Privacy Impact Assessment
for the

Password Issuance and Control System (PICS)

November 24, 2009

Contact Point
Luke McCormack
Chief Information Officer
U.S. Immigration and Customs Enforcement
(202) 732-2000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Password Issuance and Control System (PICS) is used by U.S. Immigration and Customs Enforcement (ICE) and U.S. Citizenship and Immigration Services (USCIS) for password management and to manage user access to ICE and USCIS information systems. ICE has conducted this PIA because the system collects personally identifiable information (PII).

Overview

PICS is owned by the ICE Office of the Chief Information Officer (OCIO). The system automates the process of requesting, issuing, and managing user IDs and passwords required to gain access to certain ICE and USCIS information systems. For most PICS-supported systems, PICS only supports user access to the application itself, however, for a few systems, PICS also manages user access to functionality within the application such as read/write privileges (user roles). Users whose information is stored in PICS include DHS employees and contractors; other Federal, state and local government employees; and applicants (selectees for job vacancies).

The primary function of PICS is to administer user access to certain ICE and USCIS information systems and to ensure authorized users of those systems meet the minimum security requirements for access. Each PICS-supported system is assigned a security level by the system owner at the time the system is placed under PICS control. The security level reflects the system owner's requirement for the type of background investigation and/or level-of-trust clearance users must have before they are granted access to the system. To enforce the security levels in place for each system, PICS uses personnel security information on DHS personnel and other individuals to determine if a prospective user of a PICS-supported system has obtained the appropriate level-of-trust clearance. PICS receives this personnel security information indirectly from the ICE Security Activities Reporting System (SARS), in which ICE and USCIS record and track level-of-trust clearances for their personnel and contractors. SARS passes this information to another ICE system, known as Personnel Security System (PERSECS). PERSECS also receives and stores personnel security information from U.S. Customs and Border Protection (CBP) for its employees and contractors, as well as information from other non-DHS Federal, state, and local agencies for personnel that may require access to PICS-supported systems. Personnel security information for all active individuals within PERSECS is extracted and loaded daily to PICS.

Individuals must complete ICE Standard Forms G-872A (for mainframe systems) and G-872B (for non-mainframe systems) to request access to PICS-supported ICE or USCIS systems. These forms must be approved by the individual's supervisor before access will be granted. Completed requests are processed by a PICS Security Officer for the particular system to which access is sought.

The PICS Security Officer verifies the G-872 for completeness, then signs on to the PICS application and selects the individual requesting access from the PICS database using the individual's Social Security Number. Prior to granting user access, PICS verifies that the individual's level-of-trust clearance meets the minimum security level for the PICS-supported system to which access is sought. If the individual's clearance is insufficient for the requested system, PICS will automatically deny the request to access the system. If the request is granted, PICS assigns a user ID for the new user to access

the PICS-supported system. PICS also creates a one-time-use password for the new user, which is marked for immediate expiration to force the user to change the password at the time of the first login. The password value must conform to the rules established by DHS and the particular system.

New users to ICE and USCIS systems are required to read and sign the DHS Rules of Behavior form before receiving their user IDs and initial passwords from the PICS Security Officer. This form is the user's acknowledgement and acceptance of the security rules and restrictions required by DHS in their access to the DHS system.

User access to a PICS-supported system may be terminated for several causes: (1) when a user no longer requires access to a specific system; (2) if the user failed to comply with password security regulations; or (3) if the user has separated from DHS. If the user no longer requires access to a specific PICS-supported system, the user completes the appropriate G-872 form to request account termination and submits it to the local PICS Security Officer. If a user separates from DHS or fails to comply with password security regulations, appropriate changes will be made in PERSECS, which will notify PICS to inactivate their accounts on PICS-supported systems. The user's records within the PICS database are marked by PICS as terminated and are retained for the period described in Section 3 below.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

PICS maintains information on DHS employees and contractors (including but not limited to ICE, USCIS and CBP), other federal, state and local government employees, and applicants (selectees for job vacancies). The information maintained on these individuals includes name, Social Security Number (SSN), work phone number, level-of-trust clearance, duty station location, organization code (or company name if a contractor), requestor type (employee, contractor, other government agency employee, etc.), and dates of user record creation, update, activation, and deactivation.

