Privacy Impact Assessment

OIG IT Infrastructure (OIG GSS)

- Date: February 3, 2016
- Prepared by: USDA Office of Inspector General (OIG), Information Technology Division (ITD)

United States Department of Agriculture

Privacy Impact Assessment for the OIG IT Infrastructure (OIG GSS)

February 3, 2016

Contact Point

Kimberly Din
Office of Inspector General
United States Department of Agriculture
202-720-8670

Reviewing Official

Craig Goscha
Chief Information Officer
United States Department of Agriculture
816-926-7644

Abstract

The OIG IT Infrastructure (OIG GSS) is owned and operated by the Office of Inspector General (OIG). The OIG GSS is a network information technology computing environment made up of infrastructure (network devices, email, blackberry, administrative and file/print servers and security devices) that is used to support OIG in three primary business functions: OIG's Internal Business Units; OIG Audits; and OIG Investigations. This privacy impact assessment is being conducted to document the privacy protections that are in place for the OIG GSS.

Overview

The purpose of the OIG GSS is to provide OIG with a method of supporting over five hundred (500+) users and connecting approximately 37 field offices with the necessary infrastructure to share applications, information, and resources in support of OIG's mission to conduct audits and investigations to promote economy, efficiency, and effectiveness and prevent fraud and abuse in USDA's programs and operations. The GSS system contains the backbone network infrastructure, data storage, email, blackberry, etc that relate to internal operations, audits, and investigations. The Office of Inspector General was legislatively established in 1978 with the enactment of the Inspector General Act (Public Law 95-452). The act requires the Inspector General to independently and objectively perform audits and investigations of the Department's programs and operations.

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?

The system includes many types of information, for example, information on individuals who are part of an audit or investigation, internal staff correspondence, copies of subpoenas issued during an investigation, affidavits, witness statements, transcripts of testimony, notes, reports, etc. The type and amount of PII collected depends on the objective and topic of the investigation or audit.

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

The sources of the information in this system can be members of the public (e.g. USDA consumers/customers), OIG employees or contractors, publically available information or information from other Federal, state, or local government authorities.

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

The information is either needed to fulfill OIG's audit and investigation responsibilities or the information contains information on OIG employees for internal use.

1.4 How is the information collected?

The information is collected from OIG employees, contractors, members of the public (e.g. USDA consumers/customers), public sources, or other Federal, State, or local government authorities through calls, letters, faxes, emails, interviews, meetings, investigation and audit activities which may include public information or information from other government authorities.

1.5 How will the information be checked for accuracy?

Information is reviewed by internal administrative staff, investigators, auditors, and their sources in other agencies/organizations.

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

The system is authorized to collect information under the Inspector General Act of 1978, 5 U.S.C. app. 3; 5 U.S.C. 301; 7 U.S.C. 2270. The IG Act authorizes OIG to have access to "all record, reports, audits, reviews, documents, papers, recommendations, or other material" maintained by the USDA.

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

The exposure/risk to privacy is low. The data collected is restricted to specific groups (Investigation, Audit, Management, FOIA, etc.) who must have governmental interest in the data. The risk for data in motion is mitigated through the use of approved network level encryption techniques and data loss prevention measures. The risk for data at rest is mitigated through access control and data security. 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 is being collected to perform a variety of tasks related to various investigative cases, program related audits, and internal process management.

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

The types of tools utilized to analyze data include file integrity tools, data classification processes, and access control via Active Directory. The types of data that can be produced vary depending on the audit, investigation, or internal requirement.

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

Publically and commercial data is used to assist with investigations and audits.

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

The risk is mitigated through controls such as the use of Rules of Behavior agreements and directives. Training on the sensitivity of the information and the restrictions on disclosure is performed. Data is protected by two-factor network authentication and access rights are restricted to certain individuals/groups.

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?

(A select number of records are maintained "indefinitely" aka "permanent value" by NARA: http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/chapter-4.html. Please provide statue, policy, or guideline which supports the records tenure.

