United States Department of Agriculture

Privacy Impact Assessment

March 5, 2007

UNITED STATES DEPARTMENT OF AGRICULTURE
Office of the Chief Information Officer
Information Technology Management
Washington, DC 20250

Table of Contents

1.0 Authorization **3**
2.0 Privacy Impact Assessment **4**
Appendix A: Declaration of Privacy Principles **8**
Appendix B: Policy Statement on Citizen, Client and Partner Privacy Rights **10**
Appendix C: List of Attributes from EmpowHR and Payroll-Personnel **11**

-- -- --

1.0 Authorization

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment (PIA) for Enterprise Identity Management Service (EIMS). This document has been completed in accordance with the requirements of the E-Government Act of 2002.

MANAGEMENT CERTIFICATION – Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

By our signatures below, we fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____ System Manager	_____ Date
_____ OCIO/Project Representative	_____ Date
_____ Program/Office Head	_____ Date
_____ OCIO	_____ Date
_____ Chief FOI/PA	_____ Date
_____ Senior Official for Privacy	_____ Date

2.0 Privacy Impact Assessment

Project Name: Enterprise Identity Management Service (EIMS)

Description of Your Program/Project:

EIMS provides USDA agencies with a method to synchronize employee and contractor identity information with authoritative data sources fed from EmPowHR and Payroll Personnel, and the HSPD-12 card management system. USDA Agencies connect to EIMS to receive identity information from these sources.

A. CONTACT INFORMATION

1.	Who is the person completing this document? (Name, title, office, and contact information)	Dean Lindstrom, eGovernment Security Architect, 2150 Centre Dr., Suite 220, Fort Collins, CO 80527, (970) 295-5532, dean.lindstrom@ftc.usda.gov
2.	Who is the system owner?	Owen Unangst, Program Manager, National Resources Research Center, 2150 Centre Dr., Suite 220, Fort Collins, CO 80527, (970) 295-5538, owen.unangst@ftc.usda.gov
3.	Who is the system manager for this system or application? (Name, title, office, and contact information)	Randy Barnett, EIMS Project Manager, National Resources Research Center, 2150 Centre Dr., Suite 220, Fort Collins, CO 80527, (970) 295-5471, randy.barnett@ftc.usda.gov
4.	Who is the IT Security Manager who reviewed this document ? (Name, title, office, and contact information)	Anthony J. Capo, Information Systems Security Project Manager (Acting), OCIO-ITM, 6501 Beacon Dr., Kansas City, MO 64133, Phone: (816) 926-1485, E-mail: anthony.capo@kcc.usda.gov
5.	Did the Chief FOI/PA review this document? (Name, title, office, and contact information)	None
6.	Did the Agency's Senior Office for Privacy review this document? (Name, title, office, and contact information)	Howard Baker, OCIO-eGov, 202-720-8657, Howard.Baker@usda.gov
7.	Who is the Reviewing Official? (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).	Chris Niedermayer, Associate Chief Information Officer, Information Technology Management, USDA-OCIO, 202-690-2118, Chris.Niedermayer@usda.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1.	Does this system contain any information about individuals?	Yes
1a.	Is this information identifiable to the individual?	Yes
1b.	Is the information about individual members of the public?	No
1c.	Is the information about employees?	Yes
2.	What is the purpose of the system/application?	Enterprise identity management
3.	What legal authority authorizes the purchase or development of this system/application?	eGovernment Initiative

