Privacy Impact Assessment

Technology, Planning, Architecture, & E-Government

- Version: 1.0
- Date: October 12th, 2017
- Prepared by: USDA Office of Inspector General (OIG), Office of Data Sciences (ODS) and Information Technology Division (ITD)

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

Research Aggregated Data Analysis Repository System (RADAR)

October 12th, 2017

<u>Contact Point</u>
Virginia Rone
Assistant Inspector General
Office of Data Sciences
Office of Inspector General
United States Department of Agriculture
202-720-5168

<u>Reviewing Official</u>
Joseph Esposito
Chief Information Security Officer
Office of Inspector General
United States Department of Agriculture
(202) 720-4612

Abstract

The Office of the Inspector General (OIG) Office of Data Sciences (ODS) has established a Research Aggregated Data Analysis Repository System (RADAR). RADAR is designed to collect, store, and organize information needed by ODS to conduct analyses to promote economy, efficiency, and effectiveness, and prevent fraud in U.S. Department of Agriculture (USDA) programs and operations. A System of Records Notice for RADAR was published on January 23, 2017. This privacy impact assessment further notifies the public of the existence of RADAR and documents privacy protections incorporated in RADAR.

Overview

RADAR is designed to collect, store, and organize information needed by ODS to conduct analyses related to the economy, efficiency, and effectiveness of USDA's programs and operations and to identify and prevent fraud in USDA programs.

This privacy impact assessment provides further notice of the existence of the RADAR and publicly documents the privacy protections that are in place for RADAR.

The IBM Pure Data System, including Netezza Performance System, constitutes RADAR. The IBM Pure Data System incorporates software functionality designed specifically for data analytics and data mining. The IBM Pure Data System includes an integrated analytics software package, which incorporates specialized code allowing third-party software to execute within the system. RADAR also includes a suite of specialized analytical software tools designed to fully utilize its integrated processing power and storage capacity.

Incoming raw datasets from various data sources will be temporarily held in a dedicated 'landing zone' on Information Technology Division's (ITD) Compellent SAN prior to being loaded into the Pure Data System. The Pure Data System, along with a suite of specialized analytical software tools, will be used to process and analyze the datasets. Datasets being processed by the Pure Data System do not leave the system, but are stored and processed within the system.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

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

RADAR will house data from numerous USDA agencies (including data regarding USDA program participants, recipients, borrowers, grantees, contractors, and USDA employees), other Federal and State Government agencies, Non-Government commercial organizations and publically available data sources. RADAR will also contain records OIG ODS generates that are the result of its data analysis and data analytics work.

RADAR will house many categories of data from numerous data sources. This may include, but is not limited to Personally Identifiable Information (PII) personal data, work–related data, geolocation data and data on USDA employees, grantors, contractors, subjects of investigations and/or audits.

1.2 What are the sources of the information in the system?

Information contained in this system is obtained from

1) USDA agencies
2) Other Federal and State Government agencies;
3) Non-Government commercial organizations; and
4) Publically available data sources.

For example, this system may contain the Death Master File sold by Department of Commerce, the Risk Management Agency's HyDRA crop insurance data, Food and Nutrition Service's National School Lunch Program data, Rural Development's Multi-Family Information System data, or State Supplemental Nutrition Assistance Program data.

1.3 Why is the information being collected, used, disseminated, or maintained?

The records maintained in this system are used by the USDA, OIG to fulfill its statutory mission under the Inspector General Act, as amended, to conduct, supervise, and coordinate audits and investigations relating to the programs and operations of USDA; and to promote economy, efficiency, and effectiveness in the administration of, and prevent and detect fraud and abuse in, the programs and operations of USDA. The results of these data analysis activities, including fraud leads and vulnerability assessments, may be used in the conduct of OIG audits, investigations, and other activities.

Information is being collected so that OIG will have access to a single repository of data for purposes of conducting data modeling, investigative and audit assistance, and predictive analytics. Information will be collected, stored, and maintained to support and perform the various aspects of the OIG mission.

1.4 How is the information collected?

The information is collected in a myriad of ways, including but not limited to: data extracts, manually entered data, public records, legal documents, investigations, surveys, subpoenas, internet research, emails, interviews, meetings, investigations, and audit activities.

