



# Information Security Program

## Privacy Impact Assessment (PIA) Guide

January 10, 2007



# Table of Contents

<b>Table of Contents</b> .....	<b>i</b>
<b>Preface</b> .....	<b>iii</b>
<b>Document Change History</b> .....	<b>iv</b>
<b>1. Introduction</b> .....	<b>1</b>
1.1 Purpose .....	1
1.2 Background.....	1
1.3 Scope.....	2
1.4 Document Organization .....	2
<b>2. Federal Privacy Requirements</b> .....	<b>3</b>
2.1 Federal Statutes .....	3
2.1.1 <i>The Privacy Act of 1974</i> .....	3
2.1.2 <i>The E-Government Act of 2002</i> .....	3
2.1.3 <i>The Children’s Online Privacy and Protection Act (COPPA) of 1998</i> ..	4
2.1.4 <i>The Clinger-Cohen Act of 1996</i> .....	4
2.1.5 <i>The Health Insurance Portability and Accountability Act (HIPAA) of 1996</i> .....	4
2.1.6 <i>The Paperwork Reduction Act (PRA) of 1995</i> .....	4
2.1.7 <i>The Computer Matching and Privacy Protection Act of 1988</i> .....	5
2.1.8 <i>The Freedom of Information Act (FOIA) of 1966</i> .....	5
2.2 Federal Memoranda and Other Guidance .....	5
2.2.1 OMB Circular A-130, Appendix III .....	5
2.2.2 OMB Circular A-11.....	6
2.2.3 OMB Memorandum 01-05.....	6
2.2.4 OMB Memorandum 03-22.....	7
2.2.5 OMB Memorandum 05-08.....	8
2.2.6 OMB Memorandum 06-16.....	8
2.2.7 OMB Memorandum 06-20.....	8
<b>3. PIA Roles and Responsibilities</b> .....	<b>9</b>
3.1 Department Level Roles and Responsibilities .....	9
3.1.1 HHS Senior Agency Official for Privacy .....	9
3.1.2 Inspector General (IG).....	10
3.1.3 HHS Privacy Act Officer .....	10
3.2 OPDIV Level Roles and Responsibilities .....	10
3.2.1 OPDIV Chief Information Security Officer (CISO) .....	10
3.2.2 OPDIV Senior Official for Privacy (SOP) .....	11
3.2.3 OPDIV Privacy Contact.....	12
3.2.4 System PIA Author .....	13
3.2.5 System Owners/ Program Managers .....	13
3.2.6 Website Owners/ Administrators .....	13
<b>4. Privacy Impact Assessment Process</b> .....	<b>14</b>
4.1 PIA Overview .....	14

4.1.1	Purpose of the PIA .....	14
4.1.2	Benefits of PIA.....	15
4.1.3	Scope.....	15
4.1.4	Timing.....	15
4.2	PIA Activities.....	16
4.2.1	Step One: Determine When a PIA Must Be Conducted .....	16
4.2.2	Step Two: Assign Roles and Responsibilities.....	16
4.2.3	Step Three: Prepare to Begin the PIA.....	16
4.2.4	Step Four: Compose a PIA.....	17
4.2.5	Step Five: Characterize the System .....	18
4.2.6	Step Six: Complete the PIA .....	18
4.2.7	Step Seven: Approve or Demote the PIA .....	19
4.2.8	Step Eight: Maintain the PIA.....	19
<b>5.</b>	<b>Conclusion.....</b>	<b>20</b>
	<b>Appendix A: Document Feedback .....</b>	<b>21</b>
	<b>Appendix B: References .....</b>	<b>22</b>
	<b>Appendix C: Acronyms .....</b>	<b>25</b>
	<b>Appendix D: Glossary .....</b>	<b>27</b>
	<b>Appendix E: PIA Question-by-Question Tutorial .....</b>	<b>30</b>

## Preface

---

As the Department of Health and Human Services (HHS) Information Security Program evolves, this document will be subject to review and update. The *HHS Privacy Impact Assessment (PIA) Guide* will undergo such changes annually, or whenever alterations occur, which suggest that the HHS PIA Guide's content should be modified. These changes may include the following:

- Modifications of roles and responsibilities;
- Release of new executive, legislative, technical, or Departmental guidance;
- Guidance issued from the Office of Management and Budget (OMB);
- Identification of changes in governing policies;
- Changes in vulnerabilities, risks, or threats; and/or
- HHS Inspector General (IG) findings that stem from a security audit.

The HHS Chief Information Security Officer (CISO) must approve all revisions to the *HHS PIA Guide*. Revisions are to be highlighted in the Document Change History table. Each revised guidance document is subject to HHS' document review and approval process before becoming final. When it is approved, a new version of the *HHS PIA Guide* will be issued and all affected parties will be informed of the changes made.

The procedures outlined in the *HHS PIA Guide* are proven practices that will provide guidance to the Department in meeting or exceeding the baseline requirements identified in the *HHS Information Security Program Policy* document. The *HHS PIA Guide* provides specific information for the recommended implementation of Privacy compliance. While the specifics of how to undertake the implementations are not mandatory, any security implementation undertaken by an Operating Division (OPDIV) must result in security controls and processes that are equal to, or stronger than, those articulated in the policies, handbooks, and related guides. If an OPDIV or Staff Division (STAFFDIV) chooses not to adopt the baseline guidance set forth in this *HHS PIA Guide*, it must document this decision and assume responsibility for the creation of procedures of equal or greater stringency.

## Document Change History

<b>Version Number</b>	<b>Release Date</b>	<b>Summary of Changes</b>	<b>Section Number/ Paragraph Number</b>	<b>Changes Made By</b>
1.0	07/12/2004	Final Document Release with content changes	N/A	N/A
1.1	03/16/2005	Release with content changes	1.4,4.2.8, 4.2.9, Appendix E	N/A
2.0	07/19/2005	Updated to reflect new HHS guidance and regulatory requirements.	Throughout	HHS CISO
3.0	07/26/2006	Updated to reflect data migration and process changes.	Throughout	Secure One HHS
3.1	01/10/2007	Updated Roles and Responsibilities	Throughout	Secure One HHS

# 1. Introduction

---

HHS is responsible for implementing and administering an information security program to protect its information resources. The program will comply with applicable public laws, federal regulations, and Executive Orders (E.O.), including the *Federal Information Security Management Act (FISMA) of 2002*; the *Privacy Act of 1974*; the *Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources*, dated November 28, 2000; OMB Memorandum 06-20; OMB Memorandum 05-08; and the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. To meet these requirements, the Department has instituted the *HHS Information Security Program Policy* document and the accompanying *HHS Information Security Program Handbook*.

The *HHS PIA Guide* is part of the HHS Information Security Program, and serves as a resource for complying with Title II and III of the *E-Government Act of 2002* regarding PIA requirements.

For the purposes of this guide, the term “Department” or “Departmental” is inclusive of HHS and the OPDIVs.

## 1.1 Purpose

This guide outlines a standard approach for conducting a PIA for all Departmental systems, including developmental, operational, FISMA, contractor-owned, grantee, information technology (IT) general support systems (GSS), major applications (MA), and non-major applications. It also provides detailed instructions which aid in properly populating the PIA. Completing this form will assist the Department in incorporating privacy protections into every stage of an IT system’s life cycle. This guide also provides a summary of federal legislative, regulatory, and guidance requirements related to protecting information in identifiable form (IIF) contained in Departmental systems.

## 1.2 Background

The federal government has recognized the advantages and risks of IT, as reflected in new or improved IT security standards for federal departments and agencies. By providing this guide, the Department also recognizes the public’s growing demand that government entities protect the privacy of IIF residing in public sector, grantee, and contractor-owned information systems.

Since the Department handles a large amount of IIF that is protected by federal law, the Department must follow federal privacy guidelines. Private and public sector organizations interacting with HHS and/or the OPDIVs must be assured that sensitive information is protected in a manner that will ensure the confidentiality, integrity, and availability of the data.

## 1.3 Scope

All Departmental systems should have a current PIA to ensure compliance with the *E-Government Act of 2002*, other relevant IT privacy requirements, and HHS Departmental policy. This guide applies to all Departmental personnel, which includes the OPDIVs and contractors responsible for managing and operating systems. This guide will familiarize Departmental personnel with the IT privacy requirements set forth in the *Privacy Act of 1974*, *HIPAA*, the *E-Government Act of 2002*, OMB Circulars A-11, *Preparation, Submission and Execution of the Budget*, and A-130, as well as other applicable information privacy laws and regulations.

## 1.4 Document Organization

The remainder of this guide is structured as follows:

- Section 2 provides an overview of IT privacy-related legislative and regulatory requirements and guidance.
- Section 3 identifies the roles and responsibilities of PIA stakeholders.
- Section 4 describes the process of completing and submitting a PIA.
- Section 5 provides a conclusion, summarizing the points of this guide.

This guide also contains the following appendices:

- Appendix A provides a feedback form to submit comments on this document to HHS.
- Appendix B lists the references used in this document.
- Appendix C lists the acronyms used in this document.
- Appendix D defines terms most frequently used in this document.
- Appendix E provides a question-by-question tutorial to assist in populating the PIA Form.

