

COMPUTER MATCHING AGREEMENT
BETWEEN
THE DEPARTMENT OF HOMELAND SECURITY, UNITED STATES
CITIZENSHIP AND IMMIGRATION SERVICES (DHS-USCIS)
AND
THE MASSACHUSETTS DIVISION OF UNEMPLOYMENT ASSISTANCE

PART I: GENERAL TERMS AND CONDITIONS

A. PURPOSE AND DESCRIPTION

This memorandum constitutes an agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and the Massachusetts Division of Unemployment Assistance (MA-DUA). The purpose of this agreement is to provide the MA-DUA with electronic access to immigration status information contained within DHS-USCIS' Verification Information System (VIS) that will enable the MA-DUA to determine whether an applicant is eligible for benefits under the Unemployment Compensation (UC) program administered by the MA-DUA.

This agreement describes the respective responsibilities of DHS-USCIS and the MA-DUA for verifying immigration status, and preserving the confidentiality of and safeguarding information received from the other party pursuant to verification procedures. The requirements of this Agreement will be carried out by authorized employees and/or contractor personnel of DHS-USCIS and the MA-DUA.

B. FUNCTIONS TO BE PERFORMED

DHS-USCIS agrees to make available and maintain, as part of the Verification Division, Systematic Alien Verification for Entitlements (SAVE) Program, an immigration status verification system, which provides information on aliens' immigration status.

DHS-USCIS agrees to provide MA-DUA through the automated system the following information on each alien inquiry as appropriate: DHS-USCIS generated verification number, last name, first name, date of birth, country of birth, date of entry, immigration status data, and in some cases, certain other biographical data that may relate to the alien number or work authorization.

DHS-USCIS agrees to provide to the MA-DUA with instructional materials required for the use of DHS-USCIS verification system; a sufficient number of primary verification user codes to assure the effective implementation of the verification procedures; and instructions for obtaining necessary system access codes.

DHS-USCIS agrees to provide assistance to the MA-DUA on policies and procedures for use of the system including technical instructions for access to the system, requirements for safeguarding information contained in the system, and restrictions on disclosure of system information. DHS-USCIS also agrees to provide the MA-DUA with the name, address and telephone number of an appropriate point of contact (POC) within DHS-USCIS, or its contractor organization, who can be contacted regarding any billing questions or problems which arise in connection with the MA-DUA's participation in the verification program.

The MA-DUA agrees to provide the alien number of the applicant seeking a benefit from the MA-DUA for the purposes of primary (automated access) verification. If an alien's records are not initially located as a result of primary verification, DHS-USCIS will send a message seeking additional verification data from the MA-DUA. The additional/secondary verification process requires the agency to submit a copy of the applicant's immigration documentation along with a Document Verification Form G-845 or provide an electronic description of the applicant's immigration document which may further assist an Immigration Status Verifier in checking all necessary indices and DHS files before providing the MA-DUA with immigration status information. This data may include the type of document presented by the applicant to the MA-DUA, the expiration date of the document, document description, last name, first name, middle name, and/or also known as, a.k.a, of the applicant, applicant's date of birth, I-94 (DHS arrival/departure document), applicant's employment history data, MA-DUA case number and/or other special comments.

The MA-DUA agrees to provide a liaison with the DHS-USCIS to resolve any questions regarding this Agreement and to provide assistance to DHS-USCIS to facilitate the provision of accurate immigration status verification information.

C. SAFEGUARDS REGARDING THE USE AND DISCLOSURE OF INQUIRY DATA

The VIS shall be used in a manner that protects the individual's privacy to the maximum degree possible, and shall not be used in a manner that will allow for discrimination based on race, color, creed, national origin, sex, or disability.

The parties agree to comply with applicable Privacy Act (5 U.S.C. 552a, *et. seq.*) restrictions and requirements in the conduct of the verification procedures under the agreement, as well as, in the safeguarding, maintenance and disposition of any information received under this Agreement. The MA-DUA also agrees to the maximum extent practicable to extend the protections of the Privacy Act to non US citizens and/or non Lawful Permanent Residents (LPRs). The MA-DUA also agrees to comply with any additional requirements that may be imposed by other applicable Federal benefit program

regulations.

The MA-DUA agrees not to delay, deny, reduce or terminate applicant/recipient's UC benefits because of that individual's immigration status based solely on a response received from DHS-USCIS Verification Division's primary (automated) system or based upon any additional verification check that may be pending. No adverse action shall be taken unless the MA-DUA has received a response from the DHS-USCIS Verification Division that "additional verification" procedures were conducted and indicate that the applicant/recipient does not have the type of immigration status that makes him or her eligible for the benefit and the individual has been afforded the opportunity to refute any adverse information as provided in PART II of this Agreement.

DHS-USCIS reserves the right to use information received by it from the User Agency for any purpose permitted by law, including but not limited to the prosecution of violations of Federal criminal law.

DHS-USCIS may terminate this MOU without prior notice if deemed necessary because of a requirement of law or policy, upon a determination by DHS-USCIS that there has been a breach of system integrity or security by the User Agency, or a failure by the User Agency to comply with established procedures or legal requirements.

The MA-DUA agrees to immediately notify the SAVE Program whenever there is cause to believe an information breach has occurred as a result of User Agency action or inaction pursuant to Office of Management and Budget (OMB) Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," which concerns safeguarding and responding to the breach of personally identifiable information.

Nothing in this MOU is intended, or should be construed, to create any right or benefit, substantive or procedural, enforceable at law by any third party against the United States, its agencies, officers, or employees.

PART II: COMPUTER MATCHING ACT REQUIREMENTS

INTRODUCTION

The purpose of this section of the agreement is to comply with the Computer Matching and Privacy Protection Act of 1988 (CMPPA), Public Law 100-503, 102 Stat. 2507 (1988), which was enacted as an amendment to the Privacy Act of 1974 (5 U.S.C. 552a, et. seq.). The requirements of this Section pertain only to alien applicants for, or recipients of, benefits administered by the MA-DUA who have been accorded lawful permanent resident status by DHS-USCIS and to United States citizens whose records are

included in VIS, Section II below. Pursuant to the Department of Homeland Security's (DHS) Privacy Policy Guidance Memorandum 2007-1, to the extent practicable, privacy protections afforded to US Citizens and LPRS shall be afforded to non LPRs and non citizens.

The CMPPA applies when computerized comparisons of Privacy Act protected records contained within a Federal agency's databases and the records of another organization are made in order to determine an individual's eligibility to receive a Federal benefit. The CMPPA requires the parties participating in a matching program to execute a written agreement specifying the terms and conditions under which the matching program will be conducted.

DHS-USCIS has determined that the status verification checks to be conducted by the MA-DUA using the VIS database is a "computer matching program" as defined in the CMPPA.

A. TITLE OF MATCHING PROGRAM

The title of this matching program as it will be reported by the Department of Homeland Security and the Office of Management and Budget is as follows: Verification Division DHS-USCIS/MA-DUA.

B. MATCHING AGENCIES

- I. Source Agency: Department of Homeland Security, United States
Citizenship and Immigration Services
- Recipient Agency: Massachusetts Division of Unemployment Assistance

C. PURPOSE AND LEGAL AUTHORITIES

Section 121 of the Immigration Reform and Control Act (IRCA) of 1986, Public Law 99-603, as amended by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), Public Law 104-193, 110 Stat. 2168 (1996), requires DHS to establish a system for the verification of immigration status of alien applicants for, or recipients of, certain types of benefits as specified within IRCA, and to make this system available to state agencies that administer such benefits. Section 121(c) of IRCA, amends Section 1137 of the Social Security Act and certain other sections of law that pertain to Federal entitlement benefit programs and requires state agencies administering these programs to use DHS-USCIS' verification system in making eligibility determinations in order to prevent the issuance of benefits to those alien applicants who are not entitled to program benefits because of their immigration status. The VIS database is the DHS-USCIS system which has been established and made available to the MA-DUA and other

covered agencies for use in making these eligibility determinations

The MA-DUA seeks access to the information contained in DHS-USCIS' VIS database, for the purpose of confirming the immigration status of alien applicants for, or recipients of, benefits it administers, in order to discharge its obligation to conduct such verifications pursuant to Section 1137 of the Social Security Act (42 U.S.C. 1320b-7(a), et seq.) and to Mass. Gen. Laws ch. 151A, § 25(h).

D. JUSTIFICATION AND EXPECTED RESULTS

It has been determined by the parties that a computer matching program is the most efficient and expeditious means of obtaining and processing the information needed by the MA-DUA to verify the immigration status of alien applicants for, and recipients of, entitlement benefits. It is expected that this matching program will enable the MA-DUA to rapidly confirm the benefit eligibility of alien applicants/recipients with proper immigration status, identify those applicants who require further checks to confirm proper eligibility status and to identify and prevent improper payments to those applicants whose immigration status does not entitle them to receive the benefits administered by the MA-DUA.

It has been determined that available alternatives to the use of computer matching program for verifying immigration status would impose a much greater administrative and processing burden (i.e., be much more labor intensive), would result in higher annual administrative costs, and would protract the average query response time. The anticipated savings to be derived from the use of the electronic verification program including administrative costs and savings derived by eliminating fraudulent benefit payments is \$15,995,316 annually based on historical savings. Using a computer matching program, the MA-DUA is able to process, in an extremely expeditious manner, a higher volume of queries with reduced overall labor demands. DHS-USCIS will provide daily responses to MA-DUA batch inquiries.

Additionally, because of the rapid response capability provided by this computer matching program, this program will have a greater deterrent effect on applicants seeking to fraudulently receive entitlement benefits administered by the MA-DUA as compared to a much slower mail-in procedure. One of the major objectives of IRCA, to reduce incentives for illegal aliens to come to and remain in the United States, is furthered by this matching program's deterrent effect. Finally, this system also supports efforts to curb waste, fraud, and abuse within federally funded entitlement programs.

F. RECORDS DESCRIPTION

- I. Records to be matched:

- a. Records in the DHS-USCIS VIS database containing information related to the status of aliens and other persons on whom DHS-USCIS has a record as an applicant, petitioner, or beneficiary. See Systems of Records Notice, 72 F.R. 17569.
 - b. MA-DUA records pertaining to alien applicants for, or recipients of, entitlement benefit programs administered by the State.
2. Data elements:
- a. Data element contained within the MA-DUA's records to be matched with DHS-USCIS VIS database:
 - 1. Alien Registration Number
 - b. Data elements contained within DHS-USCIS' records to be matched with the MA-DUA data may consist of the following:
 - 1. Alien Registration Number
 - 2. Last Name
 - 3. First Name
 - 4. Date of Birth
 - 5. Country of Birth (not nationality)
 - 6. Social Security Number (if available)
 - 7. Date of Entry
 - 8. Immigration Status Data
 - 9. Employment Eligibility Data
3. Number of records: On a monthly basis, approximately 3,500 records from the MA-DUA will be matched against the DHS-USCIS' VIS database which consists of more than 110 million records.

Duration of the program: Eighteen months from the effective date of this Agreement.

F. NOTICE PROCEDURES

DHS-USCIS agrees to publish in the Federal Register a notice of this matching program as specified in the CMPPA and the Office of Management and Budget CMPPA implementing guidance.

As required by 5 U.S.C. 552(a)(1)(D), the MA-DUA will provide periodic notice to applicants for and recipients of financial assistance or payments under the Federal benefit

program(s) covered by this Agreement that any information they provide may be subject to verification through matching programs. At the time of the initial application for UI benefits the MA-DUA will provide each applicant with a booklet informing them that their eligibility status will be verified by matching against the DHS-USCIS database. Further, at the time of each weekly request for benefit payment, MA-DUA will notify all claimants that additional verification may occur. Finally, in any case where a second verification will occur, MA-DUA will notify each claimant of the need for evidence and verification with the mailing of a letter or booklet.

G. VERIFICATION PROCEDURES

1. The MA-DUA may not suspend, terminate, reduce, or make a final denial regarding the Federal benefit program eligibility of an applicant/recipient covered by this part based on that individual's immigration status, or take other adverse action against such individual as a result of information produced by the matching program until information has been independently verified. DHS-USCIS' "additional verification procedures" as described in its M-300 SAVE Users Manual, a copy of which is provided to each user upon execution of the CMA.
2. Furthermore, the MA-DUA may not suspend, terminate, reduce, or make a final denial regarding the Federal benefit program eligibility of any individual described in paragraph 1, or take other adverse action against such individual as a result of information produced by this matching program unless: (A) such individual has received notice from the MA-DUA containing a statement of the findings of the immigration status check; and (B) until the subsequent expiration of any notice period provided by such program's law or regulations, or 30 days, whichever is later. Such opportunity to contest may be satisfied by the notice, hearing, and appeal rights governing the Federal benefit program and the applicant has been provided the opportunity to refute any adverse status information as a result of the verification query. The exercise of any such rights shall not affect any rights available under this section.

H. RECORDS RELATING TO UNITED STATES CITIZENS

This Agreement authorizes the MA-DUA to use the Verification Division's system for the purposes of verifying the immigration status of alien applicants for UC benefits. Nothing in this Agreement authorizes the MA-DUA to use the DHS-USCIS system for the purposes of verifying the status of any individual claiming United States citizenship by birth. However, in addition to records relating solely to aliens, VIS contains records relating to former lawful permanent resident aliens who have become naturalized United States citizens. It is possible that applicants for UC may through fraud or error, present documentation identifying themselves as lawful permanent resident aliens, without informing the MA-DUA that they have become a United States citizen, thereby resulting

in a MA-DUA inquiry in VIS.

In the event that DHS-USCIS receives a request for a verification of MA-DUA applicant who is a LPR or United States Citizen, the request will be referred to a DHS-USCIS Immigration Status Verifier for additional verification procedures. All safeguards and protections provided by the Privacy Act, CMPPA, and this Agreement regarding the use, disclosure, and security of DHS-USCIS records apply to DHS-USCIS records regarding United States citizens to the same extent as to the DHS-USCIS records relating to lawful permanent resident aliens. Pursuant to the Department of Homeland Security's Policy, Guidance Memorandum 2007-1, to the extent practicable, privacy protections afforded to US citizens and LPRs shall be afforded to non LPRs and non citizens.

I. DISPOSITION OF MATCHED ITEMS

Records collected by DHS-USCIS in the process of establishing immigration and citizenship status or employment authorization are stored and retained in the VIS Repository for ten (10) years from the date of the completion of the verification unless the records are part of an on-going investigation in which case they may be retained until completion of the investigation. Photocopies mailed to DHS in response to a Tentative Non-Confirmation (TNC) will be maintained as long as necessary to complete the verification process, and the duration of the benefit granted.

J. SECURITY SAFEGUARDS

DHS-USCIS agrees to safeguard information it receives from the MA-DUA in connection with status verification inquiries in accordance with the Privacy Act of 1974 (5 U.S.C. 552a), the Immigration Reform and Control Act of 1986, other applicable statutes, and requirements of this agreement between the parties.

DHS-USCIS agrees to safeguard the information provided by the MA-DUA in accordance with DHS-USCIS disclosure standards and to provide the name of DHS-USCIS' program inspector responsible for compliance with these standards. Individuals who wish to obtain copies of records pertaining to themselves resulting from queries submitted to DHS-USCIS, may do so by following the Freedom of Information Act and Privacy Act procedures that can be found at www.uscis.gov. DHS-USCIS also agrees to limit access to MA-DUA provided information to individual's responsible for the verification of the alien's immigration status or who require access to the information to perform necessary support functions or follow-up actions.

The DHS-USCIS' contractor's data facility where the MA-DUA and DHS-USCIS information is stored complies with requirements of the Department of Homeland Security, National Security Systems Policy Directive 4500B. It is a secure facility accessed only by authorized individuals with properly coded key cards, authorized door

keys or access authorization. There is a security guard force on duty 24 hours a day, 7 days a week. The building is protected against unauthorized access, unauthorized use of equipment, or removal of storage media and listings. Employees at the facility have undergone background checks in order to be granted clearance and are provided access badges.

The MA-DUA agrees to safeguard information it receives from DHS-USCIS under the verification process in accordance with the requirements of the Privacy Act (5 U.S.C. 552a), and applicable Federal and State entitlement benefit program record retention and disclosure requirements.

The MA-DUA also agrees to limit access to information to those individuals responsible for the verification of the alien's immigration status or who require access to the information to perform necessary support functions. The MA-DUA will restrict further dissemination of the information unless required in connection with State or the Federal entitlement program law enforcement responsibilities.

The MA-DUA has taken measures to secure information received from DHS-USCIS for purposes of the matching program in accordance with applicable State and Federal entitlement program rules procedures. The MA-DUA's offices are located in secure buildings, and access to premises is by official identification. All records are stored in secure facilities which are maintained by the Commonwealth of Massachusetts or a government contractor, which are locked during non-duty hours. Records are stored in cabinets or machines which are also locked during non-duty office hours. Access to automated records is controlled by user identification and passwords.

The computer security systems used by both DHS-USCIS and the MA-DUA offer a high degree of resistance to tampering and circumvention. Multiple levels of security are maintained within their computer system control program. Both security systems limit access to authorized personnel strictly on a "need-to-know" basis, and control an individual user's ability to access and alter records within the system. All users are given a unique ID with personal identifiers and interactions with the system are recorded.

K. RECORDS USE, DUPLICATION AND REDISCLOSURE RESTRICTIONS

The parties agree to comply with the data maintenance and disclosure control requirements specified within Part I of this Agreement. The parties agree not to duplicate or redisclose any records received from the other party pursuant to this matching agreement, except where it is necessary to verify the immigration status of alien applicants for, or recipients of, the UC benefit programs administered by the MA-DUA (including follow-up actions). Additionally, if the matching program uncovers evidence of fraudulent claims or the use of fraudulent immigration documents, the parties may redisclose the records necessary to conduct law enforcement investigations or

prosecutions or as otherwise required by law.

L. RECORDS ACCURACY ASSESSMENT

DHS-USCIS currently estimates that information within its VIS database is 90-95% accurate in reflecting immigration status, but continues to undertake various actions to further improve the quality of the VIS database. In addition, in cases where status is not confirmed through the VIS, additional verification procedures are used, which allows DHS-USCIS to check all necessary indices and files before providing the MA-DUA with immigration status information. This process includes procedures for DHS-USCIS to correct any errors detected in the immigration status information.

M. COMPENSATION

The User Agency shall pay the standard billing rates in accordance with the terms of the reimbursement Memorandum of Agreement (MOA) addendum to the MOU and arrange the obligations, processes and methods related to the payment of required fees to DHS-USCIS and/or its authorized agents.

The current standard billing rates are attached to the MOA. The standard billing rates and methods of payment are subject to change upon prior written notification to the User Agency.

N. COMPTROLLER GENERAL ACCESS

The GAO (Comptroller General) may have access to all of the matching records of the MA-DUA and DHS-USCIS necessary to verify compliance with the requirements of the CMPPA.

O. EFFECTIVE DATE

This Agreement will be effective 40 days after a report concerning the computer matching program has been transmitted to the Office of Management and Budget (OMB) and transmitted to Congress along with a copy of the Agreement, or 30 days after publication of a computer matching notice in the Federal Register, whichever is later. The Agreement (and matching activity) will continue for 18 months from the effective date, unless within three (3) months prior to the expiration of this Agreement, the Data Integrity Board approves a one-year extension pursuant to 5 U.S.C. 552a (a) (2)(D).

P. SIGNATURES

The undersigned are officials of DHS and the MA-DUA who are authorized to represent their Agencies for purposes of this Agreement.


David Bounds
Chief
Benefits Operations
Verification Division
United States Citizenship and Immigration
Services


Edward T. Malmborg
Director
Massachusetts Division of
Unemployment Assistance

Date: 7-22-08

Date: 8-4-08

Q. DEPARTMENT OF HOMELAND SECURITY
DATA INTEGRITY BOARD APPROVAL

Approved 
Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security

Date: 1-16-09

"Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and the Massachusetts Division of Unemployment Assistance (MA-DUA)."

Based on match runs between:
Number of cases matched:

December 2004-April 2007

118,879

4.099

1. Summary of Cost Data

Monthly Avg.

DUA costs related to the match:

a. CIS Vendor Costs:	\$21,606.20	\$745.04
b. DUA S.A.V.E. Unit Personnel Costs:	\$398,817.40	\$13,752.32
c. DUA S.A.V.E. Unit Overhead & Fringe Benefit Costs:	\$112,466.39	\$3,878.15
d. DUA S.A.V.E. Technical & Administrative Service Costs:	\$265,563.79	\$9,157.37
e. DUA cost of S.A.V.E. Overpayment Recovery	\$14,434.00	\$497.72
f. Total DUA costs related to S.A.V.E. Activity	\$812,887.78	\$28,030.61

2. Summary of Benefit Data

Recovery of Overpayments:

Number of Overpayments Detected:	1995	69
a. \$ value of detected overpayments:	\$2,004,148.00	\$69,108.55
Average Amount Overpaid	\$1,004.59	
b. \$ value of recovered overpayments:	\$550,935.00	\$18,997.76
Average Amount Recovered:	\$276.16	
Recovery Rate (2 b/2.a)	27.49%	

Savings from case terminations:

Number of cases with benefits stopped:	5291	182
c. \$ value of erroneous payments stopped:	\$36,100,263.00	\$1,244,836.66
Average Amount Stopped:	\$6,822.96	

3. Benefit / Cost Ratio

Total Cost of DUA S.A.V.E. Activity (1g):	\$812,887.78	\$28,030.61
\$ Value of Benefits from S.A.V.E. (2a+2b+2c):	\$38,655,346.00	\$1,332,942.97
Benefit / Cost Ratio:	47.55 to 1	

COMPUTER MATCHING AGREEMENT
BETWEEN
THE UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES
AND
THE NEW JERSEY DEPARTMENT OF LABOR & WORKFORCE
DEVELOPMENT

Part 1: GENERAL TERMS AND CONDITIONS

A. PURPOSE AND DESCRIPTION

This memorandum constitutes an agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and the New Jersey Department of Labor & Workforce Development (NJLWD). The purpose of this Agreement is to provide the NJLWD with electronic access to immigration status information contained within the DHS-USCIS' Verification Information System (VIS) that will enable the NJLWD to determine whether an applicant is eligible for benefits under the Unemployment Compensation (UC) program administered by the NJLWD.

This Agreement describes the respective responsibilities of DHS-USCIS and the NJLWD for verifying immigration status, and preserving the confidentiality of and safeguarding of, information received from the other party pursuant to the verification procedures. The requirements of this Agreement will be carried out by authorized employees and/or contractor personnel of DHS-USCIS and the NJLWD.

B. FUNCTIONS TO BE PERFORMED

DHS-USCIS agrees to make available and maintain, as part of the Verification Division, Systematic Alien Verification for Entitlements (SAVE) Program, an immigration status verification system, which provides information on aliens' immigration status.

DHS-USCIS agrees to provide NJLWD through the automated system the following information on each alien inquiry as appropriate: DHS-USCIS generated verification number, last name, first name, date of birth, country of birth, date of entry, immigration status data, and, in some cases, certain other biographical data that may relate to the alien number or work authorization.

DHS-USCIS agrees to provide NJLWD with instructional materials required for the use of the DHS-USCIS verification system, a sufficient number of primary verification user codes to assure the effective implementation of the verification procedures, and instructions for obtaining necessary system access codes.

DHS-USCIS agrees to provide staff assistance to the NJLWD on policies and procedures for use of the system including technical instructions for accessing the system,

requirements for safeguarding information contained in the system, and restrictions on disclosure of system information. DHS-USCIS also agrees to provide the NJLWD with the name, address and telephone number of an appropriate point of contact (POC) within DHS-USCIS, or its contractor organization, who can be contacted regarding any billing questions or problems which arise in connection with the NJLWD's participation in the verification program.

The NJLWD agrees to provide the alien number of the applicant seeking a benefit from the NJLWD for the purposes of primary (automated access) verification. If an alien's records are not initially located as a result of primary verification, DHS-USCIS will send a message seeking additional verification data from the NJLWD. The additional/secondary verification process requires the agency to submit a copy of the applicant's immigration documentation along with a Document Verification Form G-845 or provide an electronic description of the applicant's immigration document which may further assist an Immigration Status Verifier in checking all necessary indices and DHS files before providing the NJLWD with immigration status information. This data may include the type of document presented by the applicant to the NJLWD, the expiration date of the document, document description, last name, first name, middle name, and or also known as a/k/a of the applicant, applicant's date of birth, I-94 (DHS arrival/departure document), applicant's employment history data, NJLWD case number and/or other special comments.

The NJLWD agrees to provide a liaison with DHS-USCIS to resolve any questions regarding this Agreement and to provide assistance to DHS-USCIS to facilitate the provision of accurate immigration status verification information.

C. SAFEGUARDS REGARDING THE USE AND DISCLOSURE OF INQUIRY DATA

The VIS database shall be used in a manner that protects the individual's privacy to the maximum degree possible, and shall not be used in a manner that will allow for discrimination based on race, color, creed, national origin, sex, or disability.

The parties agree to comply with applicable Privacy Act (5. U.S.C. 552a, (et. seq.) restrictions and requirements in the conduct of the verification procedures under the Agreement, as well as, in the safeguarding, maintenance, and disposition of any information received under this Agreement. The NJLWD also agrees to the maximum extent practicable to extend the protections of the Privacy Act to non US citizens and/or non Lawful Permanent Residents (LPRs). The NJLWD also agrees to comply with any additional requirements that may be imposed by other Federal benefit program regulations.

The NJLWD agrees not to delay, deny, reduce, or terminate an alien applicant/recipient's UC benefits because of that individual's immigration status based solely on a response received from DHS-USCIS Verification Division's primary (automated) system or based upon any additional verification check that may be pending. No such adverse action shall be taken unless the NJLWD has received a response from the DHS-USCIS Verification Division that "additional verification" procedures were conducted and indicate the

applicant/recipient does not have the type of immigration status that makes him or her eligible for the benefit and the individual has been afforded the opportunity to refute any adverse information as provided in Part II of this Agreement.

DHS-USCIS reserves the right to use information received by it from the User Agency for any purpose permitted by law, including but not limited to the prosecution of violations of Federal criminal law.

DHS-USCIS may terminate this MOU without prior notice if deemed necessary because of a requirement of law or policy, upon a determination by DHS-USCIS that there has been a breach of system integrity or security by the User Agency, or a failure by the User Agency to comply with established procedures or legal requirements.

The NJLWD agrees to immediately notify the SAVE Program whenever there is cause to believe an information breach has occurred as a result of User Agency action or inaction pursuant to Office of Management and Budget (OMB) Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," which concerns safeguarding and responding to the breach of personally identifiable information.

Nothing in this MOU is intended, or should be construed, to create any right or benefit, substantive or procedural, enforceable at law by any third party against the United States, its agencies, officers, or employees.

PART II: COMPUTER MATCHING ACT REQUIREMENTS **STATES CITIZENS**

INTRODUCTION

The purpose of this section of the agreement is to comply with the Computer Matching and Privacy Protection Act of 1988 (CMPPA), Public Law 100-503, 102 Stat. 2507 (1988), which was enacted as an amendment to the Privacy Act of 1974 (5 U.S.C. 552a, et seq.). The requirements of this Section pertain only to alien applicants for, or recipients of, benefits administered by the NJLWD who have been accorded lawful permanent resident status by DHS-USCIS and to United States citizens whose records are included in VIS as described in Section H below. Pursuant to the Department of Homeland Security's (DHS) Privacy Policy Guidance Memorandum 2007-1, to the extent practicable, privacy protections afforded to US Citizens and LPRS shall be afforded to non LPRs and non citizens.

The CMPPA applies when computerized comparisons of Privacy Act records contained within a Federal agency's databases and the records of another organization are made in order to determine an individual's eligibility to receive a Federal benefit. The CMPPA requires the parties participating in a matching program to execute a written agreement

specifying the terms and conditions under which the matching agreement will be conducted

DHS-USCIS has determined that the status verification checks to be conducted by the NJLWD using the VIS database is a "computer matching program" as defined in the CMPPA.

A. TITLE OF MATCHING PROGRAM

The title of this matching program as it will be reported by the Department of Homeland Security and the Office of Management and Budget is as follows: Verification Division DHS-USCIS/NJLWD.

B. MATCHING AGENCIES

1. Source Agency: Department of Homeland Security, United States Citizenship and Immigration Services.
2. Recipient Agency: New Jersey Department of Labor & Workforce Development.

C. PURPOSE AND LEGAL AUTHORITIES

Section 121 of the Immigration Reform and Control Act (IRCA) of 1986, Public Law 99-603, as amended by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), Public Law 104-193, 110 Stat. 2168 (1996), requires DHS to establish a system for the verification of immigration status of alien applicants for, or recipients of, certain types of benefits as specified within IRCA, and to make this system available to state agencies that administer such benefits. Section 121(c) of IRCA amends Section 1137 of the Social Security Act and certain other sections of law that pertain to Federal entitlement benefit programs and requires state agencies which administering these programs to use DHS-USCIS' verification system in making eligibility determinations in order to prevent the issuance of benefits to those alien applicants who are not entitled to program benefits because of their immigration status. The VIS database is the DHS-USCIS system which has been established and made available to the NJLWD and other covered agencies for use in making these eligibility determinations..

The NJLWD seeks access to the information contained in the DHS-USCIS VIS database for the purpose of confirming the immigration status of alien applicants for, or recipients of, benefits it administers, in order to discharge its obligation to conduct such verifications pursuant to Section 1137 of the Social Security Act and New Jersey Statute 43:21-4.

D. JUSTIFICATION AND EXPECTED RESULTS

It has been determined by the parties that a computer matching program is the most efficient and expeditious means of obtaining and processing the information needed by the

NJLWD to verify the immigration status of alien applicants for, and recipients of, entitlement benefits. It is expected that this matching program will enable the NJLWD to rapidly confirm the benefit eligibility of alien applicants/recipients with proper immigration status, identify those applicants whose status require further checks to confirm proper eligibility status, and to identify and prevent improper payments to those applicants whose immigration status does not entitled them to receive the benefits administered by the NJLWD.

It has been determined that available alternatives to the use of a computer matching program for verifying immigration status impose a much greater administrative and processing burden (i.e., be much more labor intensive), would result in a higher annual administrative costs, and would protract the average query response time. The anticipate savings to be derived from the use of the electronic verification program including administrative costs and savings derived by eliminating fraudulent benefit payments is \$1,121,268.00 based on FY 2006 savings. Using a computer matching program, the NJLWD is able to process, in an extremely expeditious manner, a much higher volume of queries with reduced overall labor demands. DHS-USCIS will provide once daily responses to NJLWD batch inquiries.

Additionally, because of the rapid response capability provided by this computer matching program, this program will have a greater deterrent effect on applicants seeking to fraudulently receive entitlement benefits administered by the NJLWD as compared to a much slower mail-in procedure. One of the major objectives of IRCA to reduce incentives for illegal aliens to come to and remain in the United States is furthered by this matching program's deterrent effect. Finally, this system also supports efforts to curb waste, fraud, and abuse within federally funded entitlement programs.

E. RECORDS DESCRIPTION

1. Records to be matched:
 - a. Records in DHS-USCIS VIS database which contain information on the status of aliens and other persons on whom DHS-USCIS has a record as an applicant, petitioner, or beneficiary. See Systems of Records Notice, 72 F.R. 17569.
 - b. The NJLWD records pertaining to alien applicants for, or recipients of, entitlement benefit programs administered by the NJLWD
2. Data elements:
 - a. Data elements contained within the NJLWD's records to be matched with DHS-USCIS VIS database:

Alien Registration Number

b. Data elements contained within the DHS-USCIS record to be matched with the NJLWD data may consist of the following:

1. Alien Registration Number
2. Last Name
3. First Name
4. Date of Birth
5. Country of Birth (not nationality)
6. Social Security Number (if available)
7. Date of Entry
8. Immigration Status Data
9. Employment Eligibility Data

3. Number of records: On a monthly basis, approximately 13,000 records from the NJLWD will be matched against the DHS-USCIS' VIS database which consists of more than 110 million DHS-USCIS records.

4. Duration of the program: Eighteen months from the effective date of this Agreement.

F. NOTICE PROCEDURES

DHS-USCIS agrees to publish in the Federal Register a notice of this matching program as specified in the CMPPA and the Office of Management and Budget CMPPA implementing guidance.

As required by 5 U.S.C. 552a(0)(1)(D), the NJLWD will provide periodic notice to applicants for, and recipients of, financial assistance or payments under the Federal benefit program(s) covered by this Agreement that any information they provide may be subject to a computer matching system with the DHS-USCIS. Specifically, the NJLWD will provide each applicant for UC benefits at the time of application a notice informing them that their eligibility status will be verified by matching against the DHS-USCIS database.

G. VERIFICATION PROCEDURES

1. The NJLWD may not suspend, terminate, reduce, or make a final denial regarding the Federal benefit program eligibility of an applicant/recipient covered by this part based on that individual's immigration status, or take other adverse action against such individual as a result of information produced by the matching program until information has been independently verified. DHS-DHS-USCIS' "additional verification procedures" as described in its M-300 SAVE Users Manual, a copy of which is provided to each user upon execution of the CMA.

2. Furthermore, the NJLWD may not suspend, terminate, reduce, or make a final denial regarding the Federal benefit program eligibility of any individual described

in paragraph 1, or take other adverse action against such individual as a result of information produced by this matching program unless: (A) such individual has received notice from the NJLWD containing a statement of the findings of the immigration status check; and (B) until the subsequent expiration of any notice period provided by such program's law or regulations, or 30 days, whichever is later. Such opportunity to contest may be satisfied by the notice, hearing, and appeal rights governing the Federal benefit program the applicant has been provided the opportunity to refute any adverse status information as a result of this verification query. The exercise of any such rights shall not affect any rights available under this section.

H. RECORDS RELATING TO UNITED STATES CITIZENS

This Agreement authorizes the NJLWD to use the Verification Division's system for the purposes of verifying the immigration status of alien applicants for UC benefits. Nothing in this Agreement authorizes the NJLWD to use the DHS-USCIS system for the purpose of verifying the status of an individual claiming United States citizenship by birth. However, in addition to records relating solely to aliens, VIS contains records relating to former lawful permanent resident aliens who have become naturalized United States citizens. It is possible that applicants for UC may through fraud or error, present documentation identifying themselves as lawful permanent resident aliens without informing the NJLWD that they have become a United States citizen, thereby, resulting in a NJLWD inquiry to the DHS-USCIS.

In the event that DHS-USCIS receives a request for a verification of a NJLWD applicant who is a LPR or a United States Citizen, the request will be referred to a DHS-USCIS Immigration Status Verifier for additional verification procedures. All safeguards and protections provided by the CMPPA, Privacy Act and this Agreement regarding the use, disclosure, and security of DHS-USCIS records apply to DHS-USCIS records regarding United States citizens to the same extent as to the DHS-USCIS records relating to lawful permanent resident aliens. Pursuant to the Department of Homeland Security's Policy, guidance Memorandum 2007-1, to the extent practicable, privacy protections afforded to US citizens and LPRs shall be afforded to non LPRs and non citizens.

I. DISPOSITION OF MATCHED ITEMS

Records collected by DHS-USCIS in the process of establishing immigration and citizenship status or employment authorization are stored and retained in the VIS Repository for ten (10) years from the date of the completion of the verification unless the records are part of an on-going investigation in which case they may be retained until completion of the investigation. Photocopies mailed to DHS in response to a Tentative Non-Confirmation (TNC) will be maintained as long as necessary to complete the verification process, and the duration of the benefit granted.

J. SECURITY SAFEGUARDS

DHS-USCIS agrees to safeguard information it receives from the NJLWD in connection with Status verification inquiries in accordance with the Privacy Act of 1974(5 U.S.C. 552a), the Immigration Reform and Control Act of 1986, other applicable statues, and the requirements of this basic agreement between the parties.

DHS-USCIS agrees to safeguard the information provided by the NJLWD in accordance with DHS-USCIS disclosure standards and to provide the name of DHS-USCIS program inspector responsible for compliance with these standards. Individuals who wish to obtain copies or records pertaining to themselves resulting from queries submitted to DHS-USCIS, may do so by following the Freedom of Information Act and Privacy Act procedures that can be found at www.DHS-USCIS.gov. DHS-USCIS also agrees to limit access to NJLWD provided information to individuals responsible for the verification of the alien's immigration status or who require access to the information to perform necessary support functions or follow-up actions.

The DHS-USCIS contractor's data facility where the NJLWD and DHS-USCIS information is stored complies with requirements of the Department of Homeland Security, National Security Systems Policy Directive 4300B. It is a secure facility accessed only by authorized individuals with properly coded key cards, authorized door keys or access authorization. There is a security guard force, on duty 24 hours a day, 7 days a week. The building is protected against unauthorized access, unauthorized use of equipment, or removal of storage media and listings. Employees at the facility have undergone background checks in order to be granted clearance and are provided access badges.

The NJLWD agrees to safeguard information it receives from DHS-USCIS under the verification process in accordance with the requirements of the Privacy Act (5 U.S.C. 552a), and applicable Federal and state entitlement benefit program record retention and disclosure requirements.

The NJLWD also agrees to limit access to information to those individuals responsible for the verification of the alien's immigration status or who require access to the information to perform necessary support functions. The NJLWD will restrict further dissemination of the information unless required in connection with state or the Federal entitlement program law enforcement responsibilities.

The NJLWD has taken measures to secure information received from DHS-USCIS for purposes of the matching program in accordance with applicable State and Federal entitlement program rules procedures. The NJLWD's offices are located in secure buildings, and access to premises is by official identification. All records are stored in government controlled buildings which are locked during non-duty office hours. Records are stored in cabinets or machines which are also locked during non-duty office hours. Access to automated records is controlled by user identification and passwords.

The computer security systems used by both DHS-USCIS and the NJLWD offer a high

degree of resistance to tampering and circumvention. Multiple levels of security are maintained within their computer system control program. Both security systems limit access to authorized personnel strictly on a "need-to-know" basis, and control an individual user's ability to access and alter records within the system. All users are given a unique ID with personal identifiers and interactions with the system are recorded.

K. RECORDS USE, DUPLICATION AND REDISCLOSURE RESTRICTIONS

The parties agree to comply with the data maintenance and disclosure control requirements specified within Part 1 of this Agreement. The parties agree not to duplicate or disclose any Records received from other party pursuant to this matching agreement except where it necessary to verify the immigration status of alien applicants for, or recipients of, the UC benefit program administered by the NJLWD (including follow-up actions. Additionally, if the matching program uncovers evidence of fraudulent claims or the use of fraudulent immigration documents, the parties may redisclose the records as necessary to conduct law enforcement investigations or prosecutions by the NJLWD or DHS-USCIS, as appropriate, or as otherwise required by law.

L. RECORDS ACCURACY ASSESSMENT

DHS-USCIS currently estimates that information within its VIS database is 90-95% accurate in reflecting immigration status, but continues to undertake various actions to further improve the quality of the VIS database. In addition, in cases where status is not confirmed through the VIS, additional verification procedures are used, which allows DHS-USCIS to check all necessary indices and files before providing the NJLWD with immigration status information. This process includes procedures for DHS-USCIS to correct any errors detected in the immigration status information.

M. COMPENSATION

The User Agency shall pay the standard billing rates in accordance with the terms of the reimbursement Memorandum of Agreement (MOA) addendum to the MOU and arrange the obligations, processes and methods related to the payment of required fees to DHS-USCIS and/or its authorized agents.

The current standard billing rates are attached to the MOA. The standard billing rates and methods of payment are subject to change upon prior written notification to the User Agency.

N. COMPTROLLER GENERAL ACCESS

The GAO (Comptroller General) may have access to all of the matching records of the NJLWD and DHS-USCIS necessary to verify compliance with the requirements of the CMPPA.

O. EFFECTIVE DATE

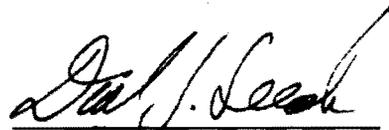
This agreement will become effective 40 days after a report concerning the computer matching program has been transmitted to the Office of Management and Budget (OMB) and transmitted to Congress along with a copy of the Agreement or 30 days after publication of a computer matching notice in the Federal Register, whichever is later. The Agreement (and matching activity) will continue for 18 months from the effective date, unless within 3 months prior to the expiration of this Agreement, the Data Integrity Board approves a one-year extension pursuant to 5 U.S.C. 552a(o)(2)(D).

P. SIGNATURES

The undersigned are officials of DHS-USCIS and NJLWD who are authorized to represent their agencies for purposes of this Agreement.



David Bounds
Chief
Benefits Operations
Verification Division
United States Citizenship and Immigration
Services



David J. Socolow
Commissioner
New Jersey Department of Labor
& Workforce Development

Date: 9/22/08

Date: 8/19/08

**Q. DEPARTMENT OF HOMELAND SECURITY
DATA INTEGRITY BOARD APPROVAL**

Approved: 

Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security

Date: 1-16-09

“Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and the New Jersey Department of Labor & Workforce Development (NJLWD)

**NEW JERSEY DEPARTMENT OF LABOR
SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS
COST/BENEFIT ANALYSIS
PROGRAM YEARS 1997-2006**

<u>YR</u>	<u>COST (1.)</u>	<u>NUMBER SUBMITTED</u>	<u>NUMBER VERIFIED</u>	<u>NUMBER SECONDARY VERIFICATION</u>
1997	\$1,622.00	135,663	131,410	4,253
1998	\$1,172.00	113,302	110,271	3,031
1999	\$ 893.00	106,661	102,388	4,273
2000	\$1,266.00	88,275	83,190	5,085
2001	\$ 904.00	86,000	74,409	6,591
2002	\$1,740.00	95,725	91,156	4,569
2003	\$1,842.00	90,967	76,709	12,988
2004	\$1,681.00	50,869	46,722	4,097
2005	\$2,656.89	35,407	23,311	12,096
2006	\$2,442.44	26,155	17,300	8,855

<u>YR</u>	<u>#UNENTITLED ALIENS</u>	<u>AVG WKLY BENEFIT AMT</u>	<u>AVERAGE DURATION</u>	<u>ADJ AVG (3) DURATION</u>	<u>EST (2) SAVINGS</u>
1997	370	\$250	16.3	14.3	\$1,322,750
1998	341	\$257	16.4	14.4	\$1,261,973
1999	166	\$269	16.7	14.7	\$ 656,414
2000	157	\$282	16.8	14.8	\$ 655,255
2001	130	\$302	17.3	15.3	\$ 600,678
2002	165	\$323	19.0	17	\$ 906,015
2003	106	\$325	17.9	15.9	\$ 547,755
2004	129	\$334	18.0	16	\$ 689,376
2005	196	\$341	18.5	16.5	\$1,102,794
2006	205	\$344	17.9	15.9	\$1,121,268

1. Cost determined from yearly Data Processing Chargeback Reports.
2. Estimates based upon averages for total claimant population; actual monetary entitlements are not available
3. This column reduces the estimated savings to allow for the possibility that, on average, a payment of two weeks of benefits could have been made prior to adjudication of the eligibility of unentitled aliens. As of January 10, 2005, the secondary verification became an automated process and we anticipate that discovery and adjudication of this issue will be completed prior to any weeks being paid.

COMPUTER MATCHING AGREEMENT
BETWEEN
THE UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES
(USCIS)
AND
THE UNITED STATES DEPARTMENT OF EDUCATION (ED)

A. INTRODUCTION

This agreement is executed to comply with the Computer Matching and Privacy Protection Act of 1988, (CMPPA) (Pub. L. No. 100-503), October 18, 1988; 102 Stat. 2507, which was enacted as an amendment to the Privacy Act of 1974 5 U.S.C. 552a et. seq. (Privacy Act). The CMPPA requires the parties involved in any matching program covered by the CMPPA to execute a written agreement specifying the terms and conditions under which matches will be conducted. The agreement must also include the procedural requirements and due process safeguards under the CMPPA.

B. MATCHING PARTICIPANTS

1. Source Agency: United States Citizenship and Immigration Services (USCIS), Department of Homeland Security (DHS)
2. Recipient: United States Department of Education (ED)

C. DEFINITIONS

1. Applicants - alien applicants for or recipients of applicable Title IV Student Financial Assistance Programs whose applications are processed through the Federal Application Central Processing System.
2. Title IV Student Financial Assistance Programs - include the Federal Pell Grant Program, the Academic Competitiveness Grant Program, the National Science and Mathematics Access to Retain Talent Grant Program, the Federal Perkins Loan Program, the Federal Work-Study Program, the Federal Supplemental Educational Opportunity Grant Program, the Federal Family Education Loan Program, the William D. Ford Federal Direct Loan Program, the Leveraging Educational Assistance Partnership Program, and the Gaining Early Awareness and Readiness for Undergraduate Program.

D. TITLE OF MATCHING PROGRAM

The title of this matching program as it will be reported to Congress and the Office of Management and Budget (OMB) is as follows:

Verification Division USCIS/ED.

E. MATCHING TERMS AND CONDITIONS

1. ED will provide identifying information from Applicant files to the USCIS using IBM's Transmission Communication Protocol/Internet Protocol (TCP/IP) capabilities via File Transfer Protocol (FTP) for the purpose of verifying each Applicant's immigration status. The USCIS agrees to provide to ED (through encrypted FTP transmission) the current immigration status of each Applicant processed through the computer matching program within 24 hours of ED's request for Primary Verification. ED will notify the Applicants of the results of the match in writing.
2. The USCIS agrees to conduct Automated Additional Confirmation for Applicants whose status could not be confirmed through Primary Verification for Title IV Student Financial Assistance Programs. The USCIS automatically initiates additional Confirmation for these records, and through the electronic data exchange, via encrypted FTP transmission, provides ED the results as the individual cases are processed (usually within 72 hours or sooner). ED will notify the Applicants of the results of the Automated Additional Confirmation in writing.
3. The USCIS agrees to provide to institutions of higher education exact verification of the Applicant's immigration status through Manual Additional Verification on the Document Verification Request (Form G-845). Institutions of higher education will submit the Form G-845 to the USCIS through district USCIS offices at no cost to the institution. Upon receipt of a G-845 request from an institution, the USCIS personnel will conduct a manual search to determine the Applicant's immigration status. The USCIS will respond to the institution's request within ten (10) working days after the request is received by the USCIS. The institution of higher education will notify the Applicants of the results of the Manual Additional Verification in writing.

F. PURPOSE AND LEGAL AUTHORITIES

ED seeks access to the information contained in the USCIS database under the Immigration Reform and Control Act of 1986 (IRCA), (Pub. L. No. 99-603), and referred to as the Verification Information System (VIS), for the purpose of confirming the immigration status of Applicants for assistance, as authorized by section 484(g) of the Higher Education Act of 1965, as amended (HEA), 20 U.S.C. 1091(g), consistent with the requirements of section 484(a)(5), 20 U.S.C. 1091(a).

ED is authorized to participate in the matching program, which is the subject of this Agreement, under the authority of section 484(g) of the HEA, as amended, 20 U.S.C. 1091(g). USCIS is authorized to participate in this immigration status verification system under section 103 of the IRCA, 8 U.S.C. 1103.

G. JUSTIFICATION AND EXPECTED RESULTS

ED and the USCIS have determined that a computer matching program is the most efficient, expeditious and effective means of obtaining and processing the information needed by ED to verify the immigration status of Applicants for the Title IV Student Financial Assistance Programs. The principal alternative to using a computer matching program for verifying immigration status would be to institute a mail-in procedure, an alternative which would impose a greater administrative burden and delay response times. Using the computer matching program, responses can be provided within 24 hours of ED inquiries. Applicants who require Automated Additional Confirmation are provided a response in as little as 72 hours from ED's additional confirmation request.

ED expects that this computer matching program will enable it to quickly and efficiently verify the status of Applicants for the purpose of determining their eligibility for Title IV Student Financial Assistance Programs. The matching program will also quickly identify those Applicants who require Manual Additional Verification before the institution of higher education can independently determine whether the Applicant meets the eligibility requirements of the Title IV Student Financial Assistance Programs.

ED estimates that this computer matching program costs \$694,293 per year to operate. Given an estimated processing time of fifteen minutes per Applicant, and an average cost per record to process a DHS verification of \$6.07 per application, and approximately 751,752 Applicants per year, verification of immigration status in the absence of computer matching (i.e., using mail-in procedures) would cost institutions approximately \$4,563,135 per year. Because computer matching reduces the number of Applicants requiring manual verification by 92%, this administrative cost to institutions is reduced by \$4,231,082. (Attached is a detailed cost/benefit analysis).

In addition to the savings in administrative costs, the computer matching program provides identification of all eligible categories of immigration status documents. The notice to Applicants informing them that their application information is subject to computer matching is expected to have a deterrent effect on Applicants seeking to fraudulently receive assistance under the Title IV Student Financial Assistance Programs.

H. RECORDS DESCRIPTION

1. Records to be matched:
 - a. ED system of records: Federal Student Aid Application File (18-11-01)
The ED system of records notification was last published in the Federal Register on April 11, 2001 (66 FR 18758).
 - b. USCIS system of records: Verification Information System Records
Notice was last published in the Federal Register on April 9, 2007 (72 FR 17569).

2. Data elements contained within the Federal Student Aid Application File to be matched with the USCIS VIS database:
 - a. Alien Registration Number;
 - b. First and last name;
 - c. Date of Birth;
 - d. Current Social Security Number; and
 - e. Gender

3. When a record containing the above data elements is matched with the VIS database, the following data elements are added to the record and returned to ED:
 - a. Primary or Secondary Verification Number;
 - b. Date of Entry;
 - c. Country of Birth;
 - d. USCIS Status Code; and
 - e. Eligibility Message Code.

Number of records: On a monthly basis, approximately 41,764 records from ED will be matched against the VIS database, which consists of more than 60 million alien records.

Duration of the program: Eighteen months from the effective date of this Agreement.

I. NOTICE PROCEDURES

As required by 5 U.S.C. 552a(o)(1)(D), ED provides a notice to Applicants for Title IV Student Financial Assistance Programs covered by this Agreement that any information they provide may be subject to verification through matching programs.

ED agrees to ensure that, at the time of application for Title IV Student Financial Assistance Programs, each Applicant is provided individual notice that the information provided on his or her application is subject to verification through computer matching programs. Because Applicants must reapply each year, an individual notice is provided annually. As a result of providing an individual notice on each application, periodic notice is not needed under this computer matching agreement.

J. VERIFICATION PROCEDURES

ED may not suspend, terminate, reduce, or make a final denial of assistance under the Title IV Student Financial Assistance Programs or take other adverse action against an individual as a result of the information produced by this matching program, (1) unless such individual has received a notice stating the results of the match and stating that the individual has 30 days to provide documentation to the institution to contest the results of the match, and (2) until the expiration of this subsequent 30 day notice period. The notice will state one of the following messages depending upon the reason(s) for the nonmatch:

- DHS has not yet confirmed your status as a non citizen, in an immigration status, commensurate with the requirements of eligibility for the financial assistance for which you have applied (Item 14). DHS will continue to check its records and we will notify you once we receive more information from DHS.
- USCIS did not confirm that you are a non citizen, in an immigration status, commensurate with the requirements of eligibility for the financial assistance for which you have applied. You must submit proof to your school that you are in the requisite noncitizen immigration status. If you do not submit proof within 30 days, or longer if your school allows, you may not be eligible for Federal student aid.
- USCIS has not yet confirmed that you are a noncitizen, in an immigration status, commensurate with the requirements of eligibility for the financial assistance for which you have applied (Item 14). You must submit proof to your school that you are a noncitizen, in the requisite immigration status. If you do not submit proof to your school within 30 days, or longer if your school allows, you may not be eligible for Federal student aid.
- USCIS did not have enough information to confirm that you are an eligible noncitizen, in an immigration status commensurate with the requirements of eligibility for the financial assistance for which you have applied (Item 14). You must contact the financial aid office at your school to find out what information is needed. If you do not submit the required information within 30 days, or longer if your school allows, you may not be eligible for Federal student aid.
- USCIS could not confirm that you are an eligible noncitizen, in an immigration status commensurate with the requirements of eligibility for the financial assistance for which you have applied (Item 14) because there is an issue with your Alien Registration Number (Item 15). You must submit proof to your school that you are a noncitizen in the requisite immigration status. If you do not submit proof within 30 days, or longer if your school allows, you may not be eligible for Federal student aid.

Applicants for, or recipients of, assistance under the Title IV Student Financial Assistance Programs may not have their benefits suspended, terminated, reduced, denied, or otherwise adversely affected as a result of information produced by this matching program until additional procedures as specified within ED guidelines have been used to independently verify such information. These additional procedures are described as follows:

- Under 34 CFR 668.33(a)(2), Applicants for assistance under the Title IV Student Financial Assistance Programs must document their immigration status to prove their eligibility. Under current policy guidelines, institutions must independently verify this eligibility before disbursing Title IV Student Financial Assistance,

either through a visual inspection and identification of the documents or reliance on the automated or manual assistance of USCIS in identifying the documents.

- If an institution's independent verification of immigration status determines an alien applicant to be ineligible for the Title IV Student Financial Assistance Programs, the institution of higher education must, under 34 CFR 668.42(b)(2), make available to such applicant any information describing the student eligibility requirements which it used to make its determination. If the applicant is in disagreement with the institution's independent determination of his or her immigration status, the institution of higher education has been advised by ED guidelines to refer the Applicant to the USCIS and the Applicant is also provided the opportunity to refute any adverse status information as a result of the verification inquiry for resolution.

K. RECORDS RELATING TO UNITED STATES CITIZENS

This Agreement authorizes ED to use the Verification Division's system for the purpose of verifying the immigration status of Applicants for the Title IV Student Financial Assistance Programs. Nothing in this agreement authorizes ED to use the Verification Division's system for the purposes of verifying the status of any Applicant claiming U.S. citizenship. However, VIS contains, in addition to records relating solely to aliens, records relating to former lawful permanent resident aliens who have become naturalized U.S. citizens. It is possible that Applicants for Title IV Student Financial Assistance Programs may, on occasion, through fraud or error, present documentation identifying themselves as lawful permanent resident aliens without informing ED that the lawful permanent resident alien with that identity has become a naturalized U.S. citizen, thereby resulting in an ED inquiry to the USCIS.

In the event USCIS receives a request for a verification of an ED applicant who is a lawful permanent resident (LPR) or a United States citizen, the request will be referred for additional verification procedures. All safeguards and protections provided by the CMPPA, and this Agreement regarding the use, disclosure, and security of the USCIS records apply to the USCIS records regarding U.S. citizens to the same extent as to the USCIS records relating to lawful permanent resident aliens. Pursuant to Department of Homeland Security Policy, privacy protections afforded to U.S. citizens and LPRs shall be afforded to nonLPRs and noncitizens, to the maximum extent practicable.

L. DISPOSITION OF MATCHED ITEMS

ED will retain all identifiable records received from the USCIS data file(s) with identifying information for a period not to exceed three years after the repayment or cancellation of a Title IV federally-insured loan in accordance with the Education Comprehensive Schedule, ED-RDS-Part 10, Item 16d. For applicants without a federally-insured loan, ED will retain all identifiable records received from the USCIS data files(s) with identifying information for a period not to exceed fifteen years after the

final Pell Grant payment or audit, whichever is first in accordance with the Education Comprehensive Schedule, ED-RDS-Part 10, Item 17a. At the conclusion of the mandatory retention period, these records will be destroyed. This procedure is consistent with legal retention requirements established by ED in conjunction with the National Archives and Records Administration.

All matching records that ED provides to the USCIS will be returned to ED with any USCIS records that are matched. The USCIS will generate an automated disclosure accounting of the records that have been disclosed to ED.

M. SECURITY SAFEGUARDS

USCIS' Security Safeguards

USCIS agrees to safeguard information it receives from ED in connection with status verification inquiries in accordance with the Privacy Act, the IRCA, and other applicable statutes, as well as the requirements of the basic Agreement between ED and the USCIS.

USCIS agrees to safeguard the information provided by ED in accordance with the USCIS disclosure standards and to provide the name of the USCIS program inspector responsible for compliance with these standards. The USCIS also agrees to limit access to information to those individuals responsible for the verification of the alien's immigration status or necessary support functions or follow-up actions, and to restrict the further dissemination of information.

USCIS contractor data facility where ED and USCIS information is stored complies with requirements of Department of Homeland Security, National Security Systems Policy Directive 4300B. It is a secure facility accessed only by authorized individuals with properly coded key cards, authorized door keys or access authorization. There is a security guard force, twenty-four (24) hours a day