1.5 How will the information be checked for accuracy?

Information is reviewed by internal OIG administrative staff, investigators, auditors, and their sources in other agencies/organizations. Since RADAR receives data from agencies, commercial entities, or publically available sources rather than from individuals directly, OIG relies on data source owners to check for data accuracy on a routine basis.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The IG Act authorizes OIG to have access to “all record, reports, audits, reviews, documents, papers, recommendations, or other material” maintained by the USDA. RADAR is an authorized repository for information collected under Inspector General Act of 1978, 5 U.S.C. app.; 5 U.S.C. 301; 7 U.S.C. 2270.

1.7 <u>Privacy Impact Analysis</u>: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

RADAR is a collection point for PII and potentially incriminating information. Risk cannot be fully eliminated; however, RADAR resides within the OIG network, which is protected by two-factor authentication and file level permission restrictions. Furthermore, RADAR may be accessed remotely only using an OIG issued computer via OIG’s Virtual Private Network (VPN) and by suppling valid two-factor authentication credentials. Single Sign-On (SSO) process was implemented in the RADAR system to allow authorized ODS users to gain access to the RADAR environment. A unique username and complex password is required to log into the system and access to the data is strictly enforced, once within the RADAR environment. Passwords must be changed every 90 days.

The exposure/risk to privacy is low. The data is primarily collected from USDA agencies and OIG components, such as, Investigations, Audit, Management, and FOIA. The data is moved to the RADAR system by an ODS employee. Once the data is processed within RADAR system, only ODS employees with appropriate permission have access to the data. ODS employee’s permission is granted based on a need to know basis. Any documents created from RADAR system will be shared with OIG components for appropriate use. The risk for data in motion is mitigated through the use of approved network level encryption techniques, role-based access control, auditing, and data loss prevention measures. The risk for data at rest is mitigated through access control, data security, and the encryption of the data. The risk for data in use is mitigated through appropriate host based security.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information will be used to perform predictive data analysis, statistical sampling, modeling, computer matching, continuous monitoring, and data mining of information pertaining to USDA programs and operations in support of OIG audits, investigations, and other activities, and to identify indicators of fraud and more generally, to promote the effectiveness and integrity of USDA programs.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Data is analyzed by a suite of statistical analysis software packages, business intelligence and analytics software packages, data extraction and analysis software packages, statistical and graphics software, data analysis and visualization software, and geographic information systems software, etc.

The data produced from these software suites include summary spreadsheets, tabular tables, graphical figures and charts, geospatial maps, summary statistics, and data visualizations.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system is designed to extract external commercial data or publically available data. External commercial data or publicly obtained data will be used as appropriate for comparative analysis to assist with Investigations, Audit, and other reviews.

2.4 <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The system implements various security concepts in order to ensure that information is handled appropriately. This includes, but is not limited to, the concept of least privilege, separation of duties, logging, real time alerting, access escalation prevention and detection, and Rules of Behavior requirements. OIG Rules of Behavior forms define appropriate behavior for both users and administrators of the RADAR system.

The system complies with NIST 800-53 controls requirements. This includes controls covering access control, risk management, audit and accountability, awareness and training, contingency planning, identification and authentication, system and information integrity, incident response, maintenance, media protection and more. The system security complies with USDA requirements to ensure that information is handled appropriately.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

All information will be retained in compliance with NARA Guidelines and OIG's records retention schedule. Specifically, records generated for and used in an investigation or an audit will be maintained in accordance with the appropriate investigations or audit retention schedule. OIG is currently developing a NARA retention schedule for this system. In the meantime, OIG is retaining all Federal records related to ODS and the RADAR system.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

No. OIG is currently developing a NARA retention schedule for ODS and the RADAR System.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

All data, whether new or old, is exposed to the same potential risk at any given moment. Data is protected by two-factor network authentication, a mandatory username and complex password is required to access the system, and data at rest is encrypted. Access to data is controlled via role based access control, which limits risk of adverse use. Only ODS personnel with authorization will have access to the data and data backups.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information may be shared with OIG's Offices of Investigations, Audit, Counsel, and/or Management for analytical purposes. These Offices do not have direct access to the system, however. In addition, RADAR-analyses incorporated into audit and investigative findings may be shared with appropriate USDA agencies. Reported findings are typically used by USDA agencies to improve internal controls, for administrative actions against USDA employees and/or USDA program participants, as well as for suspension and debarment actions.