## 2. Federal Privacy Requirements

---

Privacy and security are closely interrelated, and are a source of great concern for IT managers and system owners. The legislative and regulatory requirements, as well as the guidance, summarized in this section reflect the evolving federal approach of integrating privacy requirements into overall IT security programs and plans. The PIA requirement mandated by the *E-Government Act of 2002* is a step in this development. The questions asked in the PIA correspond to principles and requirements set out by the federal laws and regulations described in this section.

### 2.1 Federal Statutes

Public laws require federal agencies to protect the privacy of IIF residing within their agencies, improve the management of IT resources, and establish agency IT security programs. Applicable statutes, including major legislation, such as the *E-Government Act of 2002* and the *Privacy Act of 1974*, are described below. Other federal authorities referenced in this guide are listed in Appendix B, References.

The material in this guide is consistent with federal laws and guidance existing at the time it was drafted. It will be updated as federal legislation and regulations change or are made available.

#### 2.1.1 *The Privacy Act of 1974*

The *Privacy Act of 1974* protects the privacy of individuals by establishing “Fair Information Practices” for the collection, maintenance, use, and dissemination of information by federal agencies. The *Privacy Act*, along with its accompanying case law, is the most significant milestone in the history of the protection of the privacy of personal information held by the federal government. Many subsequent laws, regulations, and guidance build upon the principles first articulated in the *Privacy Act*.

#### 2.1.2 *The E-Government Act of 2002*

Title II of the *E-Government Act of 2002* requires federal agencies to conduct PIAs before developing or procuring IT systems that collect, maintain, or disseminate IIF. Once completed, the agency’s Chief Information Officer (CIO), or an equivalent official, must review the PIAs. Additional requirements include making PIAs publicly accessible and posting a machine-readable privacy notice on publicly facing websites.

Title III of the *E-Government Act*, known as FISMA, superseded and made permanent some of the provisions of the *Government Information Security Reform Act of 2000* (GISRA). FISMA amends the *Paperwork Reduction Act (PRA) of 1995* by adding a new subchapter on information security that requires certain program

management, evaluation, and reporting activities, such as performing an annual self-assessment and conducting an independent assessment by each agency's IG.

### **2.1.3 The Children's Online Privacy and Protection Act (COPPA) of 1998**

The *COPPA* applies to private sector websites that collect personal information online from children under the age of 13. OMB Memorandum (M)-00-13, *Privacy Policies and Data Collection on Federal Web Sites* (June 22, 2000), extended the provisions of COPPA to federal websites. COPPA identifies the content that a website operator must include in a privacy policy, outlines when and how to seek verifiable consent from a parent, and specifies the responsibilities an operator has for protecting children's privacy and safety online.

### **2.1.4 The Clinger-Cohen Act of 1996**

The *Clinger-Cohen Act of 1996* (which includes both the *Information Technology Management Reform Act* and the *Federal Acquisition Reform Act*) is intended to improve the productivity, efficiency, and effectiveness of federal programs through the improved acquisition, use, and disposal of IT resources. Among other effects, it makes agencies responsible for IT resource acquisition and management, under the guidance of the CIO, and emphasizes that value must be maximized and risk must be minimized in capital planning and budget processes. In effect, the *Clinger-Cohen Act* places the burden of incorporating privacy controls into IT investments at the agency and CIO levels.

### **2.1.5 The Health Insurance Portability and Accountability Act (HIPAA) of 1996**

HIPAA affects the health insurance industry and contains provisions under the heading of "Administrative Simplification" that govern how government and private sector health care institutions handle protected health information (PHI), a subset of "individually identifiable health information." Pursuant with these provisions, regulations published in 2000 established standards for providing notice on how to use and disclose health information collected from users under a covered entity's services. These regulations also grant certain rights to individuals, including the right to see one's health records and to request corrections or other amendments to those records. These regulations apply to both written and oral PHI.

Further discussion of HIPAA requirements, compliance, and implementation can be found in the *HHS HIPAA Compliance Guide* and the HHS Office of Civil Rights (OCR) HIPAA Privacy Web page at <http://www.hhs.gov/ocr/hipaa/>.

### **2.1.6 The Paperwork Reduction Act (PRA) of 1995**

PRA focuses on increasing the efficiency of the federal government's information collection practices. The PRA specifies that CIOs shall improve protection for the privacy and security of information under their agency's control. The PRA also

created the Office of Information and Regulatory Affairs (OIRA) within OMB to provide central oversight of information management activities across the federal government. Furthermore, the PRA requires agencies to receive an OMB information collection approval number (also known as an “OMB control number”) for an information system, prior to using that system to collect information from any person.

### **2.1.7 The Computer Matching and Privacy Protection Act of 1988**

The *Computer Matching and Privacy Protection Act of 1988* added several new provisions to the *Privacy Act of 1974*. “Computer matching” occurs when federal and/or state agencies share IIF. Agencies use computer matching to conduct many government functions, including establishing or verifying eligibility for federal benefit programs, or identifying payments/debts owed to government agencies. The *Computer Matching and Privacy Protection Act* requires agencies engaged in computer matching activities to:

- Provide notice to individuals if their IIF is being computer matched;
- Allow individuals the opportunity to refute adverse information before having a benefit denied or terminated; and
- Establish data integrity boards to oversee computer-matching activities.

### **2.1.8 The Freedom of Information Act (FOIA) of 1966**

FOIA requires all agencies of the executive branch to disclose federal agency records or information upon receiving a written request from any individual, except for those records (or portions of them) that are protected from disclosure by certain exemptions and exclusions.<sup>1</sup>

## **2.2 Federal Memoranda and Other Guidance**

The Department must also comply with OMB guidance when implementing the previously mentioned legislation. This section highlights important OMB memoranda on privacy and security.

### **2.2.1 OMB Circular A-130, Appendix III**

OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, requires agencies to implement security requirements for, and to protect personal information in, automated information systems. Appendix III provides specific guidelines for implementing these requirements, including a minimum set of controls for federal automated information programs. Appendix III also assigns federal agency responsibilities for the security of automated information; and links agency

---

<sup>1</sup> For more information on FOIA, its exemptions, and exclusions, see the Department of Justice, *FOIA Reference Guide* available at [http://www.usdoj.gov/04foia/04\\_3.html](http://www.usdoj.gov/04foia/04_3.html).

automated information security programs and agency management control systems established in accordance with OMB Circular A-123, *Management Accountability and Control*. OMB Circular A-130 requires agencies to adopt three types of security controls:

- **Assigning Responsibility for Security:** Responsibility for the security of IT systems must be assigned to a person with the appropriate qualifications, ability, and authority to provide security.
- **Planning for Security:** System security plans should be incorporated into the organization's information resource management planning process, consistent with guidance issued by the National Institute of Standards and Technology (NIST).
- **Reviewing Security Controls:** Agencies must review security controls whenever significant modifications are made, or at least once every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk. It is important to consider whether personal information is contained in the system when assessing risk.

### 2.2.2 OMB Circular A-11

OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, provides guidance to federal agencies regarding the preparation and submission of budget estimates to OMB. Section 31.8 of Circular A-11 requires that agency estimates "reflect a comprehensive understanding of OMB security policies and NIST guidance." This understanding needs to be supported by the following measures:

- Identifying additional security controls for systems that promote or permit public access, other externally accessible systems, and those that are interconnected with systems over which program officials have little or no control;
- Demonstrating how the agency ensures the effective use of security controls and authentication tools to protect privacy for those systems that promote or permit public access; and
- Demonstrating how the agency ensures that handling personal information is consistent with relevant government-wide and agency processes.

### 2.2.3 OMB Memorandum 01-05

OMB M-01-05 provides guidance on implementing the *Computer Matching and Privacy Protection Act of 1988*. Prior to any data sharing, the guidance states that agencies must "review and meet the *Privacy Act* requirements for computer matching, including developing a computer matching agreement and publishing notice of the proposed match in the Federal Register." The memorandum then states that it "puts forth principles on protecting personal privacy when conducting inter-agency data sharing," including:

- Notice
- Consent, as appropriate
- Re-disclosure limitations
- Accuracy
- Security controls

While M-01-05 stresses these privacy protections, it also discusses additional privacy protections in a section entitled "Other Guidance". These additional privacy protections are:

- Employing the principle of minimization;
- Employing the principle of accountability; and
- Conducting PIAs.

#### **2.2.4 OMB Memorandum 03-22**

OMB has provided federal agencies with M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003. This guidance directs agencies to conduct reviews on how technology is implemented to collect new information, and how to collect IIF with a recently purchased or newly developed IT system. According to OMB M-03-22, PIAs should be conducted following any major changes, including, but not limited to:

- **Conversions:** A conversion from paper-based methods to electronic systems.
- **Anonymous to Non-Anonymous:** The system's function, as applied to an existing information collection, changes anonymous information into IIF.
- **Significant System Management Changes:** In the case that new uses of an existing IT system, including application of new technologies, significantly change the process of managing IIF in the system.
- **Significant Merging:** When agencies adopt or alter business processes so that government databases holding IIF are merged, centralized, matched with other databases, or otherwise significantly manipulated.
- **New Public Access:** When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system, which can be accessed by the public.
- **Commercial Sources:** IIF, obtained from commercial or public sources, is systematically integrated into the existing information systems database.
- **New Interagency Uses:** When agencies work together on shared functions involving significant new uses or exchanges of IIF.
- **Internal Flow or Collection:** When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional IIF.
- **Alteration in Character of Data:** When new IIF added to a collection raises the risks to personal privacy, such as the addition of health or privacy information.

