



Departmental Administration (DA)  
Office of Security Services (OSS)  
Protective Operations Division (POD)

Physical Security Access Control System  
(PSACS)

## **Privacy Impact Assessment**

Version 1.2  
July 10, 2008

**Prepared by:**  
ICAssociates  
6551 Loisdale Road, Suite 500  
Springfield, VA 22150  
Ph: 703-822-8224, Fax: 703-822-8229

---

## TABLE OF CONTENTS

---

<b>1. INTRODUCTION .....</b>	<b>3</b>
1.1. REQUIREMENTS FOR ASSESSMENT.....	3
1.2. BACKGROUND.....	4
<b>2. DATA IN THE SYSTEM .....</b>	<b>5</b>
<b>3. ACCESS TO THE DATA.....</b>	<b>9</b>
<b>4. ATTRIBUTES OF THE DATA .....</b>	<b>12</b>
<b>5. MAINTENANCE OF ADMINISTRATIVE CONTROLS.....</b>	<b>14</b>

---

## 1. INTRODUCTION

---

The Office of Departmental Administration (DA) Office of Security Services (OSS) Protective Operations Division (POD) is within the U.S. Department of Agriculture (USDA). This Privacy Impact Assessment evaluates privacy information residing on the Physical Security Access Control System (PSACS).

The DA/OSS is responsible for providing physical, personal, and document security services. These POD services are provided in the USDA South Building/Whitten complex and at leased buildings in the National Capital Region (NCR).

The PSACS supports access of USDA employees and contractors to the USDA facilities in the National Capital Region (NCR). The system possesses identification (ID) and access control information. These will be addressed separately in this assessment. PSACS manages and maintains employee and contractor badge control system information and monitors access to the various USDA sites and offices within the NCR. PSACS is composed of two (2) servers running MDI software; eight (8) desktops; two (2) laptops, two (2) badging stations, Cisco routers in the USDA South building and four (4) other buildings, an internal private network in the USDA South/Whitten complex to various card readers, and dedicated Integrated Services Digital Network (ISDN) lines to the other 4 buildings.

One server is the primary server and the other the secondary server. The information is mirrored from the primary to the secondary server. Both servers reside in the same computer room. If the primary server goes down, the secondary server automatically takes over. Back up data is stored off-site.

### 1.1. REQUIREMENTS FOR ASSESSMENT

This assessment is for the PSACS that maintains the administrative and security systems, to include badge issuance and control; and facility access control. The assessment of the PSACS will ensure the following privacy security requirements for protecting the system are implemented:

- ♦ Privacy Act of 1974 (5 USC 552a)

- ♦ Freedom of Information Act, as amended (5 USC 552)
- ♦ Computer Security Act of 1987 (Public Law 100-235)
- ♦ Computer Matching & Privacy Protection Act (Public Law 100-503)
- ♦ OMB Circular A-130
- ♦ E-Government Act of 2002
- ♦ Federal Information Security Management Act USDA 3515-002, Privacy Requirements

## 1.2. BACKGROUND

A PIA was conducted on the PSACS based on the requirements stated above. All privacy concerns were considered and identified by analyzing system requirements and making decisions about the data usage and system design.

The ID and access control portions of PSACS were identified as part of the DA Protection Operations System (POS) applications as described in the “DA POS Application System Security Plan (SSP), dated April 2006, with Certification and Accreditation completed in 2004. Due to a recent breach of security and to minimize any continuing threat as well as to enhance the security of the information on the system, the ID and access portions of the POS application were removed and reconfigured to become a stand-alone system (an entity within itself) now known as PSACS. It is important to note that one feature that was removed immediately from the system was the use of social security numbers as an identifying factor.

The PSACS was evaluated for privacy data contained in the ID and access information that is collected from the customers (USDA employees and contractors) for physical access. This assessment not only included information inputted in the PSACS, but also the method used for obtaining that information and where such information is maintained prior to implementation on the PSACS, as well as stored/destroyed afterwards.

It is vital to recognize that this PIA is not a “one-time” procedure. A PIA should be done at various times from planning through implementation, and should become part

of ongoing system upgrades, maintenance schedules and any other modification that affects the PIA in its current state and/or affects the security posture of the system.

---

## **DATA IN THE SYSTEM**

---

The data in the DA/OSS/POD PSACS was evaluated to determine the collection, use, and disclosure. The following document addresses the PSACS Privacy Impact as required.

1. Generally describe the information to be used in the system:

The information contained on the PSACS is used for USDA employee and contractor access to the facility. The system holds Identification (ID) information and access information. The information inputted and contained within the PSACS includes:

- ◆ Name
- ◆ Agency (Name of Company if Contractor)
- ◆ Employee Status (Permanent, Temporary, Retired, or Contractor)
- ◆ Building Location (City, State)
- ◆ Clearance Status (General Status)
- ◆ Facility Access Privileges
- ◆ Work Telephone (Phone Number, Room Number and Badge Number)
- ◆ Pictures
- ◆ Fingerprints (only for those individuals using Biometrics)
- ◆ Signatures

The system has other available fields, which are not being used at this time. Those fields available are identified in the next section, 2a.