4.2 How is the information transmitted or disclosed?

The information may be transmitted through electronic mail or delivered via portable media such as a flash drive, optical media, or a hard drive. When necessary, information may be redacted, marked for limited distribution, and/orencrypted.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Should data sharing include sources of the network, encryption protocols ensure PII is not inadvertently shared in an unencrypted format. In addition, each project is limited to only those persons with a need-to-know through the use of internal, granular permissions. Dissemination of information is governed by internal policy.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA, which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

OIG may have a need to share information with other Federal, state, or local government authorities in order to assist with audit and investigation proceedings. OIG may publish results or derivations of information as part of the audit and investigation process.

OIG documents routine uses of information for this RADAR system in its System of Record Notification (SORN) that cover information sharing practices. OIG's SORN is available in the Federal Register at 82 Fed. Reg. 7,795 (Jan. 23, 2017).

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes, sharing of PII outside of the Department is generally compatible with the original collection. A record from this system containing PII may be disclosed outside of the Department, if OIG determines that such a release is compatible with the purpose for which the records were collected. In addition to those disclosures generally permitted under the Privacy Act, 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system may be disclosed to authorized entities described in § 5.1, determined to be relevant and necessary, as a routine use pursuant to 5 U.S.C. 552a(b)(3). The routine uses for the RADAR system can be found at USDA/OIG-8 at 82 Fed. Reg. 7,795 (Jan. 23, 2017) and 80 Fed. Reg. 48,486 (Aug. 13, 2015) (OIG's routine uses).

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

ODS and other OIG components will comply with IG-2595, Security and Privacy, IG-8440, Obtaining and Preserving Evidence when handling all data, and IG-2186 Records Creation, Retention, and Disposition. Information shared electronically is encrypted in compliance with the FIPS 140-2 security standard. When physical transport of PII is necessary, OIG follows the Department's double wrap procedures.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The risk of data leakage once information is shared cannot be entirely mitigated; however, OIG utilizes multiple techniques to mitigate the risk of data leakage through the use of secure technologies, policies, procedures, detection mechanism, and approval requirements

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Subjects of a criminal investigation, audit, or review are unlikely to receive prior notice their information is, or will be collected. Since RADAR receives data from agencies, commercial entities, or publically available sources but not individuals, OIG does not have a need to directly notify individuals.

The SORN for RADAR, however, does provide public notice that OIG may be using individual's information in the system.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

RADAR receives data from agencies, commercial entities, or publically available sources but not individuals. OIG's Office of Investigation and Office of Audit may subpoena records related to its investigations, audits, or reviews that could later be incorporated into RADAR. Individuals have the right to refuse to answer OIG questions.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No because information is not gathered by OIG directly from individuals.

6.4 Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The information contained in RADAR is used to support OIG investigations, audit, and for personnel, criminal, or investigatory matters. This information is integral to the OIG purpose and function as provided in the SORN (USDA/OIG-8). This information is used for official OIG operations and is not accessible to non-OIG personnel or to unauthorized OIG personnel without a valid work requirement and need to know.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

An individual may request access to a record in this system, which pertains to him/her by submitting a written request to the Counsel to the Inspector General, Office of Inspector General, U.S. Department of Agriculture, 1400 Independence Avenue SW, Stop 2308, Washington, DC 20250-2308.

7.2 What are the procedures for correcting inaccurate or erroneous information?

An individual may contest information in this system that pertains to him/her by submitting a written request to the Counsel to the Inspector General, Office of Inspector General, U.S. Department of Agriculture, 1400 Independence Avenue SW., Stop 2308, Washington, DC 20250-2308. This system may contain records originated by USDA agencies and contained in USDA's other systems of records. Where appropriate, coordination will be effected with the appropriate USDA agency regarding individuals contesting records in the relevant system of records.

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

Notice is provided consistent with SORN USDA/OIG-8, originally established on March 5, 2009 (74 Fed. Reg. 9,584) and updated on August 13, 2015 (80 Fed. Reg. 48,486) and January 23, 2017, 82 Fed. Reg. 7,795.

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

Redress is provided as stated above in Question 7.3.