### **2.2.5 OMB Memorandum 05-08**

OMB has provided federal agencies with M-05-08, *Designation of Senior Agency Officials for Privacy*. This document provides guidance, which aids in establishing the role of the Senior Agency Official for Privacy (SAOP) as having the overall responsibility for:

- Overall Department-wide responsibility for information privacy issues;
- Overall responsibility and accountability for ensuring the Department's implementation of information privacy protections; and
- Playing a central role in overseeing, coordinating, and facilitating the Department's privacy compliance efforts.

### **2.2.6 OMB Memorandum 06-16**

OMB has provided federal agencies with M-06-16, *Protection of Sensitive Agency Information*. This guidance recommends agencies follow a checklist for protection of remote information provided by NIST, as well as four additional items provided by OMB. This guidance is an effort to properly safeguard information assets, while using information technology.

### **2.2.7 OMB Memorandum 06-20**

OMB has provided federal agencies with M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. This document assigns responsibility and provides guidance for the SAOP on how to complete the new privacy questions in the annual FISMA report. As a result, OMB will no longer ask agencies to include privacy related information in their annual E-Government Act submission. The Department has extended OMB M-05-08 and M-06-20 roles and responsibilities to the OPDIV level.

## 3. PIA Roles and Responsibilities

---

Congress and OMB have imposed special responsibilities on the HHS CIO and CISO that reinforce the Department's mission to protect personal information. The infrastructure provided by the HHS CIO, HHS CISO, and the HHS SAOP will be supported by OPDIV CISOs and Senior Officials for Privacy (SOPs), as well as a host of roles and responsibilities critical to the protection of personal information.

As such, Secure One HHS outlines individual responsibilities for specific privacy roles within HHS based upon the E-Government Act of 2002, the *Privacy Act* of 1974 as amended, and supporting OMB guidance. While each individual has specific responsibilities to collaborate with the Department and OPDIV privacy stakeholders, cooperation with the entire enterprise is also essential for information security and privacy compliance. Specifically, individuals supporting the HHS CISO and the HHS SAOP should be able to identify their roles and responsibilities, as they pertain to the support of the privacy initiatives of the HHS Information Security Program.

### 3.1 Department Level Roles and Responsibilities

At the Department level, PIAs are collected from OPDIVs using an automated tool. The PIAs are then reviewed for completeness and submitted to OMB. They are also made publicly available in accordance with legislative drivers. The involvement of the following stakeholders is highly encouraged so that PIAs may meet Departmental PIA requirements, and thus, be promoted to the Department.

#### 3.1.1 HHS Senior Agency Official for Privacy

At HHS, the CIO holds the title of SAOP, and is responsible for:

- Designating responsibility for oversight of the PIA process to the OPDIV SAOP;
- Reviewing completed PIAs, and attesting that they are adequately and accurately completed;
- Allocating proper resources to permit identification and remediation of privacy weaknesses;
- Approving HHS' submission of the Privacy Management portion of the annual FISMA report;
- Coordinating privacy-related reporting activities as mandated by federal legislation and OMB guidance;
- Ensuring the proper implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy, such as the *Privacy Act* of 1974;
- Maintaining appropriate documentation regarding compliance with information privacy laws, regulations, and HHS policies;

- Overseeing, coordinating, and facilitating the Department's privacy compliance efforts, including reviewing documented information privacy procedures to ensure they are comprehensive and up-to-date, and coordinating revision, as necessary;
- Ensuring the Department's employees, contractors, and stakeholders receive appropriate training;
- Providing education programs regarding the information privacy laws, regulations, policies, and procedures governing the Department's handling of personal information; and
- Maintaining a central policy-making role in the Department's development and evaluation of legislative, regulatory, and other policy proposals pertaining to information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information.

### **3.1.2 Inspector General (IG)**

The HHS IG is responsible for:

- Approving HHS' FISMA and Agency Privacy Management submission to OMB.

### **3.1.3 HHS Privacy Act Officer**

The HHS Privacy Act Officer is responsible for:

- Reviewing HHS *Privacy Act* System of Records Notices (SORN) prior to publication;
- Responding to and reviewing *Privacy Act* related questions in the Agency Privacy Management Report section of FISMA; and
- Implementing requirements of the *Privacy Act* and corresponding operating procedures.

## **3.2 OPDIV Level Roles and Responsibilities**

OPDIVs are responsible for conducting an initial PIA on each system, and maintaining PIAs throughout the system's existence. OPDIVs must complete each PIA and promote<sup>2</sup> each PIA to the Department for review.

### **3.2.1 OPDIV Chief Information Security Officer (CISO)**

The OPDIV CISOs are responsible for:

---

<sup>2</sup> See section 4.2.7 for explanation of promoting and demoting PIAs.

- Reporting to the HHS CISO on the effectiveness of the OPDIV's information privacy program, including progress of remedial actions;
- Managing internal privacy reviews of the OPDIV's business cases, alternatives analyses, and other specific investment documents;
- Obtaining contractual assurances from third parties to ensure that the third party will protect IIF in a manner consistent with the privacy practices of the Department and applicable laws, before enabling access to IIF;
- Ensuring that all employees and contractors comply with the privacy practices of the Department and applicable laws;
- Establishing a framework to facilitate the development and maintenance of PIAs for all systems;
- Managing and certifying an inventory of all current and proposed investments that contain a privacy control component;
- Coordinating privacy reporting activities as mandated by federal privacy legislation and OMB guidance;
- Coordinating with the OPDIV's SOP to develop the organization's information privacy program;
- Integrating and implementing privacy policies, procedures, and practices that are consistent with Departmental requirements to assure that systems, programs, and data are secure and protected from unauthorized access that might lead to the alteration, damage, or destruction of automated resources, and unintended release of data;
- Documenting security and privacy considerations in acquisition documents, and maintaining contractor compliance in a manner consistent with the privacy practices of the Department; and
- Supporting general privacy awareness and role-based training activities for all personnel using, operating, supervising, or managing IT systems.

### **3.2.2 OPDIV Senior Official for Privacy (SOP)**

The SOP title was extended by the Department to each OPDIV to effectively meet the reporting requirements outlined in OMB M-06-20. The agency requirement for the title is outlined in OMB M-05-08. OPDIV SOPs are responsible for:

- Promoting PIAs to the Department, and submitting them to the SAOP once complete or seeking revisions from the PIA author, if errors are found;
- Tracking and maintaining all PIA activities in the Department's PIA reporting tool;
- Reviewing completed PIAs and attesting that they are adequately and accurately completed;
- Developing and implementing Department privacy program initiatives throughout the development and integration of privacy policy and guidance into information security practices, where applicable;
- Reporting, in coordination with the OPDIV CISO, to the HHS CISO the effectiveness of the organization's information privacy program, including progress of remedial actions, as identified;

- Establishing and implementing privacy policies, procedures, and practices consistent with Departmental privacy requirements, in coordination with the OPDIV CISO;
- Obtaining contractual assurances from third parties to ensure that the third party will protect IIF in a manner consistent with the privacy practices of the Department, in coordination with the OPDIV CISO and privacy stakeholders;
- Establishing an OPDIV policy framework to facilitate the development and maintenance of PIAs for all systems based on Department and federal legislative requirements;
- Coordinating and ensuring that privacy education and awareness activities, specific to the OPDIV privacy culture, are established for all personnel using, operating, supervising, or managing computer systems;
- Reviewing all completed OPDIV PIAs for promotion to the Department;
- Tracking and maintaining all PIA activities in the current PIA reporting tool;
- Coordinating with OPDIV budgetary offices to ensure PIA and SORN activities are included as part of Exhibit 300 development;
- Reviewing and approving OPDIV FISMA and Privacy Management Report for submission to the Department;
- Coordinating OPDIV policy, guidance, and system-level documentation to ensure Department management, technical, and operational privacy requirements are addressed;
- Supporting the Department SAOP in ad hoc privacy reporting activities as necessary, including the maintenance of President's Management Agenda (PMA) and quarterly FISMA reporting activities;
- Making recommendations to senior level officials with budgetary authority to allocate proper resources to mitigate privacy weaknesses found in system PIAs;
- Complying with and maintaining the privacy goals of the PMA; and
- Approving the OPDIV FISMA and Privacy Management Report.

### **3.2.3 OPDIV Privacy Contact**

The OPDIV Privacy Contact is responsible for:

- Serving as a point of contact (POC) for issues related to the *Privacy Act* within the OPDIV;
- Maintaining awareness of privacy laws, regulations, and issues within the OPDIV;
- Maintaining an OPDIV SORN website to post current SORNs per the guidance of the Department Privacy Act Officer; and
- Supporting the OPDIV SOP and OPDIV CISO in completing required reviews, as defined by OMB A-130.