All information contained will be retained in compliance with NARA Guidelines, which vary from five to ten years according to OIG Directive IG-2186 CH6.

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

(Indicate record schedule.)

Yes

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

Possible risks include unintentional disclosure during the retention period. The risk is mitigated through the use of Rules of Behavior agreements and directives. Training on the sensitivity of the information and the restrictions on disclosure is performed. Data is protected by two-factor network authentication and access rights are restricted to certain individuals/groups.

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 USDA and other OIG employees and contractors to carry out audit functions, investigation cases, or other support tasks. Only individuals approved by OIG management will be allowed access to information on the OIG GSS.

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, and/or encrypted.

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.

The risk of exposure is mitigated through the use of Rules of Behavior agreements and directives. Training on the sensitivity of the information and the restrictions on disclosure is performed. Data is protected by two-factor network authentication and access rights are restricted to certain individuals/groups.

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 investigation proceedings.

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 the Department is compatible with the original collection. 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, as is determined to be relevant and necessary, outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. A record from the system of records which indicates either by itself or in combination with other information, a violation or potential violation of a contract or law, whether civil, criminal, or regulatory, or which otherwise reflects on the qualifications or fitness of a licensed (or seeking to be licensed) individual, may be disclosed to a Federal, State, local, foreign, or self-regulatory agency (including but not limited to organizations such as professional associations or licensing boards), or other public authority that investigates or prosecutes or assists in such investigation, prosecution, enforcement, implementation, or issuance of the statute, rule, regulation, order, or license.
2. A record from the system of records may be disclosed to a Federal, State, local, or foreign agency, other public authority, consumer reporting agency, or professional organization maintaining civil, criminal, or other relevant enforcement or other pertinent records, such as current licenses, in order to obtain information relevant to an OIG decision concerning employee retention or other personnel action, issuance of a security clearance, letting of a contract or other procurement action, issuance of a benefit, establishment of a claim, collection of a delinquent debt, or initiation of an administrative, civil, or criminal action.
3. A record from the system of records may be disclosed to a Federal, State, local, foreign, or self-regulatory agency (including but not limited to organizations such as professional associations or licensing boards), or other public authority, to the extent the information is relevant and necessary to the requestor's hiring or retention of an individual or any other personnel action, issuance or revocation of a security clearance, license, grant, or other benefit, establishment of a claim, letting of a contract, reporting of an investigation of

an individual, for purposes of a suspension or debarment action, or the initiation of administrative, civil, or criminal action.

4. A record from the system of records may be disclosed to any source—private or public—to the extent necessary to secure from such source information relevant to a legitimate OIG investigation, audit, or other inquiry.
5. A record from the system of records may be disclosed: to the U.S. Department of Justice or in a proceeding before a court, administrative tribunal, or adjudicative body, when:
   (a) OIG, or any component thereof;
   (b) any employee of OIG in his or her official capacity;
   (c) any employee of OIG in his or her individual capacity where the Department of Justice has agreed to represent the employee; or
   (d) the United States, where the OIG determines that litigation is likely to affect USDA or any of its components,

   is a party to the litigation or has an interest in such litigation, and OIG determines that use of such records is relevant and necessary to the litigation, provided, however, that in each case, OIG determines that disclosure of the records is a use of the information contained in the records that is compatible with the purpose for which the records were collected.
6. A record from the system of records may be disclosed to a Member of Congress from the record of an individual in response to an inquiry from the Member of Congress made at the request of that individual. In such cases however, the Member's right to a record is no greater than that of the individual.
7. A record from the system of records may be disclosed to the Department of Justice for the purpose of obtaining its advice on an OIG audit, investigation, or other inquiry, including Freedom of Information or Privacy Act matters.
8. A record from the system of records may be disclosed to the Office of Management and Budget for the purpose of obtaining its advice regarding OIG obligations under the Privacy Act or in connection with the review of private relief legislation.
9. A record from the system of records may be disclosed to a private firm with which OIG contemplates it will contract or with which it has contracted for the purpose of performing any functions or analyses that facilitate or are relevant to an OIG investigation, audit, inspection, or other inquiry. Such contractor or private firm shall be required to maintain Privacy Act safeguards with respect to such information.
10. A record from the system of records may be disclosed in response to a subpoena issued by a Federal agency having the power to subpoena records of other Federal agencies if the OIG determines that: (a) The records are both relevant and necessary to the proceeding, and (b) such release is compatible with the purpose for which the records were collected.
11. A record from the system of records may be disclosed to a grand jury agent pursuant either to a Federal or State grand jury subpoena, or to a prosecution request that such record be released for the purpose of its introduction to a grand jury, provided that the grand jury channels its request through the