7.5 <u>Privacy Impact Analysis</u>: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Individuals can request access to information about them through the FOIA and Privacy Act process and may request that their information be amended by contacting Counsel to the Inspector General, Office of Inspector General, U.S. Department of

Agriculture, 1400 Independence Avenue SW, Room 441-E, Washington, DC 20250-2308.

The nature of RADAR and the data collected, processed, and stored is such that the ability of individuals to access or correct their information will be limited. However, outcomes are not predetermined and each request for access or correction is individually evaluated.

Access to the records contained in this system of records could inform the subject of an audit, review, or investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of USDA-OIG or another agency; access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden on investigative agencies.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Access to records in the system is limited to authorized personnel whose official duties require such access and is based upon the principle of least privilege. Data is protected through network single sign-on two-factor authentication, database usernames and complex passwords, database permissions, software controls, and encryption. As with most systems, Database Administrators (DBA) have access to all information; however, the data is encrypted. Only ODS personnel with authorization will have access to the data sets and access is appropriately logged.

8.2 Will Department contractors have access to the system?

No, OIG contractors and department contractors do not have access to the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All OIG personnel have privacy training in accordance with the following:

- Computer based PII training will be provided to all OIG employees on an annual basis starting in FY18. This training provides a brief overview of USDA's definition of PII, user's responsibility to safeguard and protect it, and laws and guidelines governing PII.
- "Information Security Awareness" training is required for all OIG employees, contractors, and other personnel before access to any OIG system. This training discusses data security involving PII. In addition, this training is paired with a Rules of Behavior form that requires users to agree to certain policies regarding the handling of PII.
- OIG's Office of Counsel provided specific training to ODS employees in FY17 that covered the definition of PII, examples of the types of information that might be considered PII, why it is important to protect PII, and practical tips for safeguarding PII.
- OIG provides access to privacy policies and guidelines to all employees. OIG routinely sends reminders to all users regarding Privacy policies and PII protections.

8.4 Has Assessment and Authorization (A&A) been completed for the system or systems supporting the program?

Ongoing.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system has audit capabilities that allow the ability to perform incident response and investigation type activities. The system has real time alerts set up for known potential misuse for behaviors such as privilege escalation. The system complies with NIST 800-53 requirements that help prevent the misuse of data such as routine audits and log retention requirements.

All information stored in this system is secured by utilizing database security technology and is resistant to tampering and circumvention by unauthorized users. Access to data by all authorized users will be monitored using both automated and manual controls. The information is accessed by authorized users on a “need-to-know” basis and intended systems usage basis.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk that personally identifiable information will be used inappropriately is mitigated by security training and by the use of audit mechanisms that log and monitor user activity. The assignment of roles to users to establish their access requirements based on their functions and regular review of those roles mitigates the risk that users will be able to access information beyond their requirements.

The risk of data leakage once information is shared cannot be entirely mitigated; however, OIG utilizes approved encryption and informs recipients that the information they are receiving contains PII and that they are responsible for its safekeeping. All users accessing RADAR have had a background check and hold at a minimum a ‘Secret’ level clearance.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Data repository/warehouse for conducting data analyses, predictive analytics, and statistical modeling.

9.2 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

Yes, OIG will be performing predictive data analysis, statistical sampling, modeling, computer matching, continuous monitoring, data mining, and data repository/warehousing of information. The information in RADAR pertains to USDA programs (including program participants and beneficiaries) and operations (including staff, Federal, State, and Local employees responsible for carrying out USDA programs and operations). The information is used to support OIG mission and to promote the effectiveness and integrity of USDA programs and operations. OIG has not previously conducted these types of activities for Audit and Investigations on this scale.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

OIG will not use 3rd party websites/applications to store or manipulate OIG data.

OIG may use 3rd party websites/applications to collect information in order to supplement ODS's analyses.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications.

OIG data may use 3rd party websites/applications to collect PII which includes but is not limited to:

- Name, such as, full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as, Social Security Number (SSN), driver's license number
- Address information, such as, street address
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth)

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications.

Information collected will be used to conduct analyses to promote economy, efficiency, and effectiveness, and prevent fraud in USDA programs and operations.

10.5 How will the PII that becomes available to OIG through the agency’s use of 3rd party websites and/or applications be maintained and secured?

