

## **06.3 HHS PIA Summary for Posting (Form) / OIG Audit Work System (TeamMate) [System]**

### **PIA SUMMARY AND APPROVAL COMBINED**

#### *PIA Summary*

**Is this a new PIA 2011?** No

**If this is an existing PIA, please provide a reason for revision:** PIA Validation

**1. Date of this Submission:** 8/16/2007

**2. OPDIV Name:** OIG

**3. Unique Project Identifier (UPI) Number:** 009-92-01-47-02-0001-00-301-093

**4. Privacy Act System of Records (SOR) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):** None

**5. OMB Information Collection Approval Number:** No

**6. Other Identifying Number(s):** No

**7. System Name (Align with system Item name):** Audit Work System (TeamMate)

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:** Patrick Kelly

**10. Provide an overview of the system:** The Audit Work System is a distributed information system supporting the OIG's audit responsibilities authorized by the Inspector General Act of 1978, 5 U.S.C. App. 3. The system is maintained to increase the efficiency and productivity of the audit process by automating working paper preparation, internal review, report generation, and retention. The system utilizes the commercial software product, TeamMate, to manage and integrate working papers prepared with various standard office automation products.

**13. Indicate if the system is new or an existing one being modified:** Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system? (Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether 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. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?):**  
Yes

**21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):** No

**23. If the system shares or discloses IIF please specify with whom and for what purpose(s):**  
Only authorized staff conducting or reviewing audits use TeamMate. Access to information for individual audits is limited to staff assigned to the audit. Other offices within the OIG, such as the Office of Investigations or the Office of Counsel to the Inspector General, may have a need on a case-by-case basis to review audits conducted using TeamMate. Other law enforcement agencies may be provided the information based on the scope and findings of an audit;

information may also be shared with auditees and other third parties when necessary to obtain information relevant to the audit. Triennially, the OIG's audit process is subject to a quality control review conducted by the Inspector General of another agency.

**30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:** The system is used in conducting audit work of the Department of Health and Human Services programs and in preparing related reports on behalf of the OIG. It is a vertical application that documents the audit process - planning preparation, review, report generation and storage - in an electronic format. The nature and scope of the information is determined by the objectives of the audit. Therefore, the information pertaining to a specific audit may or may not contain personally identifiable information. The conduct of audits and the issuance of audit reports are integral to OIG's mission.

**31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII 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); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) 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, etc.]**) Personally identifiable information is not directly retrievable from the Audit Work System. Such information is generally peripheral to the audit and obtained from the auditee. An audit start notice is provided to the auditee containing the description and objectives of the audit. Sufficient background is included to inform the reader of the audit process. In addition to the audit start notice, auditors send a notification letter to the auditee on all audits and reviews. A notification letter provides a means of formalizing the understanding between the OIG and the auditee concerning the objectives of the audit as well as apprising auditees of the documents and records which it should make available to auditors.

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII):** No

**37. Does the website have any information or pages directed at children under the age of thirteen?:** No

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):** Yes

**54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.:** Access to audit working papers is restricted by physical and computer-based access controls. Access within OIG is strictly limited to authorized staff members. Access to information on specific audits is further restricted based on role-based security features that limit access to assigned auditors, reviewers, and managers. All computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standard 31, and the HHS Information Resources Management Manual, Part 6, "ADP Systems Security."