2a. What are the sources of the information in the system?

The sources of the information in the system include USDA personnel and contractors with physical access to the USDA buildings (Headquarters Complex, the George Washington Carver

Center, and at selected leased headquarters buildings in the NCR). All personnel requiring access to the USDA facilities must complete the “Request for USDA Identification (ID) Badge” Form AD-1197, OMB Control #0505-0022<sup>1</sup>. The form is compliant with information required for Homeland Security Presidential Directive-12 (HSPD-12), and thus collects information not stored in PSACS. Personal information that is documented in the form includes, but is not limited to, the following section. Those identified with an asterisks mean those fields are not available in the system.

- ◆ Name
- ◆ Compliant ID Badge (Federal Employee, Press Corp, Law Enforcement, Contractor, etc.)
- ◆ Non-Compliant ID Badge (Site, Temporary, Retiree)
- ◆ BI Application Completion\*
- ◆ Expiration Date
- ◆ Work Phone
- ◆ Social Security Number\*
- ◆ Position\*
- ◆ Birth Date\*
- ◆ Organization
- ◆ Work Address (Building location)
- ◆ E-mail\*
- ◆ Identity Source Documents (e.g., Personal Identifying Federal or State governed identification)\*
- ◆ Access Requirements
- ◆ FBI Fingerprint Check/NAC results (“yes” or “no” field only)\*

Some of the information contained in this form is used for input into the PSACS, but not all the information is placed into the system. The information from the form that is contained in the system is stated above, #1.

---

<sup>1</sup> It is the responsibility of USDA DA/OSS to maintain and update this PIA in the event any changes to the form that affect the OMB reference or agency assigned form number.

The Form AD-1197 in its hard copy form is retained and maintained in a locked, GSA fire-proof safe in an access restricted room. There are three (3) USDA authorized personnel with access to this safe. Additionally, information is also retained with this form such as the person's proof of identity photocopy (i.e., passport, driver's license or other federal/state issued identification).

2b. What files and databases are used?

SQL databases are used to retain and retrieve badge information. The Form AD-1197 is used and stored in a GSA rated fireproof safe within a strictly controlled access area, containing motion detection during non-working hours. All forms that need to be destroyed are either burned or shredded in accordance with NIST 800-80. Timing for the destruction is in accordance with the USDA Records Management Program.

2c. What Federal Agencies are providing data for use in the system?

Personnel requiring access and IDs must provide US identification sources, such as passports, Social Security cards, driver's licenses, etc. Such photocopies of this information are retained with the AD-1197 form, as noted above.

There is no electronic interaction with other federal agencies outside of USDA since the PSACS is a stand-alone system in its current configuration.

2d. What State and Local Agencies are providing data for use in the system?

Personnel requiring access and IDs must provide US identification sources, such as passports, Social Security cards, driver's licenses, etc. Photocopies of this information are retained with the AD-1197 form.

There is no electronic interaction with other federal agencies outside of USDA since the PSACS is a stand-alone system in its current configuration.

2e. From what other third party sources will data be collected?

Not Applicable None collected.

2f. What information will be collected from the customer?

All information collected is identified in section 2, number 2a.

3a. How will data collected from sources other than USDA records be verified for accuracy?

Not Applicable, as data is not collected from other sources, except as provided by the customer.

3b. How will data be checked for completeness?

All forms are evaluated and accepted by high level USDA managers prior to entry into the PSACS.



---

## 2. ACCESS TO THE DATA

---

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

USDA personnel with access to the PSACS include a total of seven (7) DA/OSS/POD staff members, all with access only to that data which they need to complete their jobs. Two individuals are responsible for input of information into the system (the security officer and the security assistant). The other five (5) include the system managers, developers and administrators. Each level of access is defined by user level, technician support level, and system administration levels.

The hard copy information on Form AD-1197 has controlled access once placed into the safe, as described previously. Only three (3) DA/OSS/POD personnel have access to this safe.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Only authorized personnel are allowed into the system with access restricted based upon their job function. There are no USDA employees outside of the DA/OSS/POD with access to the PSACS. Access for those who are authorized is determined by the Chief of the Technical Security Branch. Criteria for access are based on need to know and access levels are determined by their job functions.

3. Will users have access to all the data on the system or will the user's access be restricted?

Data access is restricted by access level controls and is determined by the Chief, Technical Security Branch. Read and write capabilities are also restricted to level access. See #2 above.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?

Personnel with access to the system can only have the option to view the fields that are assigned to them and necessary to complete their job.

5a. Do other systems share data or have access to data in this system? If yes, explain.

No. The PSACS is a stand-alone system with no access to the USDA network or to other systems.

5b. Who will be responsible for protecting the privacy rights of the employees affected by the interface?

Not Applicable, as no interface exists.

