Privacy in the Shared Service Environment

Shared Service Provider

- Shared Service Provider (SSP) is a Federal organization that provisions one or more business capabilities or services from a shared platform to one or more customer/partner Agencies. SSPs strive to deliver the best value in the Federal Government for the specific service they provide, and guarantee a high level of quality and reliability to maintain trust and confidence by customers.
- Provides significant cost savings or cost avoidance and yield improvements in agency operations.
- Required to ensure that services are designed and tested to meet all security, privacy and accessibility requirements.
- Interior Business Center was approved by OMB as an Interagency Shared Service Provider for financial management, human resources and acquisitions lines of businesses.
- There may be challenges to be addressed for privacy compliance in a shared services environment.
- It is important to understand roles and responsibilities in a shared service environment.

PIA Challenges in a Shared Services Environment

- Per the E-Government Act of 2002, agencies are required to conduct PIAs for electronic information systems.
- The PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and processes for handling information to mitigate potential privacy risks.
- SSPs must clarify PIA responsibilities with customers.
- PIA responsibilities depend on the system ownership, hosting or service provided. There may be some confusion over system ownership, hosting, data ownership/data processing that should be clarified.
- Moving to shared services triggers PIA requirement as the move affects how PII data is handled, protected, and stored.

PIA Responsibilities in a Shared Services Environment

- There is a key distinction between the system (application) and the system of records (data). The Privacy Act SORN requirement is for the data owner (customer agency), but the PIA requirement is related to the system, access controls for the IT system, and system owner.
- The PIA is the responsibility of the system owner for the application, though the assessment and controls may be based on the data - but that doesn't transfer legal responsibility for that data to the system owner.
- Customer agency is the data owner and defines the data they collect and use, and has accountability for compliance, audits, accuracy of data, reporting to all external stakeholders: OMB, congress, citizens, etc.
- In some cases, the customer agency is responsible for the PIA for their application or project - only the customer knows about the sensitivity and handling requirements for their data.
- SSP is responsible for PIA for their system/platform/service/hosting environment - Customer agency and SSP review/accept each other's PIA and privacy/security controls.
- SSP must establish standard operating procedures, clear roles and responsibilities - clearly stated in shared service agreements.
- SSP is responsible for systems and access to the systems that they own/offer/support/manage.
- Agency customers retain responsibility for properly securing system interfaces. Accountability does not transfer to the Provider.
- Create standard inter-agency agreements, MOUs, shared service agreements, SLAs, contracts - creates baseline, reduce confusion, improves compliance, and manage expectations for both parties.

SORN Challenges in a Shared Services Environment

- Shared service providers must clarify SORN responsibilities with customers
- Managing a Privacy Act system of records in a Shared Services environment may cause confusion over data ownership, records processing, and other responsibilities under the Privacy Act.
- SORNs are notices published by agencies that identify the legal authority for collecting and storing information about individuals in a system of records, where the system is located, responsible official/system manager, types of information collected, how records will be used and shared, how individuals may access or amend their records, etc.
- Moving to Shared Services triggers publication of a new or updated SORN as this represents a change in record handling practices.

SORN Responsibilities in a Shared Service Environment

- The agency customer owns the data and is responsible for meeting requirements under the Privacy Act
- Customer agency has accountability for audits and accuracy of data reporting to all external stakeholders: congress, citizens, etc.
- Shared Service Provider is responsible for systems and access to the systems
- In some case the Shared Service Provider is responsible for data entry or other processes; however, ultimate accountability for data is with the customer agency
- Customer agency defines the data they collect, use, and disseminate
- Customer agency reviews and accepts the Shared Service Provider's SORN, PIA, and privacy/security controls
- Agency owner is accountable for Privacy Act requests, redress, information sharing agreements, security, records and FOIA compliance, audits, litigation, etc.

External Requests

- Customer agency is Data Owner so the SSP should pass any external requests for information back to the customer. Ensure this responsibility to clearly defined and recorded, as appropriate, in the MOUs, IAAs, Contracts, and SLAs
- Office of the President, including OMB
- Congressional (testimony and GAO)
- Audit Groups (Inspectors General, DOJ, DHS, FISMA Audits)
- Individuals included within the system (PIA)
- Privacy Offices
- National Archives
- FOIA requests
- Court Orders