C. DATA IN THE SYSTEM

1. Generally describe the information to be used in the system.	EIMS is a synchronization service that acts as a gateway between connected resources for identity-related data.
2a. What are the sources of the information in the system?	The following systems provide authoritative information for identity synchronization: EmpowHR, USDA's HR line of business; Payroll-Personnel (PP), USDA's source of payroll data maintained by the National Finance Center (NFC).
2b. What USDA files and databases are used? What is the source agency?	EmpowHR; Payroll Personnel (CED), GSA (HSPD-12) and USDA (all other sources)
2c. What Federal Agencies are providing data for use in the system?	See 2a
2d. What State and Local Agencies are providing data for use in the system?	None
2e. From what other third party sources will data be collected?	None
2f. What information will be collected from the customer?	None directly; see Appendix C for a list of attributes collected from EmpowHR & PP.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	Data are not independently verified; EIMS provides a synchronization service and is not authoritative for any attributes.
3b. How will data be checked for completeness?	EIMS uses checksums to ensure data synchronizations are complete.
3c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).	Data are not independently verified; EIMS provides synchronization services and is not authoritative for any attributes.
3d. Are the data elements described in detail and documented? If yes, what is the name of the document?	See Appendix C.

D. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes; the system is designed to provide a synchronization service for identity-related data.
2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No data are derived or created.
3. Will the new data be placed in the individual's record (customer or employee)?	No, EIMS does not keep authoritative records.
4. Can the system make determinations about customers or employees that would not be possible without the new data?	No, EIMS does not keep authoritative records.
5. How will the new data be verified for relevance and accuracy?	Not applicable.
6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	See *EIMS Security Model*.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	Not applicable.
8. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Unique attributes are specified for each connecting system.
9. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?	Reports can only be produced on system events, not on individuals.
10. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses and how individuals can grant consent.)?	Not applicable.

E. MAINTENANCE OF ADMINISTRATIVE CONTROLS

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	Not applicable (the system is not operated in more than one site).
2. What are the retention periods of data in this system?	Retention periods vary depending on the authoritative source's designated refresh date; EIMS has no say in this matter
3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?	EIMS is not a data repository per se and does not retain data.
4. Is the system using technologies in ways that the USDA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?	Yes, EIMS uses data synchronization.
5. How does the use of this technology affect public/employee privacy?	It provides an additional exposure point of employee identity information. However, security policies and procedures make it unlikely that this exposure point can be exploited. See the *EIMS System Security Plan.*
6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No, individuals cannot be identified, located, or monitored within EIMS.
7. What kinds of information are collected as a function of the monitoring of individuals?	No monitoring of individuals is done by EIMS.
8. What controls will be used to prevent unauthorized monitoring?	See the *EIMS Security Model* and the *EIMS System Security Plan.*
9. Under which Privacy Act systems of records notice does the system operate? Provide number and name.	No SORN needed; system does not contain original data or accept original data input.

10. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.	No SORN needed; system does not contain original data or accept original data input.

F. ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	Only EIMS administrators have access to the data in the system.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	No users have access to EIMS data. System administrators are granted access according to the policies described in the EIMS System Security Plan.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	No users have access to EIMS data.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	See the *EIMS Security Model.*
5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, are Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?	Yes, contractors are both involved with the design and development of EIMS, and will be involved with EIMS maintenance. Privacy Act clauses and other regulatory measures have been addressed in their contracts.
6. Do other systems share data or have access to data in this system? If yes, explain.	Identity data from EmpowHR and PP are synchronized and distributed to authorized connected systems.
7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?	The system owner.
8. Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?	No other agencies will have access to the data in EIMS.
9. How will the data be used by the other agency?	Not applicable; no other agencies will have access to the data in EIMS.
10. Who is responsible for assuring proper use of the data?	The system owner.

-- -- --

Appendix A: Declaration of Privacy Principles

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the United States Department of Agriculture to the public and are the responsibility of all USDA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the USDA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of USDA data systems, processes and facilities.

All USDA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected.To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the USDA, the USDA will be guided by the following Privacy Principles:

Principle 1: Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.

Principle 2: No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.

Principle 3: Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.

Principle 4: Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.

Principle 5: Personally identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.

Principle 6: Personally identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.

Principle 7: Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the USDA other than as authorized by law and in the performance of official duties.

Principle 8: Browsing, or any unauthorized access of citizen, client or partner information by any USDA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.

Principle 9: Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.

