Privacy Impact Assessment

Providing Advanced Network & Design Administration (OIG PANDA)

- Version: 2.1
- Date: April 2023
- Prepared by: USDA Office of Inspector General (OIG), Information Technology Division (ITD)

United States Department of Agriculture

Privacy Impact Assessment for the

OIG Providing Advanced Network & Design Administration (OIG PANDA)

April 2023

Contact Point
Eric Silberman
Chief Information Security Officer, Office of Inspector General
United States Department of Agriculture
(301)-593-5704

Reviewing Official
John Trifiletti
Chief Information Officer, Office of Inspector General
United States Department of Agriculture
(202) 603-9432

DOCUMENT ADMINISTRATION

Document Revision and History

Revision	Date	Author and Title	Office	Comments
1.0	February 19 2019	Joseph Esposito Chief Information Security Officer	OIG	First Draft
1.5	09/09/2021	Eric Silberman	OIG\OM\ITD	Review for 2021, reviewed all pages. Comments on sharing PII for Law Enforcement in sections 5, 6, 7, 9.
2.0	09/13/2021	Eric Silberman OIG ISSPM Security Branch Chief	OIG\OM\ITD	Update and approval for 2021
2.1	04/19/2023	Eric Silberman OIG ISSPM Security Branch Chief	OIG\OM\ITD	Update and approval for 2023

Abstract

The OIG Providing Advanced Network & Design Administration (OIG PANDA) is owned and operated by the Office of Inspector General (OIG). This system is a cloud system consisting of Amazon Web Service (AWS) services to serve as an alternate storage site for OIG IT Infrastructure backup data. In addition to AWS Simple Storage Service ("S3") backup storage, PANDA also contains an Ivanti Cloud Service Appliance ("CSA") where OIG leverages Ivanti service to patch and maintain endpoints that belong to OIG General Support System.

Overview

The purpose of the OIG PANDA is to provide OIG with a method of storing backup data as well as a method of patching endpoints which are not connected to the OIG network ("VPN").

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. As a matter of fact, the Data Types of PANDA – the storage system of the backup data of GSS – exactly mirror the data types of GSS, because GSS' data is replicated, backed up, and stored in PANDA. In fact, literally all of the data in PANDA comes directly – and only – from GSS. The two data sets are identical.

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

Information contained in this system is obtained directly from OIG GSS. In turn, this OIG GSS data is collected from:

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

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

The records maintained in this system reflect replicas of OIG GSS data that 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 collected into the OIG GSS 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. In turn, essentially all of GSS' data is replicated and backed up and stored in PANDA. This is logically equivalent to storing all of GSS data in PANDA.

1.4 How is the information collected?

The information is collected into GSS 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. In turn, the OIG GSS backup-data is uploaded into PANDA for the purpose of cost-effective air-gapped offsite storage.

1.5 How will the information be checked for accuracy?

Information was originally reviewed at the time of collection by internal OIG administrative staff, investigators, auditors, and their sources in other agencies/organizations. Since OIG 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. NO ADDITIONAL VALIDATION TAKES PLACE when we back up the OIG GSS data and upload it to PANDA. We just copy the data and upload it.

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

OIG PANDA is a storage point for PII and potentially incriminating information. OIG PANDA is protected by two-factor authentication and file level permission restrictions. Furthermore, OIG PANDA 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. A unique username and complex password is required to log into the system and access to the data is strictly enforced, once within the OIG PANDA environment. Passwords must be changed every 90 days.

The exposure/risk to privacy is low. The data was originally collected primarily from USDA agencies and OIG components, such as, Investigations, Audit, Management, and FOIA. 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 serve as a backup. In case of emergency, we would use the backup data to restore production data.

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

Data is neither analyzed nor produced. It's a backup system.

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

The system is designed to store data that may have been extracted from 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 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 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, 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 PANDA 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 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)?

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.

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. Access to data is controlled via role based access control, which limits risk of adverse use.

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?

Only individuals approved by OIG management will be allowed access to information on the OIG PANDA. PANDA information is never shared. When GSS information is shared, it is shared from GSS and not shared from PANDA.

4.2 How is the information transmitted or disclosed?

PANDA information is never disclosed. When GSS information is disclosed, it is transmitted from GSS and not transmitted from PANDA.

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?

PANDA information is never shared. When GSS information is shared, it is shared from GSS and not shared from PANDA.

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.

PANDA information is never shared. When GSS information is shared, it is shared from GSS and not shared from PANDA.

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

PANDA information is never shared. When GSS information is shared, it is shared from GSS and not shared from PANDA.

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, including Rules of Behavior.

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 OIG PANDA 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 OIG PANDA; 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?

PANDA does not collect data.

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.

Information is not gathered by OIG directly from individuals, therefore no notice can be provided.

The information contained in OIG PANDA 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-1/9). 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?

Information is not gathered by OIG directly from individuals, therefore no notice can be provided. Individuals cannot and may not access 'their' information in PANDA.

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

Information is not gathered by OIG directly from individuals, therefore no notice can be provided. Individuals cannot and may not access 'their' information in PANDA.

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

Information is not gathered by OIG directly from individuals, therefore no notice can be provided. Individuals cannot and may not access 'their' information in PANDA.

