the accounting of disclosures available to the person named in the record upon request, unless exempted or excluded under applicable regulations.

C. **Data Quality and Integrity.**

1. Confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;

2. Collect PII directly from the individual to the greatest extent practicable;

3. Check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems annually;

4. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of collected or disseminated information;

5. Ensure that the individual or individual's authorized representative validate PII during the collection process;

6. Ensure that the individual or individual's authorized representative revalidate annually the PII that was collected is still accurate; and

7. Document processes to ensure the integrity of PII through existing security controls.

D. **Data Minimization and Retention.**

1. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

2. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent;

3. Conduct an initial evaluation of PII holdings;

4. Establish and follow a schedule for an annual review of those holdings to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose;

5. Locate and remove or redact specified PII and use anonymization and re-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure where feasible and within the limits of technology;

6. Retain each collection of PII in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule to fulfill the purpose(s) identified in the notice or as required by law;

7. Dispose of, destroy, erase, and anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

8. Use Agency-authorized methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records);

9. Configure information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule where feasible;

10. Develop policies and procedures that minimize the use of PII for testing, training, and research;

11. Implement controls to protect PII used for testing, training, and research; and

12. Use techniques to minimize the risk to privacy of using PII for research, testing, or training where feasible.

E. **Individual Participation and Redress.**

1. Provide means for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection, where feasible and appropriate;

2. Obtain consent through opt-in, opt-out, or implied consent;

3. Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

4. Obtain consent from individuals prior to any new uses or disclosure of previously collected PII, where feasible and appropriate;

5. Ensure that individuals are aware of and consent to all uses of PII not initially described in the public notice that was in effect at the time the Agency collected the PII, where feasible;

6. Implement mechanisms to support itemized or tiered consent to specific uses of data;

7. Construct consent mechanisms to ensure that operations comply with individual choices;

8. Provide individuals the ability to have access to their PII maintained in its system(s) of records unless exempted or excluded under applicable regulations;

9. Publish procedures on how individuals may request access to records maintained in a Privacy Act system of records;

10. Publish access procedures in SORNs;

11. Adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests;

12. Provide a process for individuals to have inaccurate PII maintained corrected or amended, as appropriate;

13. Use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes;

14. Provide effective notice of the existence of a PII collection;

15. Establish criteria for submitting requests for correction or amendment;

16. Implement resources to analyze and adjudicate requests;

17. Implement means of correcting or amending data collections;

18. Review any decisions that may have been the result of inaccurate information;

19. Provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for the decision, a means to record individual objections to the decisions, and a means of requesting reviews of the initial determinations;

20. Take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information where PII is corrected or amended;

21. Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the privacy practices;

22. Provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints; and

23. Respond to complaints, concerns, or questions from individuals within 48 hours of receipt.

F. **Security.**

1. Establish, maintain, and update annually an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII;

2. Provide each update of the PII inventory to the CIO or information security official annually to support the establishment of information security requirements for all new or modified information systems containing PII;

3. Develop and implement a PIRP;

4. Establish a cross-functional PIRT that reviews, approves, and participates in the execution of the PIRP;

5. Develop a process to determine whether notice to oversight organizations or an affected individual is appropriate and to provide that notice accordingly;

6. Develop a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and take steps to mitigate any such risks, where appropriate;

7. Develop an internal procedure to ensure prompt reporting by employees and contractors of any privacy incident to information security officials;

8. Develop an internal procedure for reporting noncompliance with privacy policy by employees or contractors to appropriate management or oversight officials; and

9. Provide an organized and effective response to privacy incidents in accordance with the Privacy Incident Response Plan.

G. **Transparency.**

1. Provide effective notice to the public and to individuals regarding:

    a. Activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;

    b. Authority for collecting PII;

    c. The choice, if any, individuals have regarding how the use of PII and the consequences of exercising or not exercising the choice; and

    d. The ability to access and have PII amended or corrected if necessary.

2. Describe the PII collection and the purpose(s) for which it collects that information and consider the following:

    a. How the PII is used internally;

    b. The sharing of PII with external entities, the categories of those entities, and the purpose for such sharing;

c. The ability for an individual to consent to specific use or sharing of PII and how to exercise any such consent; and

d. How an individual can obtain access to their PII.

3. Revise public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change;

4. Provide real-time or layered notice when collecting PII;

5. Publish SORNs in the Federal Register, subject to required oversight processes, for systems containing PII;

6. Keep SORNs current;

7. Include Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected;

8. Publish SORNs on the Agency public website;

9. Ensure that the public has access to information about its privacy activities and is able to communicate with the Agency privacy officials; and

10. Ensure that privacy practices are publicly available through the Agency websites or otherwise.

H. **Use Limitation.**

1. Use PII internally only for the authorized purpose(s) identified in the Privacy Act or in public notices;

2. Train personnel on the authorized use of PII;

3. Document process and procedure for evaluating any new uses of PII to assess whether they fall within the scope of the Agency officials;

4. Obtain consent from individuals for the new use(s) of PII, where appropriate;

5. Share PII externally, only for the authorized purposes identified in the Privacy Act or described in its notice(s) or for a purpose that is compatible with those purposes;

6. Enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, where appropriate; and

7. Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

VIII. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

FSIS Directive 1300.7, *Managing Information Technology (IT) Resources*, sets forth the FSIS policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment. In addition, FSIS Directive 4735.3, *Employee Responsibilities and Conduct*, outlines the disciplinary action that FSIS may take when an employee fails to fulfill responsibilities or adhere to standards of conduct.

IX. QUESTIONS

A. For questions regarding privacy controls for information systems, contact the Agency Information System Security Program at: FSIS_Information_Security@fsis.usda.gov.

B. USDA Departmental directives are located at: http://www.ocio.usda.gov/policy-directives-records-forms and FSIS Directives and Notices are located at http://www.fsis.usda.gov/wps/portal/fsis/topics/regulations.

Assistant Administrator
Office of Policy and Program Development