Privacy Impact Assessment
for the

Automated Continuing Evaluation System (ACES) Pilot

April 9, 2007

Contact Point
Ken Zawodny
Chief, Personnel Security Division

Personnel Security Division
DHS Office of Security
officeofsecurity@dhs.gov

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The Department of Homeland Security (DHS) is working with the Department of Defense to pilot the Automated Continuing Evaluation System (ACES). ACES conducts automated records checks to identify new issues of security concern for DHS personnel and contractors requiring a security clearance. During the ACES pilot, DHS will assess the feasibility of using ACES for initial and continuing evaluation of DHS security clearance holders. This Privacy Impact Assessment (PIA) is for the DHS implementation of the ACES Pilot.

Introduction

The Automated Continuing Evaluation System (ACES) is an automated computer system developed by the Department of Defense (DoD) Defense Personnel Security Research Center (PERSEREC) to be used for DHS personnel and contractors requiring a security clearance. ACES automates the collection and analysis of information pertinent to assessing whether a person applying for or holding a security clearance meets the national standards for granting that security clearance. This process will significantly improve the checks that are conducted against multiple data sources identified below. ACES checks are only conducted on DHS employees and contractors who have signed a Standard Form (SF) 86 Authorization for Release of Information that is still valid at the time the record checks are performed. The tool is similar to the manual periodic reinvestigations that are performed on security clearance holders. ACES is a tool for the Office of Security to identify potentially derogatory information more efficiently than the manual process to ensure that national security information is protected. This tool supplements and does not replace the existing reviews by Office of Security personnel. Use of the tool is subject to applicable labor, personnel and security laws, rules and regulations, and DHS is committed to complying with those requirements when implementing this significantly improved process.

During the ACES pilot, DHS will provide personally identifiable information on approximately 20,000 of headquarters and component personnel security clearance holders or applicants to DoD PERSEREC. This data will be loaded into the ACES database. PERSEREC will use ACES to generate and transmit inquiry files to external data providers identified below and to query other databases stored internally within ACES (also identified below) to obtain matching records.

For example, a credit inquiry containing required personal identifiers will be sent electronically by ACES via a secure web service interface to a credit bureau. The individual's credit report data will be returned via the same electronic interface to ACES. The electronic records obtained from these data matches will be loaded into ACES by automated or semi-automated processes until all of the returned records have been loaded.

Automated procedures (i.e., business rules) within ACES will be applied to these records to identify individuals in the sample who may have new issues of personnel security concern. At the end of this step, ACES will generate two primary reports: (1) Central Adjudication Facility (CAF) Notification report that will list the name, personal identifiers, and the total number of issues flagged for each individual evaluated,

and (2) an ACES summary report that will contain a list of issues identified, sources checked, the number of records found, and a copy of the underlying records obtained, such as the credit report, criminal history and Standard Form (SF) 86 completed by each individual evaluated.

PERSEREC will transmit the ACES reports to the DHS Office of Security Personnel Security Division (PSD) via the Office of Personnel Management (OPM) Secure Portal. The OPM Secure Portal is a government owned system used by DHS and other government entities for the transmission of sensitive but unclassified data concerning personnel security clearance investigations. DHS PSD will distribute the ACES reports to the appropriate DHS Component Personnel Security Officer via the OPM Secure Portal. The DHS Component Personnel Security Officer will log into the OPM Secure Portal to access their ACES reports.

The Component Personnel Security Officer will review the ACES reports and print out the CAF notification and associated Summary Reports for those individuals flagged during the check. The printed ACES information will be assigned to a trained ACES adjudicator located at the DHS Component site for further evaluation. Use of the ACES reports will be subject to the existing personnel security policies and procedures in place at the Component location.

The Adjudicator will review the ACES information to determine if prior investigations had identified the issue(s), or if the new issue(s) identified has merit. The Adjudicator will then complete an ACES content evaluation form for each ACES case evaluated indicating the disposition of the possible security issues identified by ACES. These evaluation forms will help DHS and PERSEREC determine whether the pilot was successful in identifying possible security concerns. These evaluations will be identified only by an ACES generated case number to minimize privacy impact. PERSEREC will collect and retain the evaluation forms as described below, compile the results, and prepare a summary of the content evaluations for DHS at the end of the pilot.

Section 1.0 Information Collected and Maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

There are two types of data discussed in this section: 1) the data DHS collects and subsequently provides to PERSEREC for the purposes of initiating the ACES checks on a pool of eligible personnel, and 2) the data that ACES collects from its data providers to provide to DHS in the form of individual reports.

DHS COLLECTED INFORMATION

DHS Personnel Security Database Data

The data collected from DHS Headquarters and component databases will be used to identify the pool of eligible personnel for ACES checks. This information includes Social Security Number (SSN), name, date of birth (DOB), place of birth (POB), clearance eligibility and eligibility date, granting central adjudication facility (CAF), person category, date last investigation closed, investigation type and investigating agency, and current type of investigation. ACES will use this information to generate inquiry

files for other records checks conducted by ACES. The information is also displayed on the reports generated by ACES for purposes of identifying the individual and directing the information to the correct adjudication facility.

OPM Personnel Security Questionnaire Data

DHS will provide to PERSEREC the completed SF-86 data for the 20,000 DHS security clearance holders or applicants selected for this pilot. This information includes an applicant's name, date of birth, Social Security number(SSN), mother's maiden name, mailing address, phone numbers, medical notes, financial delinquencies, information about civil court actions, criminal history, education record, military status, employment history and status, foreign activities, and drug and alcohol use history. It also includes the name, date of birth, and address of all close relatives, as well as the names and telephone numbers of people who know the applicant well. ACES will use this information to identify new issues of personnel security concern and to generate inquiry files for other records checks.

ACES Summary Report

If ACES identifies a possible security concern, ACES will generate an ACES Summary Report. The ACES Summary Report contains all supporting documentation collected by ACES, as discussed below. This information is transmitted to DHS Office of Security for review and possible action. The Office of Security will follow established due process guidelines for actions taken. The ACES Summary Report will be added to the individual's security file.

DOD PERSEREC COLLECTIONS

ACES will collect and maintain detailed underlying record data from the following commercial and government data sources (the entire credit report, criminal history record, etc.). This level of detail is required in order to conduct further research when ACES identifies a match indicating a possible security issue for an individual. This allows DHS to conduct additional research to determine whether the record obtained is really associated with the subject of investigation, and not with another person. Detailed record information is also necessary for ACES to apply the business rules it uses to identify new, non-duplicate issues of personnel security or counterintelligence concern. ACES will generate a report on each individual summarizing any new issues identified and displaying the underlying records found as a result of the records checks. This report will be provided in the form of an electronic file to DHS through the OPM Secure Portal which may be printed out and retained in hard copy by DHS adjudication facilities.