PICS also maintains user account data for each PICS-supported system to which the individual has access. This information includes the system-specific user ID, account create and update dates, the encrypted password (assigned at account creation or as the result of a password reset request), account status, and date the account was terminated if applicable. There may be multiple sets of account information if the requestor has had an account for a PICS-supported system and let it expire, such as by not complying with password regulations in the required timeframe. To restore expired accounts, PICS creates a new user ID and new account records for the specific PICS-supported system.

PICS also maintains information about requests for access to specific PICS-supported systems. Information retained includes the date the privilege was granted and removed (if applicable), the date of the request, the date the request was rejected (if applicable), the system name, the assigned user role within the system, status of the privilege, and the user ID of the PICS Security Officer performing the action.

1.2 What are the sources of the information in the system?

PERSECS is the primary source of information about individuals in PICS and data for all active individuals within PERSECS are extracted and loaded daily to PICS. PERSECS receives PII in the form of personnel and personnel security data from three sources. For ICE and USCIS employees, contractors and applicants, SARS pushes personnel security data to PERSECS. For CBP personnel and non-DHS government agency personnel, personnel security data is input into PERSECS directly. The U.S. Department of Agriculture's National Finance Center (NFC), which is used by ICE and USCIS for personnel and payroll processing, also provides active personnel data for DHS employees to PICS via an interface with PERSECS.

The individual also serves as the source of information when requesting access to a PICS-supported system, and provides his or her own information using system access forms G-872A "CIS and End User requests for ADP Password" and G-872B "Client/Server requests for ADP Password."

1.3 Why is the information being collected, used, disseminated, or maintained?

This information is collected and maintained to allow DHS to administer user access and privileges to certain ICE and USCIS information systems and to ensure authorized users of those systems meet the minimum security requirements for access. The information is necessary for the authentication of users and the administration of system access processing, which includes the granting and revocation of user access to PICS-supported systems, user notification, and password management. The SSN is necessary to uniquely identify the individual and because it is the unique identifier used by the system (PERSECS) that is the primary source of data for PICS.

1.4 How is the information collected?

The individual requesting access submits information using Form G-872A "CIS and End User request for ADP Password" or Form G-872B "Client/Server requests for ADP Password." The information submitted is verified against the information received electronically by PICS from PERSECS. PERSECS data is collected from the individual by the employing agency or company during the hiring and personnel security investigation process.

1.5 How will the information be checked for accuracy?

Information provided by the individual on the form G-872 is verified against personnel information received from PERSECS.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Federal Information Security Management Act, 44 U.S.C. § 3541 et seq., allows for the collection of this information.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: There is a privacy risk that more information will be collected and maintained than is necessary to carry out the purposes of the system.

Mitigation: The risk has been mitigated by ICE's practice of collecting and maintaining a limited amount of information about individuals to carry out the purposes of the system. All PII collected is necessary in the context of PICS-supported systems to verify an individual's identity, to determine whether to grant user access requests, and to perform user account management. The limited scope of information collected ensures that any risks inherent to over-collection and accuracy of PII are mitigated.

Privacy Risk: There is a privacy risk that the information in the system is inaccurate.

Mitigation: The risk is mitigated by the collection of information directly from the requestor who completes the G-872 access request forms. This ensures that the information is as accurate as possible. Personnel information collected during the hiring and background check processes is verified by ICE using data from other systems that contain highly reliable information about the individual. Some of this information is also obtained from the individual. These factors minimize the risk that inaccurate information will be included in or will continue to exist in PICS.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

PICS information is used to track individual requests for access to certain ICE and USCIS systems, to authenticate users, and to administer system access and privileges for users. PICS uses the SSN to uniquely identify individuals within the PICS database, and to verify the individual's level-of-trust clearance to ensure they are cleared to access the PICS-supported system. SSNs are also used to ensure that any actions to grant or suspend user access to PICS-supported systems are directed at the correct individual. The name and phone number fields are used to identify and communicate with the user.

2.2 What types of tools are used to analyze data and what type of data may be produced?

PICS can run simple reports to identify users with system access by changes to level-of-trust clearance; authorized users by system and location; access requests by status and location; activity reports by PICS Security Officer; and detailed privileges by user.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

This system does not use any commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Users complete mandatory annual privacy and security training, which stresses the importance of authorized use of personal data in government systems. Individuals who are found to have accessed or used the PICS data in an unauthorized manner will be disciplined in accordance with ICE policy.