*PIA Approval*

**PIA Reviewer Approval:**

**PIA Reviewer Name:** Richard Stern

**Sr. Official for Privacy Approval:** Promote

**Sr. Official for Privacy Name:** Christopher Ballister

**Sign-off Date:** 8/17/2006

**Approved for Web Publishing:** Yes

**Date Published:** <<Date approved for Web Publishing>>

---

## **06.3 HHS PIA Summary for Posting (Form) / OIG Corporate Management System (CorpView) [System]**

### **PIA SUMMARY AND APPROVAL COMBINED**

#### *PIA Summary*

**Is this a new PIA 2011?** No

**If this is an existing PIA, please provide a reason for revision:** PIA Validation

**1. Date of this Submission:** 3/23/2009

**2. OPDIV Name:** OIG

**3. Unique Project Identifier (UPI) Number:** 009-92-01-47-02-0001-00-301-093

**4. Privacy Act System of Records (SOR) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):** 09-90-0003; 09-90-0100

**5. OMB Information Collection Approval Number:** No

**6. Other Identifying Number(s):** No

**7. System Name (Align with system Item name):** Corporate Management System (CorpView)

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:** Patrick Kelly

**10. Provide an overview of the system:** The OIG Corporate Management System is a centralized information system supporting the OIG's mission and administrative operations authorized by the Inspector General Act of 1978, 5 U.S.C. App 3. The system is maintained for the purpose of documenting, tracking, and reporting OIG's audit, inspection, and investigative activities. The investigative reporting subsystem is used to document the outcome of OIG reviews of allegations and complaints received concerning HHS programs and operations; aid in prosecutions brought against the subjects of OIG investigations; maintain a record of OIG investigations to other Departmental components for their use in operating and evaluating their programs and in imposition of civil and administrative sanctions; and serve as a repository and source for information necessary to fulfill its statutory reporting requirements. The audit information subsystem is used to maximize staff resources and to provide audit cost summary data; to track staff hours allocated towards audit preparation and active audit projects which will allow for more effective scheduling of unassigned personnel and to categorize indirect time expended for end-of-year reporting; to plan workloads; to schedule travel and to control travel costs on assigned audit projects; to assist in providing time and attendance to the centralized payroll system; and to schedule and track training.

**13. Indicate if the system is new or an existing one being modified:** Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system? (Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether 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. Does/Will the system collect, maintain (store), disseminate and/or pass**

**through PII within any database(s), record(s), file(s) or website(s) hosted by this system?):**  
Yes

**21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):** Yes

**23. If the system shares or discloses IIF please specify with whom and for what purpose(s):**

a. Information from this system may be disclosed to any other federal agency or any foreign, state, or local government agency responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation where that information is relevant to an enforcement proceeding, investigation, or prosecution within the agency's jurisdiction. b. Information from this system may be disclosed to (1) the Department of Justice in connection with requests for legal advice and in connection with actual or potential criminal prosecutions or civil litigation pertaining to the Office of Inspector General, and (2) a Federal or State grand jury, a Federal or State court, administrative tribunal, opposing counsel, or witnesses in the course of civil or criminal proceedings pertaining to the Office of Inspector General. c. Information from this system may be disclosed to a federal, state, or local agency maintaining civil, criminal or other relevant enforcement records or other pertinent records such as current licenses, if necessary to obtain a record relevant to an agency decision concerning the hiring or retention of an employee, the insurance of a license, grant or other benefit. d. Information from this system may be disclosed to a federal agency in response to its request in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the record is relevant and necessary to the requesting agency's decision on the matter. e. Relevant information may be disclosed from this system to the news media and general public where there exists a legitimate public interest, e.g. to provide information on events in the criminal process, such as indictments, and where necessary for protection from imminent threat to life or property. f. Where federal agencies having the power to subpoena other federal agencies' records, such as the Internal Revenue Service, issue a subpoena to the Department for records in this system, the Department will make such records available. g. When the Department contemplates that it will contract with a private firm for the purpose of collating, analyzing, aggregating or otherwise refining records in this system, relevant records will be disclosed to such contractor. The contractor shall be required to maintain Privacy Act safeguards with respect to such records. h. Disclosures may be made to organizations deemed qualified by the Secretary to carry out quality assessments. i. Information from this system may be disclosed in the course of employee discipline of competence determination proceedings. j. Disclosures may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual. k. Information from this system may be disclosed to the Department of Justice, to a judicial or administrative tribunal, opposing counsel, and witnesses, in the course of proceedings involving HHS, an HHS employee (where the matter pertains to the employee's official duties), or the United States, or any agency thereof where the litigation is likely to affect HHS, or HHS is a party or has an interest in the litigation and the use of the information is relevant and necessary to the litigation. l. Information from this system may be disclosed to a Federal, State or local agency maintaining pertinent records, if necessary to obtain a record relevant to a Department decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other

benefit. m. Information from this system may be disclosed to third party contacts, including public and private organizations, in order to obtain information relevant an

**30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:** No. 23 cont. violations in HHS programs and operations, or where disclosure would enable the OIG to identify violations in HHS programs or operations or otherwise assist the OIG in pursuing on-going investigations. n. Records may be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions for the Department but technically not having the status of agency employees, if they need access to the records in order to perform their assigned agency functions.

No. 30. Categories of individuals covered by the system: Individuals relevant to OIG's audit, inspection, and investigative activities, including but not limited to the subjects of an investigation, complainants, and key witnesses where necessary for documentary identification purposes. Categories of records in the System: Criminal investigative files and extracts from that file consisting of a computerized case management and tracking file. The system aggregates the management information required to effectively and efficiently execute the mission of the OIG. This includes supporting audit, inspection, and investigative management activities and day-to-day administrative management needs.