### **3.2.4 System PIA Author**

The role of the PIA author can be filled by the OPDIV Information System Security Officers (ISSOs), a system owner, or any other designee. Responsibilities for the PIA author include:

- Coordinating with appropriate OPDIV privacy stakeholders and completing PIAs;
- Identifying additional resources needed to complete PIAs;
- Submitting completed PIAs to the OPDIV SOP;
- Collaborating with the OPDIV SOP and system owners to collect information needed to complete PIAs;
- Updating (at the direction of the OPDIV CIO and the SOP) OPDIV management on the progress of PIA completion;
- Determining adequacy of the security controls that protect systems; and
- Determining whether systems are allowed to operate following consideration of the security controls that protect the integrity of IIF.

### **3.2.5 System Owners/ Program Managers**

The system owners/program managers are responsible for:

- Coordinating with appropriate OPDIV privacy stakeholders to complete system PIAs;
- Submitting complete PIAs to the OPDIV SOP and/or system or program management staff for review, as coordinated by OPDIV; and
- Working with the OPDIV SOP and system owners to collect information needed to complete PIAs.

### **3.2.6 Website Owners/ Administrators**

The website owners/administrators are responsible for:

- Identifying additional resources needed to complete machine-readable privacy policies;
- Ensuring that OPDIV websites do not employ persistent tracking technologies, or if technologies are in use, written authorization is issued from the HHS Secretary on an annual basis;
- Implementing, testing, and maintaining machine-readable privacy policies on existing websites and websites in development;
- Implementing, testing, and maintaining machine-readable policy reference files on any Web server that hosts an HHS website; and
- Ensuring that a privacy policy has been developed and is accessible as a link on each OPDIV webpage.

## 4. Privacy Impact Assessment Process

---

According to federal requirements and guidance, the Department is responsible for providing proper protections for IIF contained within its information systems. To assess whether systems are compliant with these federal requirements, system owners, system managers, SOPs, and other designated PIA authors should use the PIA methodology detailed in this section. The Department requires that a PIA be completed for all IT systems, regardless of whether or not the system contains IIF. Systems which only house federal employee IIF are similarly bound by this requirement. The tool used to assess compliance is the PIA Form located within the current PIA tool, which provides an automated ability to complete the PIA.

### 4.1 PIA Overview

This section provides a high-level explanation of the purpose, objective, timing, and scope of PIAs. Reviewing this information will provide a better understanding of the context and framework for conducting a PIA.

The PIA methodology consists of completing a PIA form. The first section of the PIA Form is the Summary tab, which collects data that is suitable to be made available via the Internet to the public as required by OMB M-03-22. The PIA Summary tab must be completed for each system, and will determine if the remaining tabs must also be completed. If required, the remaining tabs efficiently collect all relevant data necessary to provide a solid evaluation of the privacy risks, controls, and requirements of the analyzed system, as required by OMB and other applicable legislation.

#### 4.1.1 Purpose of the PIA

Conducting PIAs at the OPDIV level will allow the Department to identify which of its systems contain IIF and which do not. For those systems containing IIF, the PIA will serve as a platform to:

- Ensure that information handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining, and disseminating IIF in an electronic information system; and
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.<sup>3</sup>

---

<sup>3</sup> Taken from the definition of "PIA" in OMB M-03-22, "OMB Guidance for Implementing of the Privacy Provisions of the E-Government Act of 2002," September 26, 2003.

### 4.1.2 Benefits of PIA

Once the PIA is complete, knowledgeable Departmental officials, whether system managers or OPDIV CIOs, can determine strategies and controls to mitigate the risks and vulnerabilities that were identified. PIAs provide a number of advantages over ad hoc evaluations. These advantages include:

- Producing a PIA capable of meeting the supporting documentation requirements for budget and funding documents (i.e., Exhibit 300 and Exhibit 53);<sup>4</sup>
- Providing inputs for required reporting documents (e.g., Plan of Action and Milestones [POA&M]);
- Providing a reliable basis for policy, system design decision making, and system design;
- Generating and improving public confidence by anticipating and addressing privacy concerns;
- Improving the understanding of an agency's potential privacy risks, exposures, and liabilities; and
- Providing a PIA for the certification and accreditation (C&A) package.

### 4.1.3 Scope

The Department should use the PIA to examine all procedures that involve the usage, storage, retrievability, accessibility, retention, and disposal of IIF. The assessment requires that the system owners and developers answer privacy-related questions about:

- System characterization and data configuration;
- Information sharing practices;
- Website hosting practices;
- Administrative and technical controls; and
- Physical access.

### 4.1.4 Timing

The PIA process guides OPDIV PIA authors in assessing information systems through all phases of the system development life cycle (SDLC). PIAs should be performed in the initiation phase of a system. An initial PIA can be performed on an existing operational system. Departmental policy requires that PIAs be conducted and maintained on all systems, whether already in existence, in development, or undergoing modification.

---

<sup>4</sup> Two of the Exhibits required by A-11 affect IT. Exhibit 53 is the Agency IT Investment Portfolio, which provides budget estimates for overall IT investments and for major and significant IT systems. Exhibit 300 is a Capital Asset Plan completed for major IT systems and IT budget initiatives.

## 4.2 PIA Activities

This section provides the overarching steps in the PIA activities from assigning responsibilities for completing PIAs to submitting a completed PIA.

### 4.2.1 Step One: Determine When a PIA Must Be Conducted

Departmental policy requires the Department to complete an initial PIA on all HHS or contractor-owned systems. Please note, references to initial PIAs refer to the first complete PIA for a system. Systems that have undergone major changes will require an updated PIA to be completed and submitted to OMB. For further details on what constitutes a major change, see Section 2.2.4 of OMB M-03-22.

### 4.2.2 Step Two: Assign Roles and Responsibilities

The OPDIV SOP must designate the necessary staff to complete PIAs for each system. For example, they may choose various individuals to fulfill the role of the PIA author (e.g., system owner, business owner, or privacy contact). It is strongly encouraged that the designee possesses the knowledge and ability to understand all the issues raised by the PIA, and have sufficient understanding of the Department's IT management structure. The OPDIV SOP has the responsibility for approving and promoting the PIAs to the Department, or assigning those responsibilities via the current PIA tool.

Information in Exhibit 300, Exhibit 53, and PIAs must be consistent. Therefore, it is critical that staff familiar with Exhibit 300, Exhibit 53, and the *E-Government Act* collaborate. Such staff may include privacy experts, IT specialists, system owners, and capital planning staff. If discrepancies are discovered among these documents, the Department would need to be prepared to explain the inconsistencies to OMB. Special attention should be paid to ensure consistent characterizations of the system, including name and identification numbers and descriptions of the collection, use, and sharing of information, to enable appropriate linking of system documentation at the Department level and to OMB. For example, OMB may not be able to provide an IT system with credit for conducting a PIA in Exhibit 300 privacy and security scoring, which could potentially impact the system's funding, if it cannot link the PIA to the Exhibit 300 through the system's unique project identifier (UPI).<sup>5</sup>

### 4.2.3 Step Three: Prepare to Begin the PIA

PIA authors must use the PIA Form located in the current tool. Completed PIAs should be submitted to the OPDIV SOP via the current PIA tool, and maintained as records by the OPDIV. The PIA author's responsibility for conducting the PIA should also include familiarizing themselves with the PIA Form prior to attempting to

---

<sup>5</sup> For discussion of the UPI, see Appendix E.

complete PIAs. Individuals requiring more specific information on the PIA Form should consult Appendix E, *PIA Question-by-Question Tutorial*.

The PIA Form contains several questions that will be answered “Yes” or “No.” Often, however, clarification or system details will be required. When clarification is necessary, the PIA will prompt users for further elaboration.

As users prepare to fill out the PIA, they will gather documentation already created for the system, particularly previous PIAs, and security documentation, such as risk assessments or C&A packages. These documents contain information about the system that will make completing the PIA documents more efficient.

**TIP:** While much of the information included in a PIA may be included in a SORN, the SORN may not substitute for the PIA. The PIA is distinct in terms of what information it requires, in what format the information should be presented, and when the PIA must be updated. Even though a PIA is distinct in many ways, when a SORN needs to be updated, the PIA must also be updated accordingly to ensure the consistency of information reported to OMB.

#### **4.2.4 Step Four: Compose a PIA**

Once the PIA author has been identified and system documentation has been gathered, the PIA is ready to be completed. OPDIVs are required to submit all PIAs to the Department via the current PIA tool. The PIA is not accepted by the Department in other formats. OPDIVs may request access to the current PIA tool by contacting SecureOne HHS at [SecureOne.HHS@hhs.gov](mailto:SecureOne.HHS@hhs.gov).

The PIA Summary tab gathers preliminary information about the system. The responses to the PIA questions automatically populate into the remaining sections of the PIA, so that if OPDIVs are required to complete the remaining tabs of the PIA Form, duplication of information is minimized. In the Question-by-Question tutorial(Appendix E), the questions with asterisks are those that are in the PIA Summary tab. These questions auto-populate the remaining sections of the PIA Form.

**TIP:** OMB M-03-22 requires the PIA to be published, if possible.<sup>6</sup> To meet this requirement, the Department posts a summary of each system PIA. The PIA Summary tab should, therefore, include only nonsensitive information that can be released to the public. Descriptions of unpatched system vulnerabilities, for example, should not be included. If any such information is discovered while completing the remainder of the PIA, it should not be described in detail in the PIA Summary tab.

---

<sup>6</sup> OMB M-03-22 states that “[a]gencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information...contained in an assessment.” See OMB M-03-22, Attachment A, Section II.C.3, “Review and Publication.”