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

Information is not gathered by OIG directly from individuals, therefore no notice can be provided. Individuals cannot and may not access 'their' information in PANDA.

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

Information is not gathered by OIG directly from individuals, therefore no notice can be provided. Individuals cannot and may not access 'their' information in PANDA.

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 two-factor authentication, and complex passwords, software controls, and Individuals must also pass the mandatory USDA Information Security Awareness training and sign the Rules of Behavior forms before gaining access to the system. All OIG users who have access to PANDA are trained IT administrators who must complete the Administrator Rules of Behavior.

8.2 Will Department contractors have access to the system?

OIG contractors will have access to the system; however, USDA contractors from outside OIG 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.
- 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 provides access to privacy policies and guidelines to all employees. OIG routinely sends reminders to all users regarding Privacy policies and PII protections.
- All OIG users who have access to PANDA are trained IT administrators who must complete the Administrator Rules of Behavior and must complete Administrator Training.

8.4 Has Assessment and Authorization (A&A) 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?

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.

Access to data by all authorized users is monitored using automated controls. The information is accessed by authorized users at the time that a data restoration action is needed.

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.

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 cloud service offering. S3 storage buckets are "SaaS" software as a service in the cloud. Other AWS offerings in PANDA may be IaaS infrastructure as a service.

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

S3 (data) storage buckets must be protected, encrypted at rest, allow only access that is monitored and controlled (and authenticated by two factors). In no case may any OIG S3 bucket be allowed to be accessed/accessible from the public, except from specified authorized OIG endpoints and OIG networks.

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 any other 3rd party websites/applications except for AWS S3 buckets and Microsoft 365 Office SharePoint / OneDrive to store or manipulate OIG data. PANDA does not use any 3rd party websites/applications to collect information.

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

OIG will not use any other 3rd party websites/applications except for AWS S3 buckets and Microsoft 365 Office SharePoint / OneDrive to store or manipulate OIG data. PANDA does not use any 3rd party websites/applications to collect information.

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

OIG will not use any other 3rd party websites/applications except for AWS S3 buckets and Microsoft 365 Office SharePoint / OneDrive to store or manipulate OIG data. PANDA does not use any 3rd party websites/applications to collect information.

Information collected into GSS was used to conduct analyses to promote economy, efficiency, and effectiveness, and prevent fraud in USDA programs and operations. Information stored in PANDA, i.e. GSS backup data, is used only for the sole purpose of data restoration actions back to the original GSS data if and when such a restoration becomes necessary.

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?

OIG will not use any other 3rd party websites/applications except for AWS S3 buckets and Microsoft 365 Office SharePoint / OneDrive to store or manipulate OIG data. PANDA does not use any 3rd party websites/applications to collect information.

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 and audit logging. 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?

OIG will not use any other 3rd party websites/applications except for AWS S3 buckets and Microsoft 365 Office SharePoint / OneDrive to store or manipulate OIG data. PANDA does not use any 3rd party websites/applications to collect information.

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

N/A

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

OIG will not use any other 3rd party websites/applications except for AWS S3 buckets and Microsoft 365 Office SharePoint / OneDrive to store or manipulate OIG data. PANDA does not use any 3rd party websites/applications to collect information.

Information collected using 3rd party websites/applications will be stored in a secure manner within the OIG PANDA 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?

OIG will not use any other 3rd party websites/applications except for AWS S3 buckets and Microsoft 365 Office SharePoint / OneDrive to store or manipulate OIG data. PANDA does not use any 3rd party websites/applications to collect information.

Information collected from 3rd party websites/applications will not be shared

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 become externally available on 3rd party websites/applications therefore no modification of the current system or record notice is needed. The SharePoint, OneDrive, and S3 buckets that OIG leverages to store and process data do not ever make PII data available to anyone outside OIG.

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 Privacy Impact Analysis: 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 PANDA data stored on AWS will be stored, manipulated, or become externally available on any 3rd party websites/applications other than Amazon so those privacy risks are mitigated. OIG's contract with Amazon Web Services ("AWS") prevents AWS from sharing any data.

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 OIG PANDA 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 OIG PANDA system.

Responsible Officials

Name: John Trifiletti

Title: Chief Information Officer (CIO), Information Technology Division (ITD), Office of Inspector General (OIG), United States Department of Agriculture (USDA)

Name: Eric Silberman

Title: Chief Information Security Officer (CISO), Information Technology Division (ITD), Office of Inspector General (OIG), United States Department of Agriculture (USDA)

Approval Signature

JOHN TRIFILETTI
Digitally signed by JOHN TRIFILETTI
Date: 2023.04.19 16:12:23 -04'00'

John Trifiletti
Chief Information Officer (CIO), Information Technology Division (ITD), Office of Inspector General (OIG), United States Department of Agriculture (USDA)

Date

ERIC SILBERMAN
Digitally signed by ERIC SILBERMAN
Date: 2023.04.19 16:35:44 -04'00'

Eric Silberman
Chief Information Security Officer (CISO), Information Technology Division (ITD), Office of Inspector General (OIG), United States Department of Agriculture (USDA)

Date

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
GSS	General Support System
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 (“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 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*