6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

No other outside Federal agencies share, or have access, to the data contained in the PSACS. Other internal USDA agencies have direct access to the system via dedicated IDSN lines. These include NASS, WAOB, NITC, OIG and Forest Service. These additional USDA agencies are restricted to their individual agency information.

6b. How will the data be used by the agency?

The data in the system will be used to allow USDA personnel (Federal and Contractor) access to approved areas as designated by their management and clearance access levels, as defined in

Form AD-1197. The data will be used to identify physical access of USDA employees<sup>2</sup> and for photographic identification. The data will not be used for other identification purposes.

6c. Who will be responsible for assuring proper use of the data?

The DA/OSS/POD is responsible for ensuring that the data is used for identification and access to the USDA buildings and no other purposes.

---

<sup>2</sup> See Section 2, 1. for definition of USDA employees for the purpose of this PIA.

---

### 3. 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. Only relevant data is placed into the system.

2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No. There is no information in the system that could be aggregated.

2b. Will the new data be placed in the individual's record?

Not Applicable, as no new data is derived.

2c. Can the system make determinations about vendors or employees that would not be possible without the new data?

Not Applicable, as no new data is derived.

2d. How will the new data be verified for relevance and accuracy?

Not Applicable, as no new data is derived.

3a. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The data is restricted by logical access to any outside resources, and is contained within a secured area as depicted in the System Security Plan (SSP), dated November 2006.

3b. If the processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

Not Applicable, as no processes or data are consolidated.

4a. How will the data be retrieved? Can it be retrieved by personal identifier?

Data can be retrieved by a personal identifier (name), or by any of the fields contained in the PSACS.

4b. What are the potential effects on the due process rights of employees of: consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision making; use of new technologies?

There would be no impact on the employees' due process of rights

4c. How are the effects to be mitigated?

Not Applicable, as no effects exist.

---

#### **4. MAINTENANCE OF ADMINISTRATIVE CONTROLS**

---

1. Explain how the system and its use will ensure equitable treatment of employees.

The only use of the system is for identification and access roles.

2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system is operated solely in one environment, at the USDA South Building.

2b. Explain any possibility of disparate treatment of individuals or groups?

Not Applicable, as the only use of the system is for identification and access roles.

2c. What are the retention periods of data in this system?

The period of retention for the electronic files in the system is five (5) years. At that time, information is updated. In the event personnel leave, the information is held for one (1) year in accordance with NARA.

The hard copy forms are maintained for a period of two (2) years after termination of employment.

2d. What are the procedures for eliminating the data at the end of the retention? Where are the procedures documented?

All assets will be disposed of in accordance with USDA policies and NIST 800-88. All data (electronic and hard copy) will be purged and certified clean prior to and after disposal.

2e. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Not applicable as it is outside of the scope of the PSACS, and remains the responsibility of the USDA Human Resources department.

3a. Is the system using technologies in ways that the USDA has not previously employed?

No.

3b. How does the use of this technology affect employee privacy?

Not Applicable.

4a. Will this system provide the capability to identify, locate, and monitor individuals?

Yes. It will monitor those authorized using access cards into restricted areas.

4b. Will this system provide the capability to identify, locate, and monitor groups of people?

Not Applicable

4c. What controls will be used to prevent unauthorized monitoring?

Monitoring is conducted only by authorized personnel and is controlled in a restricted access area. Any reports that can be gathered to identify personnel monitoring is strictly controlled by the Chief, Technical Security Branch and by physical access.

5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

The System of Records Notices applicable to this system are General Personnel Records, OPM/Govt-1, and Personnel and Payroll System for USDA Employees, OP-1.

5b. If the system is being modified, will the SOR require amendment or revision?

The system is scheduled to be replaced in 2009. The existing SOR is being reviewed for amendment or revision for the new system.



## PRIVACY IMPACT ASSESSMENT AUTHORIZATION

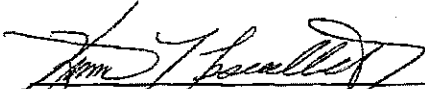
### MEMORANDUM

I have carefully assessed the Privacy Impact Assessment for the  
Physical Security Access Control System


\_\_\_\_\_  
(System Name)

This document has been completed in accordance with the requirements of the  
EGovernment Act of 2002.

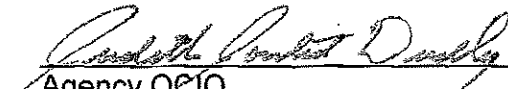
We fully accept the changes as needed improvements and authorize initiation of work to  
proceed. Based on our authority and judgment, the continued operation of this system is  
authorized.

  
\_\_\_\_\_  
System Manager/Owner  
OR Project Representative  
OR Program/Office Head.

07-10-08  
Date

  
\_\_\_\_\_  
Agency's Chief FOIA officer  
OR Senior Official for Privacy  
OR Designated privacy person

7-10-2008  
Date

  
\_\_\_\_\_  
Agency OCIO

7-10-2008  
Date