NOTE: If OPDIVs answer “No” to Question 17 (the system does not contain IIF), only the remaining Summary tab questions need to be completed and submitted. **If the system contains IIF, questions in the remainder of the PIA MUST be completed and submitted.**

#### 4.2.5 Step Five: Characterize the System

The PIA includes a section characterizing the identity, components, and functions of the system under consideration. System characterization may entail reviewing system documents and conducting interviews to obtain the information. Especially critical details including:

- **The System Name and UPI Number of the system.** This information must be consistent with reports made for Exhibit 300.
- **Life-cycle status of the system.** If the Department is at all uncertain of the correct designation of the system’s life cycle, staff should consult NIST Special Publication (SP) 800-64, *Security Considerations in the System Development Life Cycle*.
- **Description of the kind of information collected or maintained.** A description of the category of individuals to whom the information pertains; “Information about people”, for example, is not sufficiently descriptive.

Data collected from existing documentation should be reviewed and analyzed to determine the system boundaries, functionality, and security requirements. Reviewed documentation should include any *Privacy Act* SORN published in the Federal Register. A PIA cannot be performed until the system boundaries are identified and the security requirements are established.

#### 4.2.6 Step Six: Complete the PIA

The PIA should be submitted via the current PIA tool. Before submitting, ensure that:

- Printouts of the PIA have been reviewed and signed by the OPDIV SOP.
- Hard copies of the signed PIA are retained by each OPDIV, in the event of an IG, OMB, or Government Accountability Office (GAO) inquiry.

Promoting the PIA to the Department requires 100% completion of data fields, and will indicate that the appropriate review of the privacy documentation has taken place at the OPDIV level. There are two scenarios where a PIA can be considered 100% complete. If there is no IIF and question 17 is answered with “No”, then once the Summary tab is filled out, the PIA is considered complete and can be promoted. If question 17 is answered with a “Yes”, then all remaining PIA tabs must be completed for the PIA to be considered 100% complete. HHS policy requires OPDIVs to submit PIAs to the HHS Office of Chief Information Officer (OCIO). The OCIO will

perform a review of each system PIA to ensure it is complete, and will generate a system PIA Summary. Each system PIA Summary will be reviewed to ensure no sensitive information has been provided. As an OMB requirement, the Department will then submit the PIA Summaries to OMB annually, and make the PIA Summaries publicly available at <http://www.hhs.gov/pia>.

#### **4.2.7 Step Seven: Approve or Demote the PIA**

To complete the PIA, it must be promoted to the Department via the current PIA tool. This confirms that the review and signature process has been completed and that signed hard copies of PIAs are maintained by the OPDIV. If the PIA contains sensitive information, the reviewer should demote the PIA for revision back to the PIA author.

#### **4.2.8 Step Eight: Maintain the PIA**

In addition to maintaining the hard copy of the PIA, OPDIVs will periodically need to review PIAs to ensure they comply with current system practices. Each OPDIV is responsible for determining when these reviews take place. A PIA is a living document that must be updated when a major change in the system occurs. Section 2.2.4 lists several examples (found in OMB M-03-22) of system changes that may require completing a new PIA. Periodic reviews of the PIA will ensure that these triggers—or any other changes in a systems management, operational, or technical environment that may impact IIF—will be captured as required by law and Department policy.

**TIP:** Once a system expires or is retired and no longer in operation, the system's PIA may also be retired. For more information on how to retire a system PIA, please contact SecureOne HHS at [SecureOne.HHS@hhs.gov](mailto:SecureOne.HHS@hhs.gov).

## 5. Conclusion

---

The Department must perform thorough PIAs to satisfy the requirements of the *E-Government Act*, as set forth in Departmental policy. A well thought out PIA also presents the Department with the opportunity to determine whether it is complying with the requirements of the *Privacy Act*, COPPA, and other federal legislation, regulations, and OMB memoranda. Furthermore, because the PIA summaries are made publicly available, the Department is presented with an opportunity to assure the public that it is providing government services, in a manner that considers the sensitivity of the personal information it receives.

## Appendix A: Document Feedback

This form is for reviewer-suggested corrections, revisions, or updates and is intended to improve the usefulness of the document for possible inclusion in future versions. Please forward recommended changes and comments to the Department of Health and Human Services (HHS), Office of the Chief Information Officer (OCIO).

By E-mail: [SecureOne.HHS@hhs.gov](mailto:SecureOne.HHS@hhs.gov)

Subject Line: Guidance Feedback

By Phone: (202) 205-9581

<b>Document Title:</b>	
>	
<b>Section Number:</b>	
>	
<b>Category of Comment:</b>	
<b>A</b>	Administrative. Administrative comments correct what appear to be inconsistencies between sections, typographical errors, or grammatical errors.
<b>S</b>	Substantive. Substantive comments are provided because sections in the publication appear to be or are potentially incorrect, incomplete, misleading, or confusing.
<b>C</b>	Critical. Critical comments will cause non-concurrence with the publication if concerns are not satisfactorily resolved.
<b>M</b>	Major. Major comments are significant concerns that may result in a non-concurrence of the entire document if not satisfactorily resolved. This category may be used with a general statement of concern with a subject area, thrust of the document, etc., followed by detailed comments on specific entries in the publication which, taken together, constitute the concern.
<b>Category</b>	<b>Comment</b>
<b>Name of Submitting Operating Division (OPDIV):</b>	
>	
<b>Your Name and Title:</b>	
>	
<b>Telephone:</b>	
>	
<b>E-mail:</b>	
>	
<b>Note: Use an additional blank sheet if needed.</b>	

## Appendix B: References

---

Federal Trade Commission, *Children's Online Privacy Protection Rule; Final Rule*, published in the Federal Register (FR) 64, 59887-59915, November 3, 1999.

*HHS Information Security Program Policy*, July 2005.

*HHS Machine-Readable Privacy Policy Guide*, July 2005.

Internal Revenue Service (IRS), *Model Information Technology Privacy Impact Assessment*, 1996.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

Office of Management and Budget (OMB) Bulletin No. 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*, July 9, 1990.

OMB Circular A-11, *Preparing, Submitting, and Executing the Budget*, updated annually.

OMB Circular A-123, *Management Accountability and Control*, June 21, 1995.

OMB Circular A-130, *Management of Federal Information Resources*, November 28, 2000.

OMB Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, November 28, 2000.

OMB Memorandum (M), *Application of Subsection M of the Privacy Act*, November 30, 1979.

OMB M-99-18, *Privacy Policies on Federal websites*, June 2, 1999.

OMB M-01-05, *Computer Matching and Privacy Protection Act of 1988*, December 20, 2000.

OMB M-05-08, *Designation of Senior Agency Officials for Privacy*, February 11, 2005.

OMB M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, August 2, 2005.

OMB M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006.

OMB M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 17, 2006.

*OMB Privacy Act Guidelines*, published in the Federal Register (FR) 40, 28934-28978, July 9, 1975.

*OMB Order for the Confidentiality of Statistical Information*, FR 62, 35043-35049, June 27, 1997.

*OMB Revised Supplemental Guidance for Conducting Computer Matching Programs*, FR 47, 21656-21658, May 19, 1982.

*OMB Supplementary Privacy Act Guidance*, FR 40, 56741-56743, December 4, 1975.

Public Law 93-502, *Freedom of Information Act of 1966* [5 U.S.C. 552], November 21, 1974.

Public Law 93-579, *Privacy Act of 1974*, December 31, 1974.

Public Law 97-255, *Federal Manager's Financial Integrity Act of 1982*, September 8, 1982.

Public Law 99-474, *Computer Fraud and Abuse Act of 1986*, October 16, 1986.

Public Law 100-503, *Computer Matching and Privacy Act of 1988*, October 18, 1988.

Public Law 104-13, *The Paperwork Reduction Act of 1995*, May 22, 1995.

Public Law 104-106, Division E, *Information Technology Management Reform Act* (ITMRA, also known as the Clinger-Cohen Act), February 10, 1996.

Public Law 104-191, *Health Insurance Portability and Accountability Act of 1996* (HIPAA), August 21, 1996.

Public Law 106-398, *Defense Authorization Act, Title X, Subtitle G, Government Information Security Reform Act* (GISRA), October 30, 2000.

Public Law 107-347 [H.R. 2458], *E-Government Act of 2002*. Title III of this Act is the *Federal Information Security Management Act of 2002 (FISMA)*, December 17, 2002.

*Uniform Trade Secrets Act* (Drafted by the National Conference of Commissioners on Uniform State Laws), as amended 1985.

US Code, 12 U.S.C. 3401 et seq., *Right to Financial Privacy Act of 1978*.

US Code, 15 U.S.C. § 6501 et seq., *Children's Online Privacy Protection Act of 1998*.