cognizant U.S. Attorney, that the U.S. Attorney has been delegated the authority to make such requests by the Attorney General, and that the U.S. Attorney actually signs the letter specifying both the information sought and the law enforcement purpose served. In the case of a State grand jury subpoena, the State equivalent of the U.S. Attorney and Attorney General shall be substituted.

12. A record from the system of records may be disclosed, as a routine use, to a Federal, State, local, or foreign agency, or other public authority, for use in computer matching programs to prevent and detect fraud and abuse in benefit programs administered by any agency, to support civil and criminal law enforcement activities of any agency and its components, and to collect debts and overpayments owed to any agency and its components.
13. Relevant information from a system of records may be disclosed to the news media and general public where there exists a legitimate public interest, e.g., to assist in the location of fugitives, to provide notification of arrests, or where necessary for protection from imminent threat of life or property.
14. A record may be disclosed to any official charged with the responsibility to conduct qualitative assessment reviews or peer reviews of internal safeguards and management procedures employed in investigative, audit, and inspection and evaluation operations. This disclosure category includes members of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) or any successor entity and officials and administrative staff within their chain of command, as well as authorized officials of the Department of Justice and the Federal Bureau of Investigation.
15. In the event that these records respond to an audit, investigation or review, which is conducted pursuant to an authorizing law, rule or regulation, and in particular those conducted at the request of the Council of the Inspectors General on Integrity and Efficiency's Integrity Committee (CIGIE), the records may be disclosed to the CIGIE or any successor entity and other Federal agencies, as necessary.
16. A record from the system of records may be disclosed to appropriate agencies, entities, and persons when (a) OIG suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) USDA has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by USDA or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.
18. A record from the system of records may be disclosed to complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or

case arising from the matters of which they complained and/or of which they were a victim.

19. A record from the system of records may be disclosed to a former employee of OIG for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where OIG requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of official responsibility.
20. A record may be disclosed to members and employees of the CIGIE, or any successor entity, for the preparation of reports to the President and Congress on the activities of the Inspectors General.
21. To the National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. § 552(h), to review administrative agency policies, procedures, and compliance with the Freedom of Information Act (FOIA), and to facilitate OGIS' offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission? (Ensure the safeguard measures are replicated in Section 8).

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, and/or encrypted. OIG publishes reports and documents on its website, www.usda.gov/oig/.

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

Information on reports may contain the identities of individuals who are not OIG decision-makers so the FOIA staff use their best efforts to anonymize information related to those individuals. The privacy risk of external sharing is also mitigated through the use of Rules of Behavior agreements and directives. Training on the sensitivity of the information and the restrictions on disclosure is performed.

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 Does a system of record exists which the agency indexes or retrieves information by a unique personal identifier built into the system?

a. ☒ No.

b. ☐ Yes.

6.2 Does system retrieve records by any of the following:

c. ☐ Name

d. ☐ Social Security Number/Tax Identification Number

e. ☐ Photograph

f. ☐ Biometric Information

g. ☐ Other Unique Identifier that can be linked to an individual

If so, please list: _____

6.3 If 6.1, is yes, a SORN is required. Does this system require a SORN and if so, please provide SORN name and URL. Please list all SORNs that are applicable.

