Issue Date: 6/25/2008
Revision Date: <mm/dd/yyyy>

Document Purpose

This Practices Guide provides a limited overview of best practices, activities, attributes, and related templates, tools, information, and key terminology for performing and maintaining Privacy Impact Assessments (PIAs). For more detailed information, please see the existing guidelines maintained by the Department of Health and Human Services (HHS) information security and privacy program, Secure One HHS, in the *Practice Related Templates, Tools, and Information* section below.

Background

The Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC) is a framework to enhance Information Technology (IT) governance through rigorous application of sound investment and project management principles, and industry best practices. The EPLC provides the context for the governance process and describes interdependencies between its project management, investment management, and capital planning components. The EPLC framework establishes an environment in which HHS IT investments and projects consistently achieve successful outcomes that align with Department and Operating Division goals and objectives.

Titles II and III of the E-Government Act of 2002 require that agencies evaluate systems that collect personally identifiable information (PII) to determine that the privacy of this information is adequately protected. The mechanism by which agencies perform this assessment is a PIA. In accordance with federal legislation and HHS guidance, operating divisions (OPDIVs) are responsible for completing and maintaining PIAs on all systems (developmental and operational). Systems which only house federal employee PII are similarly bound by this requirement. The tool used to assess compliance is the PIA Form located within the current Security and Privacy Online Reporting Tool (SPORT), which provides an automated ability to complete PIAs. Upon completion of each assessment, agencies are required to make PIAs publicly available.

Practice Overview

To assess whether systems are compliant with these federal requirements, system owners, system managers, Senior Officials for Privacy (SOP), and other designated PIA authors should use the standard HHS PIA methodology. The Department requires that a PIA be completed for all IT systems, regardless of whether or not the system contains personally identifiable information. HHS uses the SPORT to automate the collection and reporting of both Federal Information Security Management Act (FISMA) and Privacy-related system information and milestones. The use of this automated tool allows the Department and OPDIVs a streamlined method for producing consistent audit reports for FISMA, Exhibit 300, Exhibit 53, and PIAs.

Best Practices

- **Begin Early** – Well before establishing any detailed design requirements, system owners can estimate the type of data a system may use and share during its planned operation and determine if this information is PII. This determination will affect both technical design requirements and administrative reporting requirements later in the project.
- **Use SPORT** – SPORT is available at https://prosight-fisma.hhs.gov. The online tool facilitates the completion of PIAs by guiding PIA authors through the PIA process. It also simplifies the transfer of information to other audit reports as well as simplifying the publication of new and updated PIA to the HHS website.
- **Coordinate** – The information captured in a PIA is reported through a number of critical public reports. Engaging the Business, development, privacy and security stakeholders, ensures that designs and audits represent the appropriate level of security required to protect the information. For a new PIA, the PIA author must consult the OPDIV SOP, OPDIV Privacy Act Officer, OPDIV

Capital Planning and Investment (CPIC) Contact, and system owner to coordinate the details on characterizing the system.

- **Maintain and Update** – The PIA is a living document that must be reviewed periodically and updated whenever a major change occurs to a system. For a list of what constitutes a major change, please see the HHS PIA Guide (2.2.4) or OMB M-03-22, *Guidelines for Implementing the Privacy Provisions of the E-Government Act of 2002*.

Practice Activities

Detailed practice activities can be found in the *Secure One HHS Privacy Impact Assessment (PIA) Guide* (http://intranet.hhs.gov/infosec/docs/policies_guides/PIA/PIA_Guide.doc) and the *Secure One HHS Privacy in the System Development Lifecycle* document (http://intranet.hhs.gov/infosec/docs/polices_guides/PIA/Privacy_in_SDLC.doc). Please note that this document utilizes the NIST defined system development phases which do not directly map to the EPLC phases. Please see the *EPLC Security Approach Guide* (EPLC LINK) for a discussion of how the NIST and EPLC phases correlate.

The Secure One HHS Privacy Impact Assessment (PIA) Guide outlines eight steps to the PIA process.

1. **Determine when a PIA must be conducted** – PIAs must be conducted for all new systems and whenever a major change occurs to a system.
2. **Assign roles and responsibilities** – The OPDIV SOP must designate the necessary staff to complete PIAs for each system.
3. **Prepare to begin the PIA** – PIA authors must familiarize themselves with the PIA process, the PIA tool, and the PIA Form located in the current tool.
4. **Compose a PIA** – Once the PIA author has been identified and system documentation has been gathered, the PIA is ready to be completed.
5. **Characterize the System** – The PIA Form includes a section characterizing the identity, data components, and functions of the system under consideration. A PIA cannot be finalized until the system boundaries are identified and the security requirements are established. The remainder of the PIA process will need to wait until the system is passing into the Implementation phase in order to be finalized and submitted to the OPDIV SOP.
6. **Complete the PIA** – All fields of the PIA form are completed and the PIA is submitted to the OPDIV SOP via SPORT. Upon approval, the OPDIV SOP can promote the PIA to the Department for approval, or demote it to the completion point of contact to make any necessary changes.
7. **Approve or demote the PIA** – The Department reviews the PIA and can approve or demote it for OPDIV adjustment.
8. **Maintain the PIA** – A PIA is a living document that must be updated when a major change in the system occurs.

For step-by-step information on how to complete the PIA in SPORT, please see *Appendix E: PIA Question-by-Question Tutorial* in the HHS PIA Guide. Additional information can be found in the PIA Training course located at http://intranet.hhs.gov/infosec/docs/education/privacy_impact/wrapper.html.

Practice Related Information

- HHS EPLC Security Approach
- HHS published Privacy Impact Assessments
  http://www.hhs.gov/pia/
- Secure One HHS Privacy Impact Assessment (PIA) Guide
  http://intranet.hhs.gov/infosec/docs/policies_guides/PIA/PIA_Guide.doc
- Secure One HHS Privacy Impact Assessment (PIA) Training
  http://intranet.hhs.gov/infosec/docs/education/privacy_impact/wrapper.html
- Security and Privacy Online Reporting Tool (SPORT)
  https://prosight-fisma.hhs.gov/
- HHS HIPAA Compliance Guide, Office of Civil Rights (OCR)
  http://www.hhs.gov/ocr/hipaa/
- HHS Privacy Contacts
  http://www.hhs.gov/contacts/privacy.html

- HHS IRM Information Security Program Policy, Section 3.8 Privacy Impact Assessments
  http://www.hhs.gov/ocio/policy/2004-0002.001.html#privacy
- NIST Special Publication (SP) 800-64, *Security Considerations in the System Development Life Cycle Revision 2*
  http://csrc.nist.gov/publications/drafts/800-64-rev2/draft-SP800-64-Revision2.pdf

Practice Key Terms

IIF – Information in Identifiable Form
PII – Personally Identifiable Information
***Privacy Act* System of Records Notice (SORN)** - all systems with *Privacy Act* information contained within them are required to publish a "Records Notice" in the Federal Register that informs the public what information is contained in the system, how it is used, how individuals may gain access to information about themselves, and other specific aspects of the system.
Privacy Impact Assessment (PIA)—a methodology that provides information technology (IT) security professionals with a process for assessing whether appropriate privacy policies, procedures, and business practices—as well as applicable administrative, technical and physical security controls—have been implemented to ensure compliance with federal privacy regulations.
SOP - Senior Official for Privacy
System of Records (SOR)—a group of records under the control of any agency where information is retrieved by the name of the individual, by some identifying number or symbol, or by other identifiers assigned to the individual.