45 Code of Federal Regulations (CFR) pt. 164, *DHS Freedom of Information Act Regulations*.

45 CFR Subpart 5B, *DHS Privacy Act Regulations*.

## Appendix C: Acronyms

<b>C&amp;A</b>	Certification and Accreditation
<b>CFR</b>	Code of Federal Regulations
<b>CIO</b>	Chief Information Officer
<b>CISO</b>	Chief Information Security Officer
<b>COPPA</b>	Children's Online Privacy Protection Act of 1998
<b>CPIC</b>	Capital Planning and Investment Control
<b>DHS</b>	Department of Homeland Security
<b>EO</b>	Executive Order
<b>FISMA</b>	Federal Information Security Management Act of 2002
<b>FOIA</b>	Freedom of Information Act of 1966
<b>FR</b>	Federal Register
<b>FTC</b>	Federal Trade Commission
<b>FY</b>	Fiscal Year
<b>GAO</b>	Government Accountability Office
<b>GISRA</b>	Government Information Security Reform Act of 2000
<b>GSS</b>	General Support System
<b>HHS</b>	Health and Human Services, U.S. Department of
<b>HIPAA</b>	Health Insurance Portability and Accountability Act of 1996
<b>IIF</b>	Information in Identifiable Form
<b>IG</b>	Inspector General
<b>IPSO</b>	Information Processing Service Organization
<b>IPv6</b>	Internet Protocol Version 6
<b>IRS</b>	Internal Revenue Service
<b>ISSO</b>	Information Systems Security Officer
<b>IT</b>	Information Technology
<b>ITMRA</b>	Information Technology Management Reform Act
<b>LAN</b>	Local Area Network
<b>M</b>	Memorandum
<b>MA</b>	Major Application
<b>NIST</b>	National Institute of Standards and Technology
<b>OCIO</b>	Office of the Chief Information Officer
<b>OCR</b>	Office for Civil Rights
<b>OMB</b>	Office of Management and Budget
<b>OPDIV</b>	Operating Division
<b>P3P</b>	Platform for Privacy Preferences
<b>PDF</b>	Portable Data Format
<b>PII</b>	Personally Identifiable Information
<b>PHI</b>	Protected Health Information
<b>PIA</b>	Privacy Impact Assessment
<b>POA&amp;M</b>	Plan of Action and Milestones
<b>POC</b>	Point of Contact
<b>PRA</b>	Paperwork Reduction Act
<b>SAOP</b>	Senior Agency Official for Privacy

<b>SDLC</b>	System Development Life Cycle
<b>SOP</b>	Senior Official for Privacy
<b>SOR</b>	System of Records
<b>SORN</b>	System of Records Number
<b>SP</b>	Special Publication
<b>STAFFDIV</b>	Staff Division
<b>UPI</b>	Unique Project Identifier
<b>URL</b>	Uniform Resource Locator
<b>U.S.C.</b>	United States Code
<b>VPN</b>	Virtual Private Network
<b>W3C</b>	World Wide Web Consortium

## Appendix D: Glossary

---

**Administrative Controls**—safeguards to ensure proper management and control of information and information systems. These safeguards include policy, Privacy Impact Assessments (PIA), and certification and accreditation programs. (See National Institute of Standards and Technology [NIST] Special Publication [SP] 800-12.)

**Availability**—a requirement intended to ensure that systems work properly, and service is not denied to authorized users. (See NIST SP 800-12.)

**Confidentiality**—a requirement that private or confidential information not be disclosed to unauthorized individuals. (See NIST SP 800-12, p. 8.)

**Cookie**—information that a website puts on an individual's computer so that it can remember something about the user at a later time. See also: persistent cookie, session cookie.

**General Support System (GSS)**—an interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN), including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center and its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). (Defined in Office of Management and Budget [OMB] Circular A-130, (A)(2)(c).)

**Information in Identifiable Form (IIF)**—any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. (Defined in the *E-Government Act of 2002*, Pub.L.107-347, Title II and III.)

**Integrity**—the degree to which information is timely, accurate, complete, and consistent. Data integrity refers to the quality that is preserved when information and programs are changed only in a specified and authorized manner. System integrity refers to the quality that is demonstrated when a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (See NIST SP 800-12.)

**Major Application (MA)**—an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. MAs can be either a major software application or a combination of hardware and software in which the

only purpose of the system is to support a specific mission-related function. (Defined in NIST SP 800-18.) Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as a “Major Application.” Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in OMB Circular A-130, (A)(2)(d).)

**Major Change (concerning certification and accreditations, related to question 41 of the PIA)**—any change that is made to the system environment or operation of the system. The following are examples of major changes as defined by M-03-22:

- Network, hardware, or software applications that alter the mission, operating environment, or basic vulnerabilities of the system;
- Increase or decrease in hardware, application programs, external users, or hardware upgrades;
- Addition of telecommunications capability;
- Change to program logic of application systems; and
- Relocation of system to new physical environment or new organization.

**Non-Major Application**—any initiative or investment not meeting the definition of a major application defined above but is part of the agency's IT Portfolio. (Defined in OMB Circular A-11, Section 53.4)

**Persistent Cookie**—a cookie that is stored on the user's hard drive and remains there until the user deletes it or it expires.

**Physical Security Controls**—measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. These safeguards might include protections against fire, structural collapse, plumbing leaks, physical access controls, and controls against the intercept of data. (See NIST SP 800-12.)

**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.

**Record**—any item, collection, or grouping of information about individuals that is maintained by an agency, including, but not limited to, their education, financial

transactions, and/or medical, criminal, or employment history and that contains their name; or it contains the identifying number, symbol, or other identifying information assigned to the individual, such as a finger or voice print or a photograph. (See 5 U.S.C. §552a(a)(4)).

**Routine Use**—regarding the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected.

**Session Cookie**—a small file, stored in temporary memory, containing information about a user that disappears when the user's browser is closed. Unlike a persistent cookie, no file is stored on the user's hard drive.

**System**—an organized assembly of IT resources and procedures integrated and regulated by interaction or interdependence to accomplish a set of specified functions.

**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.

**Technical Controls**—safeguards that are generally executed by the computer system. Technical safeguards include password protection, firewalls, and cryptography. (See NIST SP 800-12.)

**Unique Project Identifier (UPI)**—an identifier that depicts agency code, bureau code, mission area (where appropriate), part of the exhibit where investment will be reported, type of investment, agency four-digit identifier, year the investment entered the budget, and mapping to the Federal Enterprise Architecture. For details and explanation, see OMB Circular A-11, Section 53.8.

**Website**—a collection of interlinked web pages (on either Internet or intranet sites) with a related topic, usually under a single domain name, which includes an intended starting file called a "home page." From the home page, access is gained to all the other pages on the website.

## Appendix E: PIA Question-by-Question Tutorial

---

The PIA questions provided within this document are intended to be brief. The PIA author filling out the PIA Form may wish to consult this step-by-step tutorial when completing the PIA for explanations of terms and assistance in identifying relevant resources.

The PIA Summary tab includes 20 questions, some of which are open-ended. The PIA Summary will be made publicly available via <http://www.hhs.gov/pia>. Information in the PIA Summary tab should not contain information unsuitable for public release.

Here are some suggested guidelines to follow when preparing a PIA:

- Open-ended questions should be written concisely and in a way that is easily understood by the general public.
- Spell out each acronym the first time it is used, the acronym should be used in all subsequent references.
- Technical terms and references should be defined.
- References to governmental publications and other documents should include the complete name of the reference the first time it is used (e.g. Office of Management and Budget (OMB) Memorandum (M)-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002).

Sufficient information must be provided in the PIA Summary tab to identify the system and to ensure that reconciliation with other records and documentation of the system is possible. The accuracy of this information is critical to the correct processing and documentation of the PIA. If the PIA author completing the PIA is at all uncertain whether the system identification information is correct, he or she should consult the Operating Division (OPDIV) Senior Official for Privacy, OPDIV Privacy Contact (POC), or Capital Planning and Investment (CPIC) Contact.

In this Question-by-Question tutorial, the questions with an asterisk are a part of the PIA Summary tab.

### **PIA Required Information Tab**

**\*Background Question: Is this a new PIA? If this is an existing PIA, please provide a reason for the revision.** PIAs must be submitted for a new system. If a system has undergone a major change, then PIAs must be revised.

**\*Question 1: Date of this Submission.** Please input the projected date when the PIA will be submitted to the Department from the OPDIV Senior Official for Privacy.

**\*Question 2: OPDIV Name.** Please indicate the OPDIV where this system resides or which OPDIV manages the system.

**\*Question 3: Unique Project Identifier (UPI) Number.** The format of the UPI is established in OMB Circular A-11, Section 53.8. The number reflects information such as the OPDIV and office where the investment project was initiated, the type of investment, and other information. This number is attached to Exhibit 300s and Exhibit 53s, which are submitted to OMB prior to major investments and budget requests. If the system has a UPI, this number **must** be included in the PIA or OMB may not accurately reflect the submission of the PIA documents. A system would not require a UPI number if, for example, no Exhibit 300 exists or the system is not classified as a "Major Investment." The Department should be especially careful to ensure that the correct UPI has been included.

**\*Question 4: System of Records Notice (SORN) Number.** OMB assigns this number to the system after an OPDIV submits an SORN request to OMB pursuant to the *Privacy Act of 1974*. The HHS Privacy Act Officer or OPDIV Privacy Contact should be able to supply this number if the PIA author does not know whether the system has already completed a SORN. If no SORN number exists for the system, please explain the reason in this space (e.g., the system is in development and not yet submitted or the system does not constitute a "System of Records" under the *Privacy Act*).