N/A

6.4 Is there a form used in the collection of PII?

a. ☒ No.

b. ☐ Yes.

If the response is "Yes", is there a Privacy Act Statement/Notice on the form?

1. ☐ No.
2. ☐ Yes.

Enter OMB Form number(s): _____

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

N/A

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

N/A

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

N/A

6.8 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

N/A

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?

OIG employees and contractors have access to their own information or can request it from HR. Non-OIG individuals 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?

OIG employees and contractors can send corrections to the appropriate groups such as HR, IT, etc. Non-OIG individuals may request correction 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

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

OIG employees and contractors may contact the appropriate groups such as HR, IT, etc. to obtain procedure on how they can have their information corrected. For external information, individuals are notified of these procedures through OIG's

Systems of Records Notice published in the Federal Register at 80 Fed. Reg. 48,476 (Aug. 13, 2015).

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

N/A

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

Information associated with OIG employees or contractors can only be redressed by the individual and/or their manager (with the consent of the individual). For external entities**,** the requester must provide either a notarized statement or a statement signed under the penalty of perjury, declaring that the requester is actually the person they claim to be. Original signatures are required.

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?

Managers are responsible for requesting and approving specific access for individuals through an electronic form. IT Specialists receive the approved requests, grant the necessary permission(s), and document the change on the same form. Individuals must also pass the mandatory USDA Information Security Awareness training and sign the Rules of Behavior forms before gaining access to the system.

8.2 Will any contractors, (department or otherwise) have access to the system?

Approved contractors that have a business need to have access to the system are assigned a user account and granted the necessary permissions. Data is protected by two-factor network authentication and access rights to specific data are restricted to certain individuals/groups.

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

Privacy training is included as part of the mandatory USDA Information Security Awareness training. Users are also required to sign Rules of Behavior agreements and follow directives.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes

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

Technical safeguards include restrictions on computer access to authorized individuals, unique usernames, strong passwords that are frequently changed, use of encryption for certain data types and transfers, enabled auditing settings and logging, and data loss prevention measures.

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? (Best industry practices for safeguarding PII and FIPPS 199.

The risk is mitigated through controls such as the use of Rules of Behavior agreements and directives. Training on the sensitivity of the information and the restrictions on disclosure is performed. Data is protected by two-factor network authentication and access rights are restricted to certain individuals/groups.

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?

This is a general support system.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation. (E.g. Callerid, text telephone, webcams, etc.)

No

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. Please note: The term "third-party websites or applications" refers to web-based technologies that are not exclusively operated or controlled by a government entity. [1]

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?

N/A – the system does not use 3rd party websites and/or applications.

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

N/A – the system does not use 3rd party websites and/or applications.

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

N/A – the system does not use 3rd party websites and/or applications.

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

N/A – the system does not use 3rd party websites and/or applications.

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

N/A – the system does not use 3rd party websites and/or applications.

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

N/A – the system does not use 3rd party websites and/or applications.

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?

N/A – the system does not use 3rd party websites and/or applications.

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)?

N/A – the system does not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

N/A – the system does not use 3rd party websites and/or applications.

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?

N/A – the system does not use 3rd party websites and/or applications.

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.

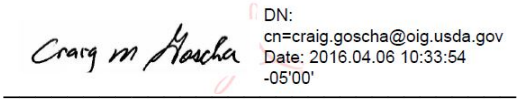
N/A – the system does not use 3rd party websites and/or applications.

Responsible Officials

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

Kimberly Din, Acting Information Systems Security Program Manager, Office of Inspector General, United States Department of Agriculture

Approval Signatures



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

Kimberly Din
Information Systems Security Program Manager (Acting)
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)
AOP	Agency Official for Privacy
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
EOM	End of Month
NIST	National Institute of Standards and Technology
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 (often referred as “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 NO.	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 NO.	PRIVACY CONTROLS
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
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*