**31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII 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); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) 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, etc.]** The OIG obtains information from a wide variety of sources during the conduct of its activities, including information from the Department and other Federal, State, and local agencies, witnesses, complainants and other nongovernmental sources. Pursuant to subsection (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2), the Secretary has exempted the criminal investigative files of this system from the access, amendment, correction, and notification provisions of the Act, 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(4)(G) and (H). The civil and administrative investigative files are exempted from certain provisions of the Act under 5 U.S.C. 552a(k)(2). Pursuant to 45 CFR 5b.11(b)(2)(ii)(D), the files are exempt from the following subsections of the Act: (c)(3), (d) (1)-(4), and (e)(4) (G) and (H).

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII):**

Yes

**37. Does the website have any information or pages directed at children under the age of thirteen?:** No

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):** Yes

**54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.:** Records are maintained in a restricted area and accessed only by Department personnel. Access within OIG is strictly limited to authorized staff members. All employees are given instructions on the sensitivity of such files and the restrictions on disclosure. Access within HHS is strictly limited to management officials and employees on a need-to-know basis. All computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standards 31, and the HHS Information Resources Management Manual, Part 6, "ADP Systems Security."

***PIA Approval***

**PIA Reviewer Approval:**

**PIA Reviewer Name:** Richard Stern

**Sr. Official for Privacy Approval:** Promote

**Sr. Official for Privacy Name:** Christopher Ballister

**Sign-off Date:** 7/24/2006

**Approved for Web Publishing:** Yes

**Date Published:** <<Date approved for Web Publishing>>

---

## **06.3 HHS PIA Summary for Posting (Form) / OIG Data Warehouse [System]**

### **PIA SUMMARY AND APPROVAL COMBINED**

#### *PIA Summary*

**Is this a new PIA 2011?** Yes

**If this is an existing PIA, please provide a reason for revision:**

**1. Date of this Submission:** 7/6/2011

**2. OPDIV Name:** OIG

**3. Unique Project Identifier (UPI) Number:**

**4. Privacy Act System of Records (SOR) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):** 09-90-1000

**5. OMB Information Collection Approval Number:** No

**6. Other Identifying Number(s):** No

**7. System Name (Align with system Item name):** OIG Data Warehouse (OIGDW)

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:** Patrick J. Kelly

**10. Provide an overview of the system:** The OIG Data Warehouse maintains federal data and federally contracted data sources including, but not limited to, an extract of Medicare paid claims data from the CMS National Claims History Data Base, DEA Retired Registrants, National Council for Prescription Drug Program file, National Plan and Provider Enumeration System file, PECOS Global Extract File, SSA's Death Master File, Unique Physician/Practitioner Identification Number (UPIN) files, and DEA Active Registrant files sufficient to conduct the data analyses underlying OIG's audits, inspections, and investigations of the Medicare program. The OIG obtains this information under the authority of the Inspector General Act of 1978, 5 U.S.C. App. 3. The information contained in the database documents paid claims information submitted by health care providers for inpatient, outpatient, home health, hospice, skilled nursing facility, physician and supplier and durable medical equipment. The information includes prescription drug event data and drug pricing data.. The information also includes beneficiary and provider enrollment data. The information contained within contains the necessary data elements to retrieve source documentation from Medicare contactors and providers in the course of audits, inspections and investigations. Data contains HIPAA and Privacy Act information.

**13. Indicate if the system is new or an existing one being modified:** New

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system? (Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether 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. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?):**

Yes



**21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):** Yes

**23. If the system shares or discloses IIF please specify with whom and for what purpose(s):**

The information is maintained for OIG internal use. However, information may be provided to entities outside the OIG where it is essential to conduct audit, inspection, and investigative activities. For example, personally identifiable information may be selectively provided to a healthcare provider or Medicare contractor in order to obtain additional medical information essential to an audit, inspection, or investigation. The OIG may also provide information to the Department of Justice to support an ongoing criminal investigation or court case.

**30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:** The information contained in the database documents paid claims information submitted by health care providers for inpatient, outpatient, home health, hospice, skilled nursing facility, physician and supplier and durable medical equipment. The information includes prescription drug event data and drug pricing data. The information also includes beneficiary, provider, and supplier enrollment data. The information contained within contains the necessary data elements to retrieve source documentation from Medicare contractors and providers in the course of audits, inspections and investigations. Data contains HIPAA and Privacy Act information. Submission of personal information is mandatory for law enforcement and oversight actions pursuant to the Inspector General Act of 1978. <http://www.ignet.gov/pande/leg/igactasof0609.pdf>