PERSEREC sends certain individual information to approximately 38 databases to determine if there is a personnel security concern. The ACES Summary Report contains all supporting documentation collected by ACES, as discussed below. Any new issues identified from these records will be summarized on the ACES Summary Report. This report is transmitted to DHS Office of Security for review and possible action.

Electronic Personnel Security Questionnaire (EPSQ)

ACES will query the EPSQ, which maintains information on any individual who has held a security clearance through DoD. PERSEREC maintains a copy of the database for searching. This information includes an applicant's name, date of birth, SSN, mother's maiden name, mailing address, phone numbers,

medical notes, financial delinquencies, information about civil court actions, criminal history, education record, military status, employment history and status, foreign activities, and drug and alcohol use history. It also includes the name, date of birth, and address of all close relatives, as well as the names and telephone numbers of people who know the applicant well. ACES uses this information to identify new issues of personnel security concern and to generate inquiry files for other records checks. ACES will summarize any new issues on the ACES Summary Report. The ACES Summary Report along with a complete copy of the EPSQ record will be provided to DHS upon completion of the ACES check.

Defense Security Service Case Control Management System

ACES will search the archived Defense Clearance and Investigation Index (DCII) for record matches. PERSEREC maintains a copy of the archived database for searching. The DCII database is no longer in use and does not receive any updates. The SSN will be used to locate any information on file for the applicant in the Defense Security Service (DSS) DCII segment of the Case Control Management System (CCMS). The Person ID is a unique ID number generated by the DSS Case Control Management System to identify the person and is not used to identify an individual outside of the database. Information from this record will include applicant's SSN, sex, name, alias names, citizenship and marital status information. Data is also collected from the applicant's CCMS clearance, clearance investigation and credit record.

DoD Joint Personnel Adjudication System (JPAS)

ACES will search the DoD Joint Personnel Adjudication System (JPAS), using the applicant's SSN and both a DoD and JPAS personal identifier to gather information on existing security clearance records. PERSEREC maintains a copy of the database for searching, and receives an update of the database on a quarterly basis. This collection includes the applicant's name, alias names, date and place of birth, citizenship, foreign relatives, military service or DoD civilian agency affiliation and separation information. Data from security clearance applicants' s investigation, clearance adjudication, and clearance access records will also be gathered. This information will be used to determine whether a clearance applicant already has, or had eligibility for access to classified information in association with DoD.

Defense Manpower Data Center Database

PERSEREC will send an inquiry file to the Defense Manpower Data Center (DMDC) to conduct a data match with twelve different types of records described below. DMDC will return the matching records to ACES. ACES will use the information to identify new issues of personnel security concern. Any new issues identified from these records will be summarized on the ACES Summary Report. The ACES Summary report along with complete copies of these records from DMDC will be provided to DHS at the completion of the ACES check.

Pay records from DoD regular officer and enlisted military pay files, reserve military pay files, DoD civilian, and OPM civilian pay files will be collected. This data will include the applicant's SSN, name, date of birth, military service, military unit, DoD or OPM civilian organization or agency, pay grade and pay status data, and income from salary, wages, allowances, bonuses, and awards. Additional information from

the officer and enlisted military pay records will include separation information and time lost. Additional information from the OPM pay records includes applicant's gender and occupation.

The DMDC Active Duty Officer and Enlisted Personnel Loss records will be queried and information from applicant's records will be collected. Information from these files will include applicant's name, SSN, DOB, sex, race and ethnic data, Service and component, pay grade, type of separation, and separation data to include date, type of loss, character of service, and reenlistment eligibility for enlisted separations.

ACES will query files at the DMDC will be queried and information from the DoD Military Reserve Personnel file collected and will include applicant's name, SSN, sex, date and place of birth, citizenship status, race, ethnicity, marital and dependent status, race, and citizenship data. Applicant's Service, component, unit, unit and individual location, pay grade, promotion and appointment data and dates, and separation information will also be collected. The separation information will include the character of service and reenlistment eligibility for enlisted personnel.

DoD Civilian Personnel and Transaction files at the DMDC will be searched and information collected will include applicant's name, SSN, date of birth, DoD bureau and/or agency affiliation and location, pay plan and pay grade data, promotion data, nature of personnel actions, date and authority for personnel actions, performance rating data, promotion information, and military reserve status.

The DMDC DoD Prior Military Service File will be checked and data pertaining to the applicant's military Service record gathered. This data will include applicant's name, SSN, date of birth, Service affiliation, and separation data. Separation data elements include date of separation, character of service, and reenlistment eligibility.

The DoD Drug Testing records at the DMDC will be checked and data on any DoD drug tests found for the applicant will be collected. This data includes applicant's name, SSN, DOB, service affiliation, specimen collection dates and places, as well as test dates and results.

Credit Bureau Reports

ACES will send inquiry files to the three major credit bureaus to obtain credit reports. Credit bureau records will be checked to include the date the data was pulled and the applicant's SSN, date of birth, name, aliases , spouse's name and SSN, current and previous address information, and current and former employer information to include applicant's salary. Creditor data will also be collected and includes account information, payment amounts, account balances, past due amounts, and payment history. Information on collections will be gathered and includes collection agency and creditor information, date paid, and outstanding balance. Public Record data on court judgments will be collected and includes court information and actions, assets, amount of liability, and plaintiff information. Data from credit vendors, to include credit counseling and other miscellaneous information will be included. ACES will use this information to identify any new issues of personnel security concern and to generate inquiry files for other records checks. The ACES Summary Report will identify any new issues from the credit report records. The ACES Summary report along with complete copies of the credit report records will be provided to DHS at the completion of the ACES check.

Real Estate Records

ACES will search the national real estate records for record matches. PERSEREC maintains a copy of the database for searching, and receives updates on a monthly basis. Real Estate records will be checked and data collected will include the applicant's name, address, address and other descriptive data regarding the real estate, the sale and assessed value of property, tax information and characteristics of the property. Information on the title, deed and loan will be included. This information will be used to identify any new issues of personnel security concern.

Boat Registration Records

ACES will send inquiry files to LexisNexis in order to obtain boat registration records associated with the individuals being checked. Boat Registration reports will be obtained from LexisNexis and include the applicants (owner's) name, SSN and mailing address. Vessel information includes the title, registration and certification data, vessel identification data, type and characteristics and value of the vessel.

Motor Vehicle Records

ACES will send inquiry files to LexisNexis in order to obtain motor vehicle registration records associated with the individuals being checked. Information collected will include owner's name, date of birth, type of ownership, organization, mailing address and co-owner data. Vehicle data will include the Vehicle Identification Number, registration, title, and plate data, characteristics and value of the vehicle. ACES will use this information to identify new issues of personnel security concern.

Airplane Registration Records

ACES will send inquiry files to the National Law Enforcement Telecommunications System (NLETS) or LexisNexis in order to obtain aircraft registration records associated with the individuals being checked. These records will include the applicant's name, SSN, date of birth, and address. This record also includes the aircraft's registration number and various dates associated with the certification, characteristics descriptive of the aircraft and data regarding its value.

Foreign Travel Records

ACES will send inquiry files to the Customs and Border Patrol Office of Information Technology in order to obtain Private Aircraft Enforcement System (PAES) and Passenger Query History Report (PQHR) records associated with the individuals being checked.

The U. S. Customs Private Aircraft Enforcement System (PAES) will be checked to determine if the applicant has been either a passenger or traveler on a private aircraft traveling to a foreign country. This collection will include the applicant's name, SSN, date of birth, travel documentation (passport, Visa) data, and information regarding flights to include departure, arrival and destination information.

The U. S. Customs Passenger Query History Report (PQHR), a module of the Treasury Enforcement Communications System (TECS), will be checked to see if the applicant has taken flights to

foreign countries aboard commercial aircraft. This report will be checked and information from it will include the applicant's name, SSN, DOB, travel documentation (passport, Visa) data, flight information and departure and arrival location information. This information will be used for to identify new issues of personnel security concern.

Criminal History and Wanted Persons Records

ACES will send inquiry files to the National Crime Information Center (NCIC) system in order to obtain criminal history and other records associated with the individuals being checked. The Federal Bureau of Investigation (FBI) and National Crime Information Center (NCIC) files will be checked to see if applicant has a criminal history, is a wanted person, or has a record on various FBI and/or NCIC lists.

The NCIC files will be checked for criminal activity, and include checks against the Wanted Persons, Foreign Fugitive, Deported Felon, persons on Supervised Release, and convicted Sex Offender lists. This information will include information on the originating agency, the person's name, SSN, sex, race, date of birth, and date of emancipation if applicable. Data descriptive of the person's physical characteristics, operator and motor vehicle license data, and a description of the vehicle are also included. Information specific to the offense or charge is also included. Sex offender records will also include information on the victim and the offender's address and telephone number.

The NCIC files will be checked to see if the applicant has an association with a violent gang or terrorist organization. This information will include the gang or organization name, points of contact, identifying tattoos, dress, hand signals, graffiti, and other descriptive data.

The NCIC files will also be checked to see if the applicant has a Missing Person record or is the subject of a protection order. This information will include information on the originating agency, the person's name, SSN, sex, race, date and place of birth, and date of emancipation if applicable. Data descriptive of the person's physical characteristics, operator and motor vehicle license data, and a description of the vehicle are also included. Missing person records will include data more specific to identification and the protective order record will include data specific to the circumstances of the protection.

Criminal history records from FBI and or state criminal history repositories will be checked to identify criminal history records. This information will include names, sex, race, date of birth, height, weight and other personal descriptors, SSN, arresting agency, arrest date, case number, description of charges, and disposition.

ACES will use this information to identify any new issues of personnel security concern. Any new issues identified from the NCIC records will be summarized on the ACES Summary Report. The ACES Summary report along with complete copies of the underlying NCIC records will be provided to DHS at the completion of the ACES check.

Fraud Detection Records

ACES will send an inquiry file to another PERSEREC system which will send a file to Trans Union and Equifax to obtain fraud detection records associated with the individuals being checked. This

information will provide fraud detection scores derived from checking the veracity of the name, address, SSN, date of birth, and telephone number the applicant provided.

Financial Records

ACES will send an inquiry file to the Department of Treasury to obtain financial records associated with the individuals being checked. Financial records from the Department of the Treasury will be obtained. ACES will use this information to flag the individual for new issues of personnel security concern. Any new issues identified from the financial records will be summarized on the ACES Summary Report. The ACES Summary report along with copies of the underlying financial records will be provided to DHS at the completion of the ACES check.

National and International Terrorists and Denied Persons

ACES will search the national and international terrorist and denied person data outlined in Section 1.2 that is maintained by PERESEREC. For the purposes of this document, "denied person" includes individuals who have been banned from receiving U.S. exports by the U.S Department of Commerce; those who have been barred from trade transactions by the U.S Department of State, Directorate of Trade Controls; Office of Foreign Assets Controls lists of individuals who pose a threat to the interests and security of the U.S.; and individuals on international sanctions programs lists relating to the suppression of terrorism, money laundering and international drug trafficking. Information on these records include the subject's name, the matching terrorist or denied person's name, and a score of how well the names matched. If available, the individual's address, phone number, title, and position will be collected as well as the date the record was inserted into the terrorist/denied person list. The source of the list and information on affiliations and sanction programs will be included if available.

Citizenship and Immigration Records

ACES will send an inquiry file to Customs and Border Patrol (CBP) Office of Information Technology to obtain Form I-94 records associated with individuals being checked. Form I-94 records contain information provided by nonimmigrant visitors to the U. S. who have completed an Arrival-Departure Record (Form I-94). Data returned from the Form I-94 match will include applicant's name, date of birth, gender, citizenship, passport, and visa information. The Form I-94 match will also include the address while in the U. S. and the mode of travel and information regarding the trip.

ACES will send an inquiry file to another PERSEREC system that will send an inquiry to the U.S. Citizenship and Immigration Services Systematic Alien Verification for Entitlements (SAVE) program. The information returned from the verification of citizenship status will include the alien identification number, applicant's name, date and country of birth, arrival and departure record numbers and current non-resident status.

Social Security Administration

ACES will send an inquiry file to another PERSEREC system that will send an inquiry to the Social Security Administration (SSA). SSA will return a verification code regarding the individual's name and

SSN.

1.2 From whom is information collected?

DHS collects information directly from the individuals applying for a security clearance and receives a CAF Notification Report and an ACES Summary Report for each DHS Component from the DoD.

DoD PERSEREC receives the information from the DHS Office of Security in the form of a delimited data file over the OPM Secure Portal. PERSEREC sends the information out to various data sources listed below, and receives a response based on the information sent.

The data sources presently checked by ACES are:

1. Experian (credit report)
2. Equifax (credit report)
3. Trans Union (credit report)
4. Defense Security Service (DSS) Case Control Management System records (i.e., Defense Central Index of Investigations, SF86 personnel security questionnaires archived in an electronic format (EPSQ) by DSS, and archived credit reports)
5. Real Estate Ownership (Assessor/Recorder) records
6. FBI's National Crime Information Center records (Interstate Identification Index for criminal history)
7. Treasury Financial databases
8. Custom's Private Aircraft Enforcement System (Private Aircraft Foreign Travel)
9. Custom's Primary Query History System (Commercial Foreign Travel) (TECS)
10. DoD Civilian Pay File
11. DoD Civilian Personnel Transaction File
12. DoD Civilian Personnel Master File
13. DoD Enlisted Pay File
14. DoD Officer Pay File
15. Reserve Pay File
16. Reserve Personnel File
17. OPM Pay File
18. DoD Military Drug Test File
19. DoD Prior Military Service File
20. Lexis-Nexis Motor Vehicle Registrations
21. Lexis-Nexis State Boat Registrations

22. JPAS (person and clearance information)
23. DoD Enlisted Loss File
24. DoD Officer Loss File
25. National Law Enforcement Telecommunications System (NLETS) (criminal history)
26. Treasury Denied Persons List (DPL); Canadian Office of the Superintendent of Financial Institutions List of Names Subject to Terrorist Suppression Regulations; Bank of England Consolidated List; Office of Foreign Assets Control, US Treasury; and the Bureau of Industry and Security Denied Persons List.
27. Land Border Crossings
28. Form I-94 non-immigrant entry/departure records
29. DOJ Wanted Person File, Foreign Fugitive File, Missing Person File, Violent Gang and Terrorist Organization File, Protection Order File, Deported Felon File, Convicted Sexual Offender Registry File, Convicted Person on Supervised Release File, U.S. Secret Service Protective File (NCIC)
30. DHS/US Citizenship and Immigration Services Systematic Alien Verification for Entitlements (SAVE) (immigration status of non-citizens and naturalized US citizens)
31. e-QIP (SF86 record)
32. DHS person, category, eligibility, investigation data
33. Some or all of the following Comprehensive Person Report records from LexisNexis Accurint:

    Also Known As (AKAs,, addresses, date of birth, DoD, Phone numbers, SSN

    Imposters (others using the same SSN as our subject)

    Properties and prior properties (assets)

    Drivers Licenses (for current address information)

    Motor vehicles and Watercrafts (assets)

    Merchant vessel registrations

    Court Records (Civil and Criminal)

    Professional Licenses (suspensions/revocations, names, addresses, employer)

    Sexual Offenses

    FAA Aircraft registrations (assets)

    Hunting and fishing licenses (for addresses)

1.3 Why is the information being collected?

Information is collected by DHS to determine the suitability or eligibility of an individual to receive or maintain a security clearance.

DoD PERSEREC collects and analyzes information pertinent to assessing whether a person applying for, or holding a national security clearance to determine if they meet the national standards for being granted that security clearance on behalf of DHS.

1.4 How is the information collected?

The Department of Homeland Security collects information from the SF86, which is submitted by the person applying for a security clearance. This information is transmitted through the OPM Secure Portal.

The DoD PERSEREC uses ACES to match the relevant personnel security records described above on the basis of name, date of birth, SSN, and/or address of the individuals undergoing the ACES personnel security checks. Those checks are performed either through electronic interfaces with the data provider or by sending the data provider the list of personal identifiers to be checked (e.g., by tape) and then manually running a batch query against the applicable files. (Note: A manual batch query is a data processing term indicating that a database administrator will issue a command to the database referencing a file that contains multiple record entries.) The files being sent out for matching by the data providers are sent electronically or manually from either PERSEREC or the Defense Manpower Data Center (DMDC) by personnel under contract to PERSEREC.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The legal authorities to gather and use the information are outlined in Executive Order (EO) 12968, EO 10450, U.S. Code 5 Part 732. The SF86 used to collect the information contains a Privacy Act "Routine Uses" section describing how the information will be used.

Section 1.2 of EO 12968 specifies:

> b. Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.
>
> d. All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

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

In order to mitigate the risk of incorrect information being attributed to an individual both DHS and PERSEREC has implemented the following technologies, policies, and procedures: 1. Once the records are received, ACES applies additional algorithms to identify potential bad matches based on personal descriptors and identifiers. The data stored in PERSEREC databases used for ACES checks are updated on a regular basis (see Section 1.1), other sources are queried at the time of the ACES check. 2. If ACES identifies potentially adverse information, ACES flags the case for an adjudicator to review. 3. DHS manually reviews the ACES CAF Notification and Summary reports. DHS trained adjudicators will review issues identified in the reports. The adjudicators may seek corroboration from other sources or the subject. Subjects undergoing ACES checks have the full due process rights specified under Section 5.2 of Executive Order 12968, including the right to: written notice, opportunity to correct errors or provide mitigating information, and appeal.

Certain databases have downloads into ACES in order to allow for: (1) a more cost effective search, as some sources charge by the inquiry; (2) improved database search, as ACES can perform a more detailed search than a provider may allow; and/or, (3) download was the only mechanism available from the source. In order to ensure actions are taken only on the most up-to-date information, these databases are updated either on a monthly or quarterly basis.

In order to mitigate the risk that a person's data may be viewed by people unauthorized to see their information, PERSEREC has the limited access of authorized employees. The ACES database is accessible by authorized Department of Defense PERSEREC employees and contractors at two locations, one site at DMDC in Seaside, CA and the other site at PERSEREC located in Monterey, CA. While the ACES data is not classified, it does contain sensitive information and all members of the PERSEREC staff with access to ACES hold Top Secret level security clearances. Upon receiving their clearances they read and sign nondisclosure agreements and receive annual security refresher briefings to update them on government security requirements and remind them of their individual security responsibilities. ACES staff members are also instructed in the control and monitoring of access to the database. Personal information is kept secure and confidential and is not discussed with, nor disclosed to, any person within or outside the ACES program other than as authorized by law and in the performance of official duties.

ACES users have role-based access to data within the system. Multiple controls are employed to prevent misuse of the data. These measures are documented in the System Security Authorization Agreement and Defense Information Systems Agency (DISA) Security Technical Information Guides referenced therein. The SSAA and its appendices also document the procedures, criteria, controls and responsibilities regarding access to ACES. All users must apply for access to the system, receive role-appropriate security awareness training and read the ACES Rules of Behavior prior to obtaining an account.

All ACES records at the DMDC and PERSEREC sites are protected from unauthorized access by systems that include external security, access control, and identification procedures. Records at the development site are stored under lock and key, in secure containers or on electronic media with intrusion safeguards. A combination of technical, administrative, and physical security controls are employed to protect ACES and its data.

Access to reports of results of data checks is restricted to personnel with a need to know the information in order to perform their official duties. ACES reports are transmitted to authorized agents of the federal government security programs, and once received by that agent become the responsibility of that agent. ACES transmits these reports using secure transfer methods and includes appropriate security and privacy notices in ACES instructions on the use and protection of these reports.

Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

DHS personnel security managers review the information generated by ACES to assist in the identification of issues of concerns relevant to granting and maintaining national security clearances for individuals. As previously noted, only sources of information with a direct nexus to one or more of the "Adjudicative Guidelines for Determining the Eligibility for Access to Classified Information," approved by the President on December 29, 2005 for making classified information access determinations is collected and analyzed by ACES.

PERSEREC uses the information to assist DHS in this process. DoD does not use this information for any other purposes.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

ACES collects raw data from various sources and analyzes that data to identify cases that appear to contain issues of security concern applicable to granting new or continued access to classified information. The data collected is subjected to a set of pre-defined Business Rules, which are developed and refined based upon direction from DHS personnel security adjudicators and policymakers in coordination with DoD PERSEREC. The business rules are used by the system to determine whether or not issues of possible security concern are present. Information describing any issues meeting those thresholds is summarized and collated with reports generated from the record checks performed. The results are furnished to adjudicators and managers with a "need to know". The managers and adjudicators are responsible for initiating any follow-up measures needed for corroborating derogatory information and identifying relevant mitigating information applicable to those incidents, as well as for making the security clearance determinations. Individuals subject to these checks have the same due process rights as they are afforded during regularly scheduled national security background investigations. ACES does not make any adverse action determinations; rather, it identifies any new information, which is a small subset of cases where human intervention and follow-up may be warranted. Data collected during the ACES process is stored in the ACES database and provided to requesting agencies in the form of ACES Summary Reports and CAF Notification Reports.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Prior to submitting the personally identifiable information of the DHS employees and contractors to receive the ACES checks, DHS will ensure:

1. All DHS contractors and employees to receive ACES checks are listed in an appropriate DHS database as either still holding a DHS security clearance or still being considered for one,

2. All DHS contractors and employees to receive ACES checks are listed in an appropriate DHS database indicating they signed a Release of Information Authorization that is still valid.

PERSEREC will initiate ACES batch runs on the DHS personnel within 30 days of receiving each list of eligible employees and contractors from DHS.

ACES matches relevant personnel security records on the basis of name, date of birth, SSN, and/or address of the individuals undergoing the ACES personnel security checks. After the records are received, ACES applies additional algorithms to identify potential bad matches based on personal descriptors and identifiers. When ACES identifies potentially adverse information, the case is flagged for human review. The information is reviewed by a skilled adjudicator who may seek corroboration from the subject or from other sources. Subjects undergoing ACES checks have the full due process rights specified under Section 5.2 of Executive Order 12968, including the right to: written notice, opportunity to correct errors or provide mitigating information, and appeal.

ACES serves as a means of filtering through personnel security relevant records and only alerting authorized personnel when possible issues of security concern are detected by the system that might warrant human review and investigative follow-up. In approximately 96% of the cases run by only ACES no issues of concern are detected (Note: this figure applies to continuing evaluation cases).

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Prior to discussing the controls it is important to highlight the risks associated with use of this type of data. Privacy risks to the individual associated with the use of information contained in ACES include: Suspension of access to classified information, Additional Investigation, and Misuse or breach of ACES. The sections below describe the risk and associated controls.

DHS identified the frequency of an investigation as a perceived risk. Under E.O. 12968, Access to Classified Information, all employees are subject to investigation by an appropriate government authority prior to and at any time during the period of access to determine whether they continue to meet the requirements for access. This investigation may include a review of files, contacting the individual's security manager, interviews of the individual and others who may know the individual, and/or records checks. Individuals are currently subject to such investigation at any time information should surface that would call into question the subject's ability to hold a national security clearance. ACES does not change these requirements and merely automates the searches.

DHS identified the appropriateness of the business rules as a risk. In order to mitigate this risk, the DHS business rules used by ACES were developed as a result of a collaborative effort between DHS and DoD. During this process, DHS and DoD reviewed the baseline set of ACES business rules and tailored the rules to meet DHS requirements. The ACES business rules are consistent with the adjudicative guidelines in use today by agencies performing background investigations. Accordingly, the greatest impact that ACES could have on an individual is comparable to that of a security incident report, self or co-worker report (reference E.O. 12968 employee reporting responsibilities). As a decision support system, ACES parallels the policies and procedures that govern access to classified information to ultimately protect individual's privacy rights. To the extent that an individual may be subject to investigation based upon information provided by ACES, the systems of records notice for ACES provides the greatest mitigation to the risk that information may be improperly obtained or inappropriately accessed or used.

Further controls on the use of information collected by ACES include the training of users on the ACES output dissemination policy, authorized use and proper handling of the ACES generated output. ACES information on a given individual will be limited to the adjudication facility who granted eligibility. This information will be assigned to a specific adjudication team which further limits the risk of unauthorized disclosure. Policies, procedures and laws that govern the personnel security background investigation process also protect the individual rights. The professionalism applied by authorized personnel involved in the security clearance investigations and adjudications process serves to further protect individual privacy rights.

DHS identified misuse or breach of the ACES system as a risk. To mitigate that risk, the ACES user roles are highly restricted and audited. ACES employs role-based access. Access to the ACES system is granted on a "need to know" basis. PERSEREC staff and contractors with access to ACES are required to complete security and data privacy training on an annual basis. Data on ACES may only be accessed by individual user account and password. Connectivity to external networks is tightly restricted to prevent the authorized transfer of ACES data outside the secure ACES network enclave. System security logs are audited on a regular basis to ensure compliance with all privacy and data security requirements.

DHS has developed ACES Pilot Test Procedures and ACES Adjudicator training and user guides to ensure that the data resulting from the statistics run is available to only those trained and vetted security specialists with a need to adjudicate a Subject's case.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system?

The ACES reports received by DHS will be stored on the OPM Secure Portal for the duration of the pilot. At the completion of the pilot, DHS will delete ACES reports from the OPM Secure Portal. ACES reports will be printed and stored in the individual's security file.

The information received by DoD will be destroyed 25 years after the date of the last action (i.e., last investigation or separation). During the ACES pilot, DHS information containing personal identifiers used by, or collected by, ACES and stored at the PERSEREC and/or DMDC site, to include the evaluation

form data, will follow the DoD 5200.2R, Chapter 10 retention policy. The DoD policy states that personnel security investigative reports resulting in an unfavorable administrative personnel action or court-martial or other investigations of significant nature due to information contained the investigation shall be destroyed 25 years after the date of the last action. Personnel security investigative reports on persons who are considered for affiliation with the Department of Defense will be destroyed after 1 year if the affiliation is not completed.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

DHS personnel security files are destroyed in accordance with legal requirements and the disposition instructions in the General Records Schedule 18 issued by the National Archives and Records Administration (NARA). DoD 5200.2R is an official DoD directive and is consistent with NARA policies.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The information must be retained for the indicated period to ensure that a complete security record exists for the length of a Subject's employment/service with DHS. Periodic reinvestigations typically involve reviewing older case information to identify patterns that point to a Subject's trustworthiness as it pertains to classified information. Also, the information is necessary to determine whether an issue that may be identified in the future has previously been reviewed and mitigated.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

The ACES Summary Report and CAF notification reports generated by ACES will be shared with the DHS Office of Security Personnel Security Division (PSD). PSD will share relevant findings with the appropriate DHS Component. The information that is received from ACES will be used to assist adjudications within the Component Security Office holding the Security Clearance for an individual. ACES information is not shared with other organizations.

4.2 For each organization, what information is shared and for what purpose?

The ACES CAF Notification and Summary reports are shared with the DHS Component Security Office holding the individual's Security Clearance in order to allow that office to make an adjudicative review and decision concerning an individual's access to classified information. The information provided

will include a description of the sources checked, and depending on the source that flags a potential issue, additional details will be provided to facilitate further research.

For example, should a NCIC check identify an arrest record, the details of that arrest would be provided to the Office of Security as part of the ACES report in order to determine whether this arrest has an impact on the individual's ability to access classified information.

The Adjudicator will review the ACES information to determine if prior investigations had identified the issue(s), or if the new issue(s) identified has merit. The Adjudicator will then complete an ACES content evaluation form for each ACES case evaluated indicating the disposition of the possible security issues identified by ACES. These evaluations will be identified only by an ACES generated case number to minimize privacy impact.

4.3 How is the information transmitted or disclosed?

Information is exchanged between DHS and DHS Components via a secure portal maintained by the Office of Personnel Management (OPM) for the purpose of exchanging sensitive personnel security information.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The Office of Security is aware of the risks associated with unauthorized disclosure. As such, the information is released only to the authorized agents used to perform checks and is transmitted via a secure portal maintained by OPM to prevent unauthorized disclosure.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

The initial DHS collection of information initiated by the security clearance request is shared with DoD PERSEREC. Then certain information is shared by DoD PERSEREC to the following organizations:

Defense Manpower Data Center (Department of Defense), the Social Security Administration, U.S. Customs and Border Protection Office of Information Technology, U.S. Customs and Immigration Service, Department of the Treasury, Experian, Equifax, Trans Union, LexisNexis, the Federal Bureau of Investigation Criminal Justice Information Services, and State and federal law enforcement agencies that participate in the National Law Enforcement Telecommunication System. In order to obtain information from these data providers some of the individual's personal identifiers must be shared as described in Section 1.1.

PERSEREC will share the results of ACES checks on DHS personnel with the DHS Office of Security Personnel Security Division (PSD). PSD will share information with the appropriate DHS components.

5.2 What information is shared and for what purpose?

As discussed in detail in section 1.1, DHS will share information with DoD PERSEREC. PERSEREC shares information with the above listed organizations.

5.3 How is the information transmitted or disclosed?

Information is exchanged between DHS and DHS Components via a secure portal maintained by the Office of Personnel Management (OPM) for the purpose of exchanging sensitive personnel security information.

Aside from the development and production sites and the reports generated to DHS, data is shared with the systems involved in the government and commercial databases checked during the ACES process. Data sharing agreements, which were subjected to rigorous legal review, have been executed with agents representing these databases.

ACES uses Secure Sockets Layer (SSL) to encrypt personally identifiable information transmitted to commercial vendors. Recent OMB guidance (M-06-16) regarding protection of sensitive agency information relates to data that is accessed remotely or that is physically transported outside the agency's security physical perimeter (e.g., on media, laptop or PDA). Neither of these methods are used by ACES for transmission of personally identifiable information to commercial vendors.

ACES further protects data from unauthorized use by preventing external data providers from pulling data from ACES. Data transmissions for record matches with external data providers are initiated by ACES.

Commercial data providers used by ACES provide comprehensive security controls to protect sensitive personal information from unauthorized access or misuse. Such controls include providing their authorized employees with only the level of access to sensitive information needed to perform their job function, use of encryption when transporting data over open networks, and background checks on all individuals who have access to sensitive information. Commercial data providers may store some of the personal identifiers provided by ACES for a limited period of time for billing and auditing purposes only

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

DHS has an interagency agreement with DoD to perform the ACES pilot.

PERSEREC maintains Memorandum of Understandings (MOUs), contracts or user agreements with all of the data providers used by ACES. Each data provider has been contacted to determine whether modifications or amendments of these agreements are required in order to use their data for purposes of the DHS pilot evaluation. When required the MOUs, contracts or agreements have been modified or

amended in a manner that permits ACES to conduct checks on DHS personnel in addition to DoD personnel. In addition, a Statement of Work issued by DHS to DoD for the ACES DHS pilot study was issued that specifies the project's scope of work to be performed, the DHS furnished information, the place of performance, and security requirements.

5.5 How is the shared information secured by the recipient?

The information is transmitted between DoD PERSEREC and the previously mentioned organizations in an encrypted fashion and the system used to perform the checks restricts access to only authorized users who have been fully vetted.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

The results of the checks are not shared externally to DoD PERSEREC and DHS, and as such there is no external user community to train. Training for the internal specialists is described in Sections 2.4 and 5.7.

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

ACES only provides commercial providers with the personal identifiers required to conduct the match and no additional information about an individual. In many cases, the information ACES provides is data that the commercial vendor already has on file for an individual. ACES further protects the privacy of the individual by requiring that the credit bureaus post a "soft inquiry." A "soft inquiry" will only appear on the credit report if it is accessed by ACES or by the individual. If a third party (e.g., a credit card company, bank, employer) pulls the credit report, the ACES inquiry will not appear, nor will it be used to calculate the individual's credit score. In this way, the individual's credit rating is protected and the individual's employment and the fact that they were the subject of a national security investigation is not compromised.

The results of the checks are provided to DHS by the DoD PERSEREC ACES team and are not distributed externally. The information is reviewed internally at DHS by trained security specialists. Additionally, further controls on the use of information collected by ACES include the training of users on the ACES output dissemination policy, authorized use and proper handling of the ACES generated output. This information will be assigned to a specific adjudication team which further limits the risk of unauthorized disclosure. Policies and procedures and laws that govern the personnel security background investigation process also protect the individual rights

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Information related to the collection of information is provided on the SF86 completed by each Subject and provided to DHS for review. That information is provided as an Appendix. The Systems of Records Notice DHS Office of Security 001 (71 FR 53700) serves as a form of notice and this SORN is included in the Appendix.

The DoD SORN DHRA 02, PERSERC Research Files (November 29, 2002, 67 FR 69205 covers present and former DoD civilian employees, military members, and DoD contractor employees who have had or applied for security clearances.

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

Individuals submitting information to DHS have a right to decline to provide their information to the DHS Office of Security. If this information is declined, then the individual can not be cleared for a position that requires a security clearance.

As previously noted, ACES itself takes no adverse action against the subject's access or eligibility. When the system flags information pertaining to the subject of an ACES check that could lead to an adverse action (e.g., a warning, a reprimand, counseling, denial or revocation of security clearance, etc.) information will be corroborated with the subject and/or the provider of the source records (e.g. lender, police department, etc.) prior to taking any adverse action. Subjects undergoing ACES checks have the full due process rights specified under Section 5.2 of Executive Order 12968, including the right to: written notice, opportunity to correct errors or provide mitigating information, and appeal.

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

By signing the Authorization for Release of Information, the individuals consent to the use of the information. ACES checks are only conducted on people who have signed an Authorization for Release of Information that is still valid at the time the record checks are performed. Signing the release and both seeking and maintaining national security clearances are voluntary acts. However, being granted and allowed to keep a national security clearance does require the individual to adhere to certain standards of conduct specified in EO 12968 and the thirteen adjudication guidelines prescribed by the President for making classified information access determinations.

ACES checks help agency heads meet their EO 12968 continuing evaluation requirements for contractors and civilian employees working for their organization.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

DHS has published a Systems of Records Notice (SORN), this PIA, and DoD has published a SORN to cover these activities, and ACES checks are only performed on individuals who have signed an SF86 Authorization for Release of Information and whose release is still valid at the time the record checks are performed. In addition, prior to submitting the personal identifiers of the DHS employees and contractors to receive the ACES checks, DHS will prepare and distribute an announcement to participating DHS Component Security Officers. The announcement will outline the purpose of the ACES pilot project and will recommend distribution to the affected community.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Each Subject has the ability to address and provide mitigating information related to any derogatory information that is identified as part of his/her background investigation. Subjects are notified of any pending actions based on derogatory information and are provided a mechanism to provide information. If a derogatory finding is made, they have appeal rights, and also the ability to request information regarding their case via the DHS Freedom of Information Act (FOIA) office.

7.2 What are the procedures for correcting erroneous information?

The specific procedures depend on the findings and the type of case. Subjects are notified in writing when DHS is prepared to make a derogatory finding based on the information at hand. The written notice advises the Subject of the mechanism for addressing the derogatory information. To correct erroneous information in DoD PERSEREC, an individual would need to contact the original information source provider. This information is included in the notices to the subject.

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

The specific procedures depend on the findings and the type of case. Subjects are notified in writing when DHS is prepared to make a derogatory finding based on the information at hand. The written notice advises the Subject of the mechanism for addressing the derogatory information. The individual will

be notified based on a review of their response whether the derogatory information will be result in a change to their clearance status. If their clearance is suspended or revoked, they will be notified in writing and be provided with the specific information regarding their appeal rights and due process.

7.4 If no redress is provided, are alternatives available?

Redress is provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The Subject is provided with procedural rights and is provided with the opportunity to provide mitigating information that becomes part of their security file and is used to make a determination regarding their ability to have access to classified information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

DHS security managers and adjudicators will have access to the ACES reports. PERSEREC will transmit the ACES reports to the DHS Office of Security Personnel Security Division (PSD) via the OPM Secure Portal. DHS PSD will distribute the ACES reports to the appropriate Component Personnel Security Officer via the OPM Secure Portal. The Component Personnel Security Officer will log into the OPM Secure Portal to access their ACES reports.

PERSEREC user groups include system administrators, database administrators, operations staff, data analysts, program managers, and software engineers as required for performance of their assigned duties on ACES.

8.2 Will contractors to DHS have access to the system?

Yes, certain Northrop Grumman contractors working on-site at PERSEREC and/or DMDC will have access to the system. Each PERSEREC contractor having access is required to meet the same personnel security and "need to know" standards required of the government personnel. DHS contractors who provide support to the Office of Security will have access to ACES reports. DHS contractors having access to ACES reports are required to meet the same personnel security and "need to know" standards required of the government personnel.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, ACES user access is restricted in the form of Mandatory Access Controls assigned based on the user's role. Users cannot assign their roles to any other user, nor can they elevate their own rights within the system. User access is enforced with the ACES System Security Authorization Agreement procedures referenced in section 1.6. Roles are assigned only after supervisor request, process owner approval, and appropriate security checks have been verified.

PERSEREC will transmit the ACES reports to the DHS Office of Security PSD via the OPM Secure Portal. PSD will then distribute the ACES reports to the appropriate Component Personnel Security Officer via the OPM Secure Portal. The Component Personnel Security Officer will log into the OPM Secure Portal to access their ACES reports.

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

Before being granted access to any ACES resources, a request must be submitted by the user's first line or higher-level supervisor. Further, such requests is subsequently must be approved by the ACES Program Management Office (PMO). The request is submitted using the System Authorization Access Request (SAAR) form. Approval of the request requires that the user sign the SAAR form acknowledging they have read and will abide by the ACES Rules of Behavior. Verification of the user's background investigation and security clearance is also captured for the SAAR approval. The procedures are documented in the SSAA: Appendix J, Rules of Behavior and Appendix M, Personnel and Technical Security Controls.

Prior to submitting the personal identifiers of the DHS employees and contractors to receive the ACES checks, DHS will ensure:

1. All DHS contractors and employees to receive ACES checks are listed in an appropriate DHS database as either still holding a DHS security clearance or still being considered for one,

2. All DHS contractors and employees to receive ACES checks are listed in an appropriate DHS database indicating they signed a Release of Information Authorization that is still be valid.

The ACES reports will be subject to the existing personnel security policies and procedures in place at the DHS location.

DHS adjudicators assigned to the ACES pilot conduct business in a physically secured area, hold at a minimum a SECRET clearance with a Minimum Background Investigation (MBI), and attend training on: DHS records management, safeguarding of classified national security information and Sensitive but Unclassified Information, and ACES Pilot Test Training (includes an ACES Security Awareness Training component). In addition, PERSEREC has developed an ACES Output Dissemination Policy that provides guidance on the specific handling requirements for ACES data.

Active personnel security clearance paperwork (paper based files) are stored in a secured area at all times. Closed personnel security files are stored in a controlled file room. Electronic personnel security records are stored in a DHS approved system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The ACES PMO verifies the appropriate level of access for a user when the SAAR form is received. System and database administrators are responsible for verifying the adequacy and authenticity of the account request (new account or modification to an existing account) before creation or modification of an account. Users are assigned a unique personal identifier (user ID) and set of privileges. The user ID is used for auditing individual activities on the systems.

DHS defines the business rules used for analysis of the DHS data set. PERSEREC will implement the business rules in ACES.

DHS Personnel Security Managers are responsible for distributing ACES reports to trained ACES Adjudicators.

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

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is a process whereby DoD ensures the security of its computer networks. Operating under DoD Instruction 5200.40 of December 30, 1997, DITSCAP provides instruction on the certification and accreditation of DoD information technology. It is the standard process for identifying information security requirements, providing security solutions, and managing information system security activities. In November 2005 PERSEREC received interim approval from DITSCAP to operate ACES at DMDC.

As part of the pilot process, DHS adjudicators will be trained on how to review ACES cases and to interpret output. In addition the training will cover the security policies and restrictions on dissemination of report information. DoD will provide statistical reports to the DHS Office of Security on the DHS data set and the effectiveness of the rules. DoD will transmit these reports to DHS via the OPM Secure Portal.

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

The system is planned to be operational at only one site at any time. Consistent use of the system and data is maintained at all sites through use of operator's manuals, checklists, and other documented procedures.

All government and contractor personnel at PERSEREC are required to receive annual Privacy training. Information Assurance training is also provided on an annual basis.

PERSEREC will provide DHS with training material that addresses the proper use, storage, and dissemination of the ACES reports.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The applicable Certification and Accreditation (C&A) requirement for DoD systems is the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The system was certified on October 24, 2005 for interim authority to operate. Full authority to operate was granted on October 26, 2006.

DHS will maintain ACES reports in accordance with DHS policies and procedures governing personnel security information.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The privacy risks identified for the system include potential risks during data collection and transmission, data storage, and data usage.

Potential privacy risks to DoD PERSEREC during data collection and transmission were mitigated by the following:

- Using a highly segmented network architecture that isolates all segments that receive inputs from external sources,
- Data transmissions are encrypted both on the external connection as well as for transmission across the internal network, and
- All data extracted from government or commercial resources is deleted from the site's collection servers and workstations once the data is properly posted to the secure Oracle database.

Potential privacy risks for DoD PERSEREC during data storage were mitigated by the following:

- The Oracle database that aggregates the collections of data is isolated on its own secure network segment to provide a higher degree of protection, and
- The procurement of encryption software to provide for encryption of system backup tapes.

Potential privacy risks for DoD PERSEREC during data usage were mitigated by the following:

- Privacy Act Data Responsibilities as defined in the Rules of Behavior document; system users are required to read and sign that they will abide by these rules, and

- Definition and distribution of the ACES Output Dissemination Policy that defines the various types of ACES reports and underlying data sources, along with the applicable legislation that determines the rules for dissemination of the information.

Potential Privacy Risks for DHS for the handling of ACES reports are mitigated by the following:

- The OPM Secure Portal for the transmission and storage of DHS ACES reports.
- Training of DHS personnel on the handling of ACES information and reports.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

ACES was built from the ground up, however, it does utilize commercial off-the-shelf (COTS) fuzzy logic matching and address standardization software. The system also utilizes a COTS database server, application server, network intrusion detection, operating system, firewall, backup, and change management application software.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is a process whereby DoD ensures the security of its computer networks. Operating under DoD Instruction 5200.40 of December 30, 1997, DITSCAP provides instruction on the certification and accreditation of DoD information technology. It is the standard process for identifying information security requirements, providing security solutions, and managing information system security activities. In November 2005 PERSEREC received interim approval from DISTCAP to operate ACES.

DHS worked with DoD officials regarding the data sources and processes involved with ACES.

In addition to having a clear nexus with security clearance adjudication criteria, other factors used in determining which commercial data sources and vendors to utilize in ACES were data accuracy and coverage.

The commercial computer operating system and database selected for ACES were also chosen in part because of the security and audit functions that were included.

9.3 What design choices were made to enhance privacy?

A highly segmented network architecture was chosen to isolate interface functions (data collection and distribution) from data storage and processing functions. A multiple port firewall is used for this purpose along with the creation of a DMZ segment for external connectivity purposes. Internal network traffic is required to cross the firewall and this provides much flexibility in defining access control lists (ACLs) to

restrict the type of allowed traffic by various criteria such as IP address, port, and protocol. So a user or process operating on one network segment cannot gain access to other network segments unless this access is specifically defined by an ACL on the firewall. Use of host-based intrusion detection software on the servers and workstations, along with use of a network intrusion detection device allow for monitoring of suspicious activity or attacks on the system that could compromise privacy of the data.

DHS will store the ACES Notification and Summary reports on the OPM Secure Portal. ACES information extracted from any report will be maintained in accordance with DHS policies and procedures governing personnel security information.

Conclusion

DoD developed ACES with a focus on ensuring the privacy of individuals who are evaluated for a personnel security clearance. The system contains security and procedural controls to ensure that data is made available to only those with a legitimate need as defined by the underlying legal authorities. During this pilot to test DHS use of ACES, DHS is committed to maintaining this focus on privacy.

Responsible Officials

Ken Zawodny

Chief, Personnel Security Division, Office of Security

Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security