Principle 10: The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the USDA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

-- -- --

Appendix B: Policy Statement on Citizen, Client and Partner Privacy Rights

The USDA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the USDA recognizes that compliance with legal requirements alone is not enough. The USDA also recognizes its social responsibility which is implicit in the ethical relationship between the USDA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the USDA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the USDA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The USDA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. USDA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the USDA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the USDA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the USDA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.

-- -- --

Appendix C: List of Attributes from EmpowHR and Payroll-Personnel

Attributes from EmpowHR	Attributes from Payroll-Personnel (PP)	
▪ birthDate	▪ SSN	▪ DUTY_STATION_CITY_CODE
▪ SSN	▪ AGCY_CODE	▪ DUTY_STATION_CNTY_CODE
▪ CITIZEN_COUNTRY	▪ PAY_PERIOD	▪ DUTY_STATION_STATE_CODE
▪ BIRTHCOUNTRY	▪ LNAME	▪ RESID_ADR_1ST_LINE
▪ BIRTHPLACE	▪ FNAME	▪ RESID_ADD_ADR
▪ sponsorID	▪ MI	▪ RESID_ADD_ADR_2
▪ sponsorEmail	▪ DOB_FMTD	▪ RESID_ADR_CITY_CODE
▪ isPivCardRequired	▪ PAY_GRADE	▪ RESID_ADR_ST_CTRY_CODE
▪ pivCardReqDate	▪ PAY_STEP	▪ RESID_ADR_ZIP_5
▪ cardActivator	▪ NET_PAY	▪ RESID_ADR_ZIP_4
▪ cardOfficeID	▪ APPT_TYPE_CODE	▪ NAME_ADDR_1
▪ cardAddrLine1	▪ EMP_STAT_CODE	▪ NAME_ADDR_2
▪ cardAddrLine2	▪ EMP_TYPE_CODE	▪ CITY_NAME
▪ cardAddrCity	▪ ACTN_CODE	▪ STATE_NAME
▪ cardAddrState	▪ PAY_PLAN_CODE	▪ BLDG_ZIP_5
▪ cardAddrPostalCode	▪ OCCUP_SERIES_CODE	▪ BLDG_ZIP_4
▪ isPriorBckgndInvComplete	▪ POSITION_OFCL_TITLE	▪ POI
▪ equipTrackNumber	▪ POSITION_WORK_TITLE	▪ SCD_FMTD
▪ bckgndInvSubmittingOfficerNumber	▪ TA_CONT_PT_STATE_CODE	▪ OLD_SSN
▪ bckgndInvSecurityOfficerID	▪ TA_CONT_PT_CITY_CODE	▪ SEP_ACCESS_TYPE
▪ bckgndInvOpacAlc	▪ TA_CONT_PT_UNIT_CODE	▪ EAUTH_ID
▪ adjudicationEffectiveDate	▪ AGCY_CODE_AGCY	▪ DS_LAST_UPD_DATE
▪ adjudicatorID	▪ AGCY_CODE_2ND_LEV	▪ DS_CREATE_DATE
▪ adjudicationNotes	▪ AGCY_CODE_3RD_LEV	▪ EM_LAST_UPD_DATE
▪ invTypeDesc	▪ AGCY_CODE_4TH_LEV	▪ EM_CREATE_DATE
▪ isAjudicationApproved	▪ AGCY_CODE_5TH_LEV	▪ SUBAGENCYSTARTDATE
▪ BIRTHSTATE	▪ AGCY_CODE_6TH_LEV	▪ SUBAGENCYENDDATE
▪ sex	▪ AGCY_CODE_7TH_LEV	▪ MIDDLENAME
▪ ETHNIC_GROUP	▪ AGCY_CODE_8TH_LEV	▪ DUTYSTATION_STFIPSCODE
▪ MILITARY_STATUS	▪ PROM_PLAN_CODE	
▪ homeAddress1		
▪ homeAddress2		
▪ homeAddress3		
▪ homeCity		
▪ homeState		
▪ homePostalCode		
▪ homeCountryCode		
▪ BUSN_EMAILID		
▪ HOME_EMAILID		
▪ PHONE		

-- -- --