**31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII 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); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) 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, etc.]**) OIG obtains CMS National Claims History Data Base data from the Centers for Medicare & Medicaid Services. The OIG obtains this information under the authority of the Inspector General Act of 1978, 5 U.S.C. App. 3. OIG also obtains information from other CMS systems – the Medicare Enrollment Database, the National Provider Identifier database, the Medicare Advantage Prescription Drug System data file, the Unique Physician Identification Number system files, the Provider Enrollment Chain Ownership System Global Extract file, and the Part B Overpayment Processing System. Drug pricing and drug dispenser information is obtained from a variety of sources (third party vendors and CMS). Drug Enforcement Agency (DEA) active and retired Controlled Substances Act registrant information is obtained from the DEA. Social Security Administration Master Death File data is obtained from the Department of Commerce.

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII):** No

**37. Does the website have any information or pages directed at children under the age of thirteen?:**

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):**

**54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.:** The information is maintained on a centrally managed OIG computer system. Access is restricted by physical and computer-based access controls. Access is strictly limited to authorized OIG staff members via a two level authentication process. Users must be initially authenticated as valid OIG staff and are then authenticated to the OIG Data Warehouse by an independent second level authentication system. All computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standard 200, and the HHS Information Systems Security and Privacy Policy.

***PIA Approval***

**PIA Reviewer Approval:**

**PIA Reviewer Name:** Patrick J. Kelly

**Sr. Official for Privacy Approval:** Promote

**Sr. Official for Privacy Name:** Patrick J. Kelly

**Sign-off Date:** 7/6/2011

**Approved for Web Publishing:** Yes

**Date Published:** <<Date approved for Web Publishing>>

---

## **06.3 HHS PIA Summary for Posting (Form) / OIG Infrastructure Services [System]**

### **PIA SUMMARY AND APPROVAL COMBINED**

#### *PIA Summary*

**Is this a new PIA 2011?** No

**If this is an existing PIA, please provide a reason for revision:** PIA Validation

**1. Date of this Submission:** 3/23/2009

**2. OPDIV Name:** OIG

**3. Unique Project Identifier (UPI) Number:** 009-92-02-00-02-0002-00-404-139

**4. Privacy Act System of Records (SOR) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):** NA

**5. OMB Information Collection Approval Number:** No

**6. Other Identifying Number(s):** No

**7. System Name (Align with system Item name):** Corporate Mission Support System (IGSS)

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:** Patrick Kelly

**10. Provide an overview of the system:** The Corporate Mission Support System provides the computing and communications infrastructure for OIG offices nationwide. It supports all OIG direct mission and administrative activities performed by the OIG under the authority of the Inspector General Act of 1978, 5 U.S.C. App. 3.

**13. Indicate if the system is new or an existing one being modified:** Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system? (Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether 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. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?):**  
No

**21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):** No

**23. If the system shares or discloses IIF please specify with whom and for what purpose(s):**  
NA

**30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:** The Corporate Mission Support System is not an information system in itself. It provides the computing and

communications foundation for and integrates with OIG's information systems. In that capacity, it provides the first level of identification and authentication of OIG staff authorized access to OIG systems and their information. To accomplish this function, it maintains basic identify and organizational assignment information on OIG staff extracted from the Department's Enterprise Human Resource and Payroll (EHRP) System. The information maintained by the Corporate Mission Support System assures the OIG that only OIG staff are authenticated and provided access to OIG's computing and communications infrastructure.

**31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII 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); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) 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, etc.]) None

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII):** No

**37. Does the website have any information or pages directed at children under the age of thirteen?:** No

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):** Yes

**54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.:** The information is maintained on a centrally managed OIG computer system. Access is restricted by physical and computer-based access controls. Access is strictly limited to authorized OIG staff members based on role-based security features that limit access to system administrators, designated administrative personnel, and senior management officials. All computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standard 31, and the HHS Information Resources Management Manual, Part 6, "ADP Systems Security."

*PIA Approval*

**PIA Reviewer Approval:**

**PIA Reviewer Name:** Richard Stern

**Sr. Official for Privacy Approval:** Promote

**Sr. Official for Privacy Name:** Christopher Ballister

**Sign-off Date:** 8/17/2006

**Approved for Web Publishing:** Yes

**Date Published:** <<Date approved for Web Publishing>>

---

## **06.3 HHS PIA Summary for Posting (Form) / OIG Security Program**

### **PIA SUMMARY AND APPROVAL COMBINED**

#### *PIA Summary*

**Is this a new PIA 2011?** No

**If this is an existing PIA, please provide a reason for revision:**

**1. Date of this Submission:** 8/1/2006

**2. OPDIV Name:** OIG

**3. Unique Project Identifier (UPI) Number:** None

**4. Privacy Act System of Records (SOR) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):** N/A

**5. OMB Information Collection Approval Number:** No Value

**6. Other Identifying Number(s):** No Value

**7. System Name (Align with system Item name):** No Value

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:** Lynn Melton

**10. Provide an overview of the system:** No Value

**13. Indicate if the system is new or an existing one being modified:** Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system? (Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether 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. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?):**  
No