In the standard operating procedures for the system and in the training provided to staff members, system users are instructed how to protect information in the system from disclosure to inappropriate third parties. For example, requests for access are submitted to local PICS Security Officers since they are usually co-located with the requestor. The local PICS Security Officer verifies the identity of the requestor through visual inspection of government identification. If a face to face meeting is not possible, the requestor faxes the G-872 to the closest PICS Security Officer and the requestor's supervisor is contacted to confirm the requestor's identity, the requestor's official need to access the system, and the supervisor's approval of the request. These procedures ensure privacy risks associated with the potential misuse of data remain mitigated.

Section 3.0 Retention

3.1 What information is retained?

All information entered into PICS is retained in the system. This includes the information described in Question 1.1. The system will also retain any historical activities related to the individual, such as granted privileges, revoked privileges, and inactivated user IDs.

3.2 How long is information retained?

Pursuant to General Records Schedule 24 (GRS24) item 6a, "User Identification, Profiles, Authorizations, and Password Files," PICS records are to be destroyed / deleted six (6) years after user separates from DHS, or when no longer needed for investigative or security purposes, whichever is later.

The G-872 forms used for requesting access to PICS-supported systems are scanned onto a secure location on the network and are destroyed / deleted after six (6) years. The physical G-872 forms will be retained in a locked environment and are to be destroyed after six (6) years at the field offices or destroyed immediately after scanning at headquarters.

PICS system backups are to be destroyed / deleted after six (6) months.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Because ICE is relying on a General Records Schedule, NARA is not required to approve the retention period. The retention schedule for PICS is in progress and will be approved within ICE.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: The risk presented is that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: The information in PICS is retained for a period of time intended to ensure it is available throughout the individual's association with DHS and as may be needed for security investigations or audits. The retention period is consistent with NARA's General Records Schedule for these types of system access records and appropriate in length given the agency's mission and the purpose of the password management program.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Upon request from the owners of PICS-supported systems, ICE provides PICS data to those system owners containing extracts of user data for that system (specifically, user name, level of access, and organization code). For non-mainframe systems, PICS also provides user information to PICS-supported system databases in order to process requests to grant and revoke system access. PICS discloses only the individual's SSN, initial password and the access level within the receiving system. For mainframe systems, PICS shares data with another ICE system to allow for the control of access to those systems.

4.2 How is the information transmitted or disclosed?

The data extracts and file transmissions occur within the DHS network behind the DHS firewall.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risks: There is a risk that data will be shared using an unsecure interface / method.

Mitigation: The privacy risks posed by PICS's outgoing interfaces with other DHS databases are mitigated by several factors. First, the interfaces are performed through a batch process. A batch process is more secure than a real-time connection because it is an executable routine that is not accessible to PICS online users. The interfaces also occur within the DHS network behind the DHS firewall, and are therefore highly secure.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

PICS data are not shared outside of DHS.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

PICS data are not shared outside of DHS. The data in PICS is covered by DHS/ALL-023, Personnel Security Management SORN (74 FR 2906, January 16, 2009) and by the General Information Technology Access Account Records System (GITAARS) SORN (73 FR 28139, May 15, 2008).[1]

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

PICS data are not shared outside of DHS.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Since PICS data are not shared outside of DHS, there are no risks associated with external sharing.

[1] Please visit www.dhs.gov/privacy for additional information on the Personnel Security Management and General Information Technology Access Account Records System SORNs.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

The G-872 forms contain a Privacy Act statement that provides notice to the individual before his or her information is collected for purposes of adjudicating an access request for a PICS-supported system. PICS also receives PII on individuals from other federal systems that maintain that information for personnel management and security related purposes. Individuals that provided that information to the agency initially in job applications or on personnel security application forms received notice of the purposes and uses of the information being collected.