**\*Question 5: OMB Information Collection Approval Number. OMB Information Collection Approval Number Expiration Date.** This number should be identical to the one OMB assigned pursuant to a Paperwork Reduction Act filing and is sometimes referred to as an OMB control number. The number reflects OMB's approval for collecting information. An agency may not conduct nor sponsor a collection of information unless it displays a valid OMB control number. Likewise, individuals are not required to respond unless such a number is displayed. If the Department is unsure of this number, it may wish to consult the HHS Report Clearance Officer, or the OPDIV Report Clearance Officer

**\*Question 6: Other Identifying Number(s).** If the Department uses any system identification methodology that is specific to the Department, such as a purchase order number or an internal inventory number, please supply that number here. Please **do not** use this number instead of the unique identifier, SORN number, or OMB information collection approval number, as this will confuse record keeping and PIA approval efforts.

**\*Question 7: System Name.** If the system is included in the Department's Federal Information Security Management Act (FISMA) submission, the name of the system should be the same as the one reported to OMB.

**Question 8: System Location: (OPDIV or contractor office building, room, city, and state).** Fill in as appropriate. The system location referred to in this

question is the physical location of the system. If a system has multiple locations, indicate at least one physical location for the system.

**\*Question 9: System POC. The System POC is the person to whom questions about the system and the responses to this PIA may be addressed.** Provide the name and/or title of an individual to whom questions about the system and the information provided in the PIA may be addressed. The system owner or administrator is acceptable for this purpose.

**\*Question 10: Provide an overview of the system.** While the PIA's primary purpose is to convey the impact of privacy on the system in question, this question provides system owners with an excellent opportunity to explain the importance of the system and of the work the system users perform.

### **System Characterization and Data Categorization Tab**

Once the system is precisely identified, the System Characterization and Data Categorization (questions 11-21) of the PIA can be answered. These questions are intended to describe the use, function, information contained, and other aspects of the system. Completing this tab may require coordination with the system owner, system users, or others with knowledge of the operational aspects of the system under consideration.

**Question 11: Does HHS own the system? If no, identify the system owner.** The Department "owns" a system if it funds the design, development, or implementation of the system. In situations where the PIA is being completed pursuant to a system that is in the process of being procured or developed, the Department should still respond "Yes" to this question. See OMB M-03-22, section B1.

**Question 12: Does HHS operate the system? If no, identify the system operator.** The Department "operates" a system if it uses it to perform a Department function and/or maintains and upgrades the infrastructure of the system. See OMB M-03-22, section B1. As an example, if an OPDIV or contractor operates the system and/or manages the system on behalf of the Department, then HHS operates the system.

**\*Question 13: Indicate if the system is a new or an existing one being modified.** Select "New" if the system is in development or "Existing" if the system is currently in operation or has undergone a major change as described in OMB M-03-22.

**Question 14: Identify the life-cycle phase of this system.** The Department may wish to fill in more than one box if no single response adequately describes the life-cycle phase of the system. If the agency is uncertain what stage the system is in, the OPDIV should consult NIST SP 800-64, *Security Considerations in the System Development Life Cycle*.

**Question 15: Have any of the following major changes occurred to the system since the PIA was last submitted?** Major changes include the nine triggering events listed in OMB M-03-22 and in Section 2.2.4 of this document. Please answer "Yes" or "No" to the listed major changes.

**Question 16: Is the system a General Support System (GSS) or a Major Application (MA)?** If the Department is unsure whether the system meets this definition, refer to OMB A-130, Appendix III. Definitions for "General Support System" and "Major Application" are also provided in Appendix D of this document.

**\*Question 17: Does/Will the system collect, maintain (store), disseminate, and/or pass through IIF within any database(s), record(s), file(s), or website(s) hosted by this system?**

**Note: This question seeks to identify all personal information associated with the system. This includes IIF that is subject to the *Privacy Act*; whether the individuals are employees, the public, research subjects, or business partners; and whether the IIF is provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the *Privacy Act* or other legislation.**

**Note: If no IIF is contained in the system, please answer questions 21, 23, 30, 31, 32, 37, 50 and 54, then promote the PIA to the OPDIV Senior Official for Privacy who will authorize the PIA.**

**If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.**

For question 17, if it is answered "Yes," please fill out all questions on the remaining tabs of the PIA. If answered "No," please complete the Summary tab only, and have the PIA approved by the OPDIV PIA Reviewer, OPDIV Senior Official for Privacy, and HHS Senior Agency Official for Privacy.

**Please select "Yes" for all applicable IIF categories. If the applicable IIF category is not listed, please use the Other field to identify the appropriate category of IIF.** Please see the PIA Summary tab for instructions. If the response was "Yes" in the Summary tab, please identify the category of IIF.

**Question 18: Please indicate the categories of individuals about whom IIF is collected, maintained, disseminated, and/or passed through. Note: If the applicable IIF category is not listed, please use the Other field to identify the appropriate category of IIF. Please answer Yes or No to all of these choices.** Responses must be sufficiently specific to describe only those individuals whose information is collected. Individuals may, for example, be limited to recipients of specific benefits or services, individuals requesting further information

concerning a particular government function or service, or individuals subject to particular laws or regulations.

**Question 19: Are records on the system retrieved by one or more data elements? If yes, please select all applicable IIF categories. If the applicable IIF category is not listed, please use the Other field to identify the appropriate category of IIF.** If the Department ever retrieves records using IIF data elements, it shall answer "Yes" to question 19. The Department should answer "Yes" to this question if the system is in the procurement or development stage and does not yet contain IIF, but is intended or expected to be populated with IIF. OMB Guidelines for the *Privacy Act* clarify what it means to "retrieve" a record by stating that a system of records exists if the capability exists for "indexing or retrieval capability using identifying particulars [that is] built into the system"; and the Department "does, in fact, retrieve records about individuals by reference to some personal identifier." OMB Guidelines, 40 Fed. Reg. 28,948, 28,952 (1975).

**Question 20: Are 10 or more records containing IIF maintained, stored, or transmitted/passed through this system?** A "record" is any item, collection, or grouping of information about an individual that is maintained by an agency. This information includes education, financial transactions, medical history, and criminal or employment history and that contains the name, identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint, or a photograph. (See 5 U.S.C. §552a(a)(4) [the *Privacy Act*]). In general, United States federal courts have construed what constitutes a "record" fairly broadly. An item, collection, or grouping of information containing even a single item of information about an individual has been held to constitute a "record." If the Department is at all uncertain whether the contents of the system constitute "records" under the *Privacy Act*, it should consult its Privacy Contact.

**\*Question 21: Is the system subject to the *Privacy Act*?** As noted in the questionnaire, the system is likely to be subject to the *Privacy Act* if the answers to questions 17, 19, and 20 are each "Yes." System owners should contact their OPDIV Privacy Contact for assistance with this question if they are uncertain about the applicability of the *Privacy Act*.

**Question 21 A. If yes, but a SORN has not been created, please provide an explanation.** If the system is subject to the *Privacy Act*, the system should also have a SORN to comply with the *Privacy Act*, OMB Guidance, and the Secure One HHS Information Security Program Policy. If the system does not have a SORN, and is subject to the *Privacy Act*, please provide an explanation.

### **Information Sharing Practices Tab**

Questions 22 through 31 concern the way in which information is used, transferred, stored, and processed. These questions are especially critical in determining whether the use and operation of the system is consistent with federal law and regulations.

**Question 22: Does the system share or disclose IIF with other divisions within this agency, external agencies, or other people or organizations outside the agency? If yes, please identify the category of IIF shared or disclosed. If the category of personal information is not listed, please check Other and identify the category.** This question seeks to find how the system shares information.

**\*Question 23: If the system shares or discloses IIF please specify with whom and for what purpose(s).** The Department should provide an affirmative explanation regardless of whether disclosure is on paper, electronic, or oral. If no IIF is shared or disclosed, indicate "N/A" in the text field.

**Question 24: If the IIF in the system is or will be matched against IIF in one or more other computer systems, are computer data-matching agreement(s) in place?** No record contained within a system of records can be disclosed to an agency or non-federal agency for use in a computer-matching program except pursuant to a written agreement between the source agency and the recipient agency. If no matching takes place, the appropriate response is "No." For more information on the requirements of a computer data matching agreement, see OMB M-01-05.

**Question 25: Is there a process in place to notify organizations or systems that depend on the IIF contained in this system when major changes occur (e.g., revisions to IIF or when the system is replaced)?** Change management, incident response, and continuity of operations procedures should all include communications plans or procedures that explicitly address how to inform users, organizations, and other stakeholders of changes to this system that affect their activities or operations. If the process for notifying data users is unwritten, the Department should answer "No" to this question.

**Question 26: Are individuals notified how their IIF is going to be used? If yes, please describe the process for allowing individuals to have a choice.** Notification procedures should be explicitly documented. If the process for notifying individuals is unwritten, users should answer "No" to this question.

**Question 27: Is there a complaint process in place for individuals who believe that their IIF has been inappropriately obtained, used, or disclosed, or that the IIF is inaccurate? If yes, please describe briefly the notification process.** The availability of the complaint process should be documented and the Department should be able to demonstrate that it makes reasonable efforts to inform individuals of the correct procedures to follow in registering a complaint.