**21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):** No

**23. If the system shares or discloses IIF please specify with whom and for what purpose(s):**  
No Value

**30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:** No Value

**31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII 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); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) 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, etc.]) No Value

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII):** No

**37. Does the website have any information or pages directed at children under the age of thirteen?:** No

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):** No

**54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.:** No Value

*PIA Approval*

**PIA Reviewer Approval:**

**PIA Reviewer Name:** Lynn Melton

**Sr. Official for Privacy Approval:**

**Sr. Official for Privacy Name:** Christopher Ballister

**Sign-off Date:** 8/1/2006

**Approved for Web Publishing:** Yes

**Date Published:** <<Date approved for Web Publishing>>

---

## **06.3 HHS PIA Summary for Posting (Form) / OIG Snap Survey [System]**

### **PIA SUMMARY AND APPROVAL COMBINED**

#### *PIA Summary*

**Is this a new PIA 2011?** Yes

**If this is an existing PIA, please provide a reason for revision:**

**1. Date of this Submission:** 3/19/2012

**2. OPDIV Name:** OIG

**3. Unique Project Identifier (UPI) Number:**

**4. Privacy Act System of Records (SOR) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):** N/A

**5. OMB Information Collection Approval Number:** N/A

**6. Other Identifying Number(s):** N/A

**7. System Name (Align with system Item name):** SNAP Survey

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:** Patrick Kelly

**10. Provide an overview of the system:** It is not a system but rather software to build data collection instrument (web surveys), send them as HTML documents, and have the returned information downloaded into databases. The data collection instrument is sent by web server and the completed instrument returned by the respondent will be stored on NIH web server.

**13. Indicate if the system is new or an existing one being modified:** New

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system? (Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether 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. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?):**  
Yes

**21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):** No

**23. If the system shares or discloses IIF please specify with whom and for what purpose(s):**  
N/A

**30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:** The Office of Evaluation and Inspections will collect information from respondents and review their responses as a part of our oversight and review of HHS programs. This information will be analyzed and reported out in OIG published reports but these will not contain will not contain PII data. The information the

regional offices of OEI will collect, maintain or disseminate will vary among each regional office based on the type Medicare or Medicaid study being conducted. The studies ranges from gathering general questions about a Medicare or Medicaid provider type of services, estimate of number of services performed, issues, payment processes, summary of procedures performed, and etc. OEI has asked that PII information is not obtained using the survey. OEI will use the information gathered to report any findings, violations, or issues found in a written report. The survey will not obtain submission or request for personal information. The request for non personal information is voluntary but the survey may require some questions to be answered mandatory in order to analyze and report the information gathered.

**31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII 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); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) 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, etc.])** Each regional inspector general of OEI (POC) will follow OEI change control process if major changes are being planned for the SNAP application. A change request document/email from each regional inspector general of OEI must be sent to Dave Graf the Director of Technical Support Staff in Baltimore, Maryland and OMP IT specialist before changes are implemented. The OEI change control is the only processes we have in place when major changes occur to the system. It is not the purpose of this survey system to collect PII. However, if PII is collected, each regional office will include a statement on how the information will be used or shared. OEI regional office has the option of selecting whether the format of notice of consent will be written or electronic. The method of communicating the notice of consent may be either via mail or email.

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII):**

Yes

**37. Does the website have any information or pages directed at children under the age of thirteen?:**

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):**

**54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.:** The information is maintained on a centrally managed OIG computer system. Access is restricted by physical and computer-based access controls. Access is strictly limited to authorize OIG staff members via a two level authentication process. Users must be initially authenticated as valid OIG staff and are then authenticated to the Audit & Evaluation System by an independent second level authentication system. All computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standard 31, and the HHS Information Resources Management Manual, Part 6, ``ADP Systems Security."

***PIA Approval***

**PIA Reviewer Approval:**



**PIA Reviewer Name:**

**Sr. Official for Privacy Approval:** Promote

**Sr. Official for Privacy Name:** Patrick J. Kelly

**Sign-off Date:** 3/19/2012

**Approved for Web Publishing:** Yes

**Date Published:** <<Date approved for Web Publishing>>

---