Additionally, notice is provided by this PIA and the DHS Personnel Security Management SORN and General Information Technology Access Account Records System SORN.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes, but if an individual elects not to provide the information requested on the G-872 forms, he or she will be unable to gain access to the PICS-supported system.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. If the requestor provides the information on the form, there is no opportunity to consent to some uses and not others. Each use of the information will comport with the DHS Personnel Security Management SORN, and the General Information Technology Access Account Records System SORN.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Individuals who seek to access PICS-supported systems are provided four forms of notice: this PIA, the DHS Personnel Security Management SORN, the General Information Technology Access Account Records System SORN, and the Privacy Act Statement included on the G-872 forms. Notices are accurate and reflect the current stated uses and sharing of the information. This notice is sufficient to mitigate any risks associated with a lack of notice of the collection of the information or the uses of the information.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals are encouraged to create a copy of their request (Form G-872) at the time of the form's submission. In addition, individuals may request access to records about them in PICS by following the procedures outlined in the DHS Personnel Security Management SORN, and the General Information Technology Access Account Records System SORN.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If individuals obtain access to the information in PICS pursuant to the procedures outlined in the DHS Personnel Security Management SORN, and the General Information Technology Access Account Records System SORN they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the DHS Personnel Security Management SORN, and the General Information Technology Access Account Records System SORN.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). If an individual believes more than one component maintains Privacy Act records concerning him or her

the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.3 How are individuals notified of the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in the DHS Personnel Security Management SORN, the General Information Technology Access Account Records System SORN, and in this PIA in Questions 7.1 and 7.2.

7.4 If no formal redress is provided, what alternatives are available to the individual?

As stated, individuals may submit Privacy Act requests for information and correction, which will be reviewed and corrected on a case-by-case basis.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risks: A risk is presented that individuals may not have a method of correcting information about them in PICS.

Mitigation: This risk is mitigated by the fact that individuals have the means to access and correct information about them in PICS through the ICE FOIA office by submitting a formal request to access or correct their records under the Privacy Act where appropriate.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

Requests for PICS user access must be submitted using the Form G-872. The G-872 is prepared by prospective PICS users and signed by a supervisor, who must identify the type of PICS access the individual requires. These requests are then forwarded to a PICS Security Officer for processing. The ability to grant access to PICS is restricted to PICS personnel at ICE Headquarters, which provides consistent oversight. User roles in PICS ensures that the individual only has access to appropriate data as determined by the individual's supervisor, and that access is related to the individual's official duties.

8.2 Will Department contractors have access to the system?

Yes. PICS access is granted to DHS contractors performing password management related activities. All contractors must request access through the procedures described in Question 8.1.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All ICE personnel and contractors complete annual mandatory privacy and security training and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information. PICS training for PICS Security Officers is conducted by ICE Headquarters PICS personnel or by DHS contractors authorized by the ICE Headquarters PICS Office.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. PICS was granted an Authority to Operate (ATO) on December 29, 2006. This ATO expires on December 29, 2009.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

PICS verifies user credentials with each read to the PICS database to ensure the user is authorized to view the data. The type of access executed by the user within PICS is also verified with every activity. The audit records capture information associated with any insert, update, or delete of records in PICS. This information will include the date/time of the activity, identification of the user that performed the activity and the values changed during the activity through the capture of before and after record images. This audit trail provides adequately detailed information to facilitate the reconstruction of the events prior to the time of system compromise or malfunction. The database level audit trail provides information pertaining to users attempting to logon to, view, and /or edit data in PICS. All audit trails are protected from actions such as unauthorized access, modification and destruction that would negate its forensic value.

ICE has a process in place for investigating and responding to suspicious activities on the system. That process includes automated tools to assist the administrators in their monitoring, analysis, and reporting. The process is consistently followed. PICS runs within the DHS network and is protected by DHS network firewalls. The real time interfaces from PICS to other ICE applications are protected by DHS firewalls.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risks: The privacy risks to this system are primarily the risks of unauthorized system access or use and inadequate system security.

Mitigation: Both risks have been mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above and elsewhere in this PIA, those controls include user access controls, auditing, intrusion detection software, and user training.

Section 9.0 Technology

9.1 What type of project is the program or system?

PICS is an internal ICE application designed to track requests for system access, automate and support system access, and to authenticate system users of multiple ICE and USCIS systems.

9.2 What stage of development is the system in and what project development lifecycle was used?

This project is in the Operations and Maintenance stage and was developed using the governance documents in force at the time of its development, specifically the Immigration and Naturalization Service System Development Life Cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security