**Question 28: Are there processes in place for periodic reviews of IIF contained in the system to ensure the data's integrity, availability, accuracy, and relevance? If yes, please describe briefly the review process.** If such processes are in place, the Department may also have processes for retaining and

destroying files, documents, or other records deemed corrupted, outdated, inaccurate, or irrelevant. The Department should consider these practices in answering question 50, which concerns data retention and destruction practices.

**Question 29: Are there rules of conduct in place for access to IIF on the system? If yes, identify all users with access to IIF on the system and briefly state the purpose for each user to have access.** If the Department has informal or unwritten rules only, the agency should answer "No" to this question. Agencies with "Acceptable Use Policies" that apply to the system covered by the PIA as well as other systems may respond "Yes" to this question. "Acceptable Use Policies" must, however, be comprehensively written. Agencies must also make all users aware of "Acceptable Use Policies" through awareness and/or training activities.

**\*Question 30: Please describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information. In this description, indicate whether the information contains IIF and whether submitting personal information is voluntary or mandatory.**

This question seeks a narrative response similar to information found in a SORN publication.

**\*Question 31: Please describe in detail any processes in place to:**

- **Notify and obtain consent from the individuals whose IIF is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection)**
- **Notify and obtain consent from individuals on what IIF is being collected from them and how the information will be used or shared.**

**Note: Please describe in what format individuals will be given notice of consent (e.g., written notice, electronic notice).**

Notification procedures should be explicitly documented. If the process for notifying individuals is unwritten or the system does not contain IIF, the PIA author should answer "No" to this question.

### **Website Hosting Practices Tab**

Questions 32 through 40 concern systems that host websites. If a system hosts a website, agencies may need to comply with several requirements involving notice and information collection practices. If the system does not host a website, the majority of these questions can be answered "no."

**\*Question 32: Does the system host a website? If yes, please indicate what type of site the system hosts.** This question applies only to the system under consideration. If the system under consideration does not host a website, the

Department should answer “No” to this question. If yes, the Department should indicate whether the website is hosted on an intranet (available to system users only), Internet (publicly available), or both. If the site is only available to users via a Virtual Private Network (VPN), intranet, or other access-limitation scheme, the Department should still answer “Yes” to this question, even though many of the requirements that apply to publicly accessible websites do not apply to these internal-use-only websites.

**Question 33: Is the website accessible by the public or other entities (e.g., federal, state, and local agencies, contractors, third-party administrators)?**

This question seeks to find if the website is accessible by any other parties other than HHS.

**Question 34: Is a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) posted on the website?**

OMB M-99-18 requires all federal agencies to ensure websites that collect “substantial information from the public” include a privacy policy. The policy must “clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it. Privacy policies must be clearly labeled and easily accessed when someone visits a website.” OMB M-03-22 adds requirements for consent to collecting and sharing IIF and explains the rights under the *Privacy Act* and other laws. If the Department is uncertain of whether its privacy policies comply with these requirements, see OMB M-99-28 and Section III of OMB M-03-22.

**Question 35: Is the website’s privacy policy in a machine-readable format, such as that provided by Platform for Privacy Preferences (P3P)? If no, please indicate when the website will be P3P compliant.**

P3P is a tool for reporting a website’s privacy practices to users that access those websites. P3P-enabled websites make this information available in a standard, machine-readable format. P3P-enabled browsers can “read” this snapshot automatically and compare it to the viewer’s own set of P3P privacy preferences. More information on P3P and ways to implement it is available at the website of the World Wide Web Consortium (W3C), the developer of P3P: <http://www.w3.org/P3P/>. For specific assistance at HHS, please see the *HHS Machine-Readable Privacy Policy Guide*.

**Question 36: Does the website use persistent tracking technologies?**

Persistent tracking technologies are small amounts of information that a website puts on an individual’s computer so that it can remember something about the user at a later time. Examples include persistent cookies, Web bugs, and Web beacons. This differs from tracking technologies such as session cookies, which are removed from a user’s computer once that session ends. If the Department’s website sends any form of persistent tracking technology to a user’s computer, the Department should answer “Yes” to this question. Using persistent tracking technologies is forbidden unless there is a compelling need for their use and an agency head (or sub-agency head specifically authorized by an agency head) approves of their use. For more

information on persistent tracking technologies, see Section III (D)(2)(v) of OMB M-03-22.

**\*Question 37: Does the website have any information or pages directed at children under the age of thirteen? If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?** If the Web page has any material that is intended for school-age children, especially children under the age of 13, the Department should answer “Yes” to this question. The answer to this question determines whether the website must comply with COPPA. The Federal Trade Commission (FTC), which is charged with enforcing COPPA, states that in determining whether a website or online service is targeted at children, the FTC will consider the website’s “subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertisements promoting or appearing on the website or online service is directed at children.” The FTC will also consider “evidence regarding audience composition; evidence regarding the intended audience, and whether a site uses animated characters and/or child-oriented activities and incentives.”<sup>7</sup>

**Question 38: Does the website collect IIF from individuals? If yes, please indicate the category of IIF.** If users of the website fill out forms that result in collecting the IIF items listed through the website, the Department should answer “Yes” to this question. If the website merely provides portable data formats (PDF) of standard forms for printout or publishes addresses where information may be mailed, it is not necessary to answer “Yes” to this question. If the website is under development, but is intended or expected to collect IIF from individuals, the Department should answer “Yes” to this question. If the response is “Yes,” please also answer “Yes” for the categories of IIF that is collected from individuals.

**Question 39: Are rules of conduct in place for access to IIF on the website?** The Department may answer “Yes” to this question only if rules of conduct are written, apply to all users who have access to IIF on the website, and are distributed to all users of IIF on the website.

**Question 40: Does the website contain links to sites external to the OPDIV that owns and/or operates the system? If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by the OPDIV.** “Link” refers to a “hyperlink”—a text, graphic, or other feature on a website—that, when the user clicks on it with a mouse or cursor, automatically directs the viewer to another Web page or site. If the site contains links that take the user to a website that is not owned and/or operated by the Department, a link must be provided to a disclaimer stating that the information the user is about to view is not under the control of the Department.

### **Administrative Controls Tab**

---

<sup>7</sup> See 16 CFR Part 312, *Children’s Online Privacy Protection Rule*.

Administrative controls are safeguards to ensure proper management and control of information and information systems. These safeguards include policies, the PIA itself, and certification and accreditation (C&A) programs. Questions 41 through 50 are relevant to the administrative controls in place to protect the IIF in the system in question.

**Question 41: Has the system been certified and accredited (C&A)? If the system requires a C&A and one has not been completed, please indicate when the C&A is scheduled for completion.**

For more information on process authorization, see National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

**Question 42: Is there a system security plan for this system?** Developing a system security plan is part of the C&A process for federal information systems. For more information on developing a system security plan, see NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

**Question 43: Is there a contingency (or back up) plan for the system?** For more information on contingency plans for federal systems, see NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*.

**Question 44: Are files backed up regularly?** For more information on back-up strategies, see NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*.

**Question 45: Are the back-up files stored off-site?** For more information on back-up strategies, see NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*.

**Question 46: Are there user manuals for the system?** This question concerns specific instructions for using the system to carry out its intended function, rather than general privacy, security, or acceptable use policies.

**Question 47: Have personnel (system owners, managers, operators, contractors, and/or program managers) using the system been trained and made aware of their responsibilities for protecting personal information that is being collected and maintained?** For more information on developing a security awareness and training program for users of federal information systems, see NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*.

**Question 48: If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?** Answering this question may require coordination with the contract office. The CIO's

office should be able to provide the correct information or POC to gather the information.

**Question 49: Are methods in place to ensure least privilege (i.e., “need to know” and accountability)? If yes, please specify method(s).** “Least privilege” refers to the security objective of granting users only those accesses they need to perform their official duties. For more on the concept of least privilege, see NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, pages 109-110.

**\*Question 50: Are there policies or guidelines in place concerning the retention and destruction of IIF? If yes, please provide some detail about these policies/practices.** This question is specifically concerned with OPDIV-level, specific policies and procedures. At the Department level, policy guidelines are established by the *HHS Information Security Program Policy*, Section 4.4 (“Media Control”), July 2005. OPDIV-level policies should be consistent with or stricter than the Departmental policy. For more information on which retention schedule pertains to the collection contact the OPDIV Records Management Office.

### **Technical Controls Tab**

Technical controls are safeguards that the computer system generally executes. Technical safeguards include password protection, firewalls, and cryptography. Questions 51 and 52 focus on the technical controls of the system.

**Question 51: Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system? If yes, check all technical controls that are currently in place.** For more information on technical controls, see NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. For technical controls that are currently in place, please answer “Yes” from the list.

**Question 52: Is a process in place to monitor and respond to privacy and/or security incidents? If yes, please briefly describe the process.** For more information on security incident handling programs, see NIST SP 800-61, *Computer Security Incident Handling Guide*.

### **Physical Access Tab**

Physical controls are measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. These safeguards might include protections against fire, structural collapse, plumbing leaks, physical access controls, and controls against the intercept of data.

**Question 53: Are physical access controls in place? If yes, check all physical controls that are currently on the system.** For more information on physical security, see NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. For all physical controls that are currently on the system, please respond "Yes" on the list below.

**\*Question 54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.** Please provide general information about security practices, rather than detailed information about information security. If no IIF is collected, maintained, or disseminated, please answer "No" to the question.