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications.

Information collected will be transmitted and stored using secure technologies. Data in motion is secured using approved network level encryption techniques and data loss prevention measures. Data at rest is secured through access control, data security, and the encryption of the data. Data in use is secured through appropriate host based security.

10.6 Is the PII that becomes available through the agency’s use of 3rd party websites and/or applications purged periodically?

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications.

OIG is currently developing a NARA retention schedule for this system.

If so, is it done automatically?

OIG is currently developing a NARA retention schedule for this system.

If so, is it done on a recurring basis?

OIG is currently developing a NARA retention schedule for this system.

10.7 Who will have access to PII that becomes available through the agency’s use of 3rd party websites and/or applications?

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications.

Information collected using 3rd party websites/applications will be stored in a secure manner within the ODS system that provides role based access control. These roles are based on the concept of least privilege.

10.8 With whom will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be shared - either internally or externally?

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications.

Information collected from 3rd party websites/applications will not be shared however the output of ODS analyses may get shared as defined in this systems System of Record Notice.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications therefore no modification of the current system or record notice is needed.

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Not applicable

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

No.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

Not applicable

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

No OIG data will be stored, manipulated, or become externally available on 3rd party websites/applications so those privacy risks are mitigated.

OIG mitigates the privacy risk exposure of collecting information from 3rd party websites/applications data by using secure technologies to transmit and store data. The RADAR system limits adverse use using a variety of policies, technologies, and security requirements to ensure the confidentiality, integrity, and availability of the data in the RADAR system.

Responsible Officials

Name Virginia Rone
Title Assistant Inspector General, Office of Data Sciences, Office of Inspector General, United States Department of Agriculture

Name Craig Goscha
Title Chief Information Officer, Office of Inspector General, United States Department of Agriculture

Name Joseph Esposito
Title Chief Information Security Officer, Office of Inspector General, United States Department of Agriculture

Approval Signature

VIRGINIA RONE

Digitally signed by VIRGINIA RONE
Date: 2018.01.11 08:45:11 -05'00'

Virginia Rone, Assistant Inspector General Office of Data Sciences
Office of Inspector General, United States Department of Agriculture

CRAIG GOSCHA

Digitally signed by CRAIG GOSCHA
Date: 2018.01.11 08:36:59 -05'00'

Craig Goscha, Chief Information Officer
Office of Inspector General, United States Department of Agriculture

JOSEPH ESPOSITO

Digitally signed by JOSEPH ESPOSITO
Date: 2018.01.11 07:55:10 -05'00'

Joseph Esposito, Chief Information Security Officer
Office of Inspector General, United States Department of Agriculture

Appendix A. Acronyms

Acronyms used in this document are listed below in alphabetical order.

Acronym	Description
A&A	Assessment and Authorization (formerly Certification & Accreditation (C&A))
AOP	Agency Official for Privacy
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
RADAR	Research Aggregated Data Analysis Repository
EOM	End of Month
NIST	National Institute of Standards and Technology
ODS	Office of Data Sciences
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PTA	Privacy Threshold Analysis
SAOP	Senior Agency Official for Privacy
SORN	System of Record Notice
SP	Special Publication
SSN	Social Security Number
SSP	System Security Plan
TIN	Tax Identification Number
USDA	United States Department of Agriculture “Department”)

Appendix B. Definitions

Term	Definition
Third party websites/applications	The term “third-party websites or applications” refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a “.com” website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official website.

Appendix C. NIST SP 800-53 Revision 4

Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. There are eight privacy control families with each family aligning with one of the Federal Information Processing Standards (FIPS.) The privacy control families can be implemented at the organization, department, agency, component, office, program, or information system level, under the leadership of the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO)[1] and in coordination with the Chief Information Security Officer (CISO), Chief Information Officer (CIO), program officials, and legal counsel. Table below provides a summary of the privacy controls by family in the privacy control catalog

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

CNTL	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information

[1] All federal agencies and departments designate an *SAOP/CPO* as the senior organizational official with the overall organization-wide responsibility for information privacy issues. OMB Memorandum 05- 08, provides guidance for the designation of SAOPs/CPOs.

CNTL	PRIVACY CONTROLS
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy ActStatements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Source:

NIST Special Publication 800-53-Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations*