



USDA Privacy Impact Assessment

Fiscal Year 2026

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project	3
Mission Area System/Program Contacts	3
Abstract	4
Overview.....	4
Section 1: Authorities and Other Requirements	6
Section 2: Information Characterization	7
Section 3: Information Uses	9
Section 4: Notice	10
Section 5: Data Retention	11
Section 6: Information Sharing.....	13
Section 7: Redress	14
Section 8: Auditing and Accountability.....	15

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Platform Hosted Applications (PHA) Professional Standards Training Tracker Tool (PSTTT)
Program Office	Office of Information Technology
Mission Area	Food, Nutrition, and Consumer Service
CSAM Number	1177
Date Submitted for Review	11/20/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Deea Coleman	None
Information System Security Manager	John Rosselot	571-563-5260
System/Program Managers	Kaushalya Heendeniya	703-305-0037

Abstract

The Professional Standards Training Tracking Tool, a web-based application, was developed to meet the training requirements outlined in the Healthy Hunger Free Kids Act (HHFKA) of 2010 Professional Standards Rule, and to assist school nutrition professionals in keeping track of completed training hours. It includes a SQL-server database and is available to local educational agencies and school food authorities through the FNS public website. Since its first public release in 2017, the tool has been updated with updates to enhance the user experience.

Overview

The Professional Standards Training Tracker Tool (PSTTT) was developed by Nutrition, Education, Training and Technical Assistance Division (NETTA). The Healthy Hunger Free Kids Act of 2010 (Section 306) requires Professional Standards for state and local school district nutrition professionals. In addition to hiring standards, mandatory annual training is required for all individuals involved in preparing school meals. To meet the training requirements and assist in keeping track of training and training courses, NETTA developed a web-based application tool with a SQL-server database and made available to local educational agencies and school food authorities through the FNS public website, with a login authentication. This tool facilitates compliance with HHFKA requirements and is provided at no cost to the state, district, or individuals. In addition, the tool is mobile friendly -- compatible with all mobile operating systems (iOS, Android, and Windows) -- to ensure easy usage and accessibility across mobile devices.

The user creates a user profile with the following information:

- School district, address
- School name, address
- School Nutrition Professional contact information, email address
- School Nutrition Professional title, or role in school nutrition program
- Hiring date

The user logs in the following information:

- Training Title
- Key Area
- Training Topic
- Learning Objective
- Training Hours/Minutes
- Date of Training
- Provider or Organization offering training, including state, local or national

The user can enter multiple names for one specific training without having to repeatedly enter training information. A certificate of completion can also be printed. The tool also provides the user with the ability to export and save results in multiple file formats, including PDF (.pdf), Excel and Word 2000 or higher (.docx). It has a user-centered, simple, intuitive interface.

Streamlined and intuitive navigation is offered for easy access to all functionalities.

Managers/directors are only able to create and/or view user profiles and recorded training courses for their own employees. State agency users can only view and print reports of completed training records for school users only in their states. FNS admin can only view user profiles. At the request of users, FNS admin can deactivate accounts of users no longer with the organization and also reactivate users. Users have access to the tool via eAuthentication Level 1.

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which SORN applies, if an ATO has been completed, and if there is Paperwork Reduction Act coverage:

What legal authorities and/or agreements permit the collection of information by the project, application, or system?

HHFKA 2010, Section 243(c) of Public Law 106–224, the Agricultural Risk Protection Act of 2000, which amended section (42 U.S.C. 1766(d)(5)(E)(i) and (ii)) of the Richard B. Russell National School Lunch Act

Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

Yes, approved 10/24/2024.

Which System of Records Notices (SORNs) apply to the information?

[SORN Food and Nutrition Service FNS-11](#)

Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

What information is collected, used, disseminated, or maintained in the project, application, or system?

Identifying Numbers:

- Employee Identification Number
- Personal Mobile Phone Number

Biographical Information:

- Name (Including Nicknames)
- Mother's Maiden Name
- Personal Email Address
- Employment Information

Employee information that can be stored and tracked within PSTTT for both users and for individuals who do not have user accounts, which includes their names, employee IDs, email addresses, and job information.

What are the sources of the information in the project, application, or system?

The user (member of the public) enters the information directly into PSTTT.

How is the information collected?

Information is collected electronically directly from the users of PSTTT.

Does the project, application, or system use information from commercial sources or publicly available data? If so, explain why it is used.

Yes. FNS developed a web-based application tool with a SQL-server database which is available to local educational agencies and school food authorities through the FNS public website. Publicly available data that is used in the tool includes school name and addresses and list of available Professional Standards training. These data are used to auto-populate fields as a way of making the tool more user friendly.

How will the information be checked for accuracy? How often will it be checked?

Individuals (i.e., educational employees and managers) are responsible for checking for accurate information. FNS staff do not check PII for accuracy. Once a year, FNS staff will review the training titles that are submitted by users.

Does the project, application, or system use third-party websites?

Not applicable

What is the purpose of the use of third-party websites?

Not Applicable

What PII will be made available to the agency through the use of third-party websites?

Not Applicable

List the privacy risks and mitigations related to the characterization of the information.

Privacy Risk: Over-Collection of Data. Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: Documentation and Procedures. Document procedures for the proper handling, storage, and sharing of different categories of personal information, ensuring compliance with privacy regulations.

Section 3: Information Uses

These questions delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the project, application, or system's business purpose.

The information is being collected to help school nutrition professionals track their annual training hours for professional standards as required in the HHFKA 2010 (Section 306). This tool is optional and not required to use.

Does the project, application, or system use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No

List the privacy risks and mitigations related to uses of the information.

Privacy Risk: Data Misuse. Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Mitigation: Data Minimization. Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

Section 4: Notice

These questions are intended to provide notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

How does the project, application, or system provide notice to individuals prior to collection?

The OMB Burden Statement and the Privacy Act Notice is provided on the home/front-facing page of the tool.

What options are available for individuals to consent, decline, or opt out of the project?

Track training is mandatory as stated on HHFKA 2010; however, using the USDA tool to track the trainings is voluntary. Users may use other mechanisms to track their training.

List the privacy risks and mitigations related to notice.

Privacy Risk: Privacy Act risks associated with notices include:

- Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.
- Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

- Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.
- Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

Section 5: Data Retention

These questions outline how long information will be retained after the initial collection.

What information is retained and for how long?

Since records must be maintained and made available to the State agency upon request, school nutrition professionals are advised to keep their training records for 3 years, plus the current school year. The tool enables users to view and print reports from previous years they have used the USDA tool to record training hours. In the information that is saved is the training and the number of hours of training completed for the school year for each employee.

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, indicate the name of the records retention schedule.

Retention schedule is as follows:

- Individual employee training records: GRS 2.6, Item 30 - Temporary. Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first.
- Inputs: GRS 5.2, Item 020 - Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
- Outputs: GRS 5.2, Item 020 - Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
- System Documentation: GRS 3.1, Item 051 - Temporary. Destroy 5 years after the project/activity/ transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system.
- Social Media (Social Media Public Relations and Information Dissemination Content): FNS -107 Temporary. Destroy when no longer needed. (Destroy when 7 years old).
- Public correspondence and communications not requiring formal action: GRS 6.4, Item 020 Temporary. Destroy when 90 days old.
- Public customer service operations records: GRS 6.5, Item 010 Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.
- Customer/client records: GRS 6.5, Item 020 Temporary Delete when superseded, obsolete, or when customer requests the agency to remove the records.
- Public comments: GRS 6.6; Item 030- Temporary. Destroy 1 year after publication of final rule or decision to abandon publication.
- Agency input into the unified agenda: GRS 6.6; Item 050 - Temporary. Destroy when 2 years old.

List the privacy risks and mitigations related to data retention.

Privacy Risk: Obsolescence of Data. Retained data may become outdated or irrelevant, leading to inaccuracies in decision-making or service delivery, which can affect individuals negatively.

Mitigation: Retention Schedule: Follow a retention schedule that specifies the duration for retaining different types of records and when they should be reviewed or disposed of.

Section 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared, received, and/or transmitted? What information is shared, received, and/or transmitted, and for what purpose? How is the information transmitted?

With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Recorded training reports and/or certificate of completion are shared by the users with FNS and State agency employees for the purpose of tracking training hours for Administrative Review. The information is available online through the tracking tool with the ability to view and print reports.

List the privacy risks and mitigations related to internal information sharing and disclosure.

Privacy Risk: Unauthorized Access. Sharing PII increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Mitigation: Need-to-Know Basis. Limit the sharing of PII to only what is necessary for the intended purpose, adhering to the principle of data minimization.

With which external organizations (outside USDA) is information shared, received, and/or transmitted? What information is shared, received and/or transmitted, and for what purpose? How is the information transmitted?

The information shared includes employee name, school name, title of their position, email address, hiring date, training title, key area, training topic, learning objective, and training hours. The information will be shared with FNS and State agencies employees for Administrative Review purposes. The information is shared so school nutrition professionals can personally track their own training hours for professional standards requirements. Managers can enter training for their own employees only.

FNS does not share any information collected. Schools will share the following information with states during the Administrative Review: employee name, school name, title of their position, email address, hiring date, training title and training hours.

List the privacy risks and mitigations related to external information sharing and disclosure.

Privacy Risk: Loss of Control. Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Mitigation: Need-to-Know Basis. Limit the sharing of PII to only what is necessary for the intended purpose, adhering to the principle of data minimization.

Section 7: Redress

These questions address the individual's ability to ensure the accuracy of the information collected about him or her.

What are the procedures that allow individuals to gain access to their information?

The tool is available online and access is available to all State agency personnel and school nutrition professionals. School nutrition professional individual users and/or their manager/director can access and update user profiles.

What are the procedures for correcting inaccurate or erroneous information?

Each user has the ability to edit or delete their recorded information. A direct link to FNS email address is also available on the application to send in questions and trouble shoot.

How are individuals notified of the procedures for correcting their information?

The tool clearly identifies how a user can edit/delete entries.

If no formal redress is provided, what alternatives are available to the individual?

The procedures have been set up; the primary source is to contact the user's manager. However, users can also use the Contact Us feature on the tool to contact FNS for additional assistance.

List the privacy risks and mitigations related to redress.

Privacy Risk: Inadequate Processes. If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Mitigation: Establish Clear Procedures. Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

How is the information in the project, application, or system secured?

Auditing measures currently in place include. Sending audit events to Splunk centralized log aggregation tool. Splunk has the ability to alert when certain audit events are triggered. Additionally log reports are viewed on a monthly basis. Database audits are integrated to track the actions of database users. FNS-674 forms must be on file and their need to access the system is validated at least annually. e-Authentication controls user access.

What procedures are in place to determine which users may access the project, application, or system, and are they documented?

Users of the system are audited at least annually. FNS-674 forms must be on file and their need to access the system is validated at least annually

How does the project, application, or system review and approve information sharing requirements?

Information sharing requirements are reviewed and approved on a yearly basis according to our annual assessment and review schedule

Describe what privacy training is provided to users either generally or specifically relevant to the project, application, or system.

Privacy training is part of the annual security awareness training that all employees and contractors must complete prior to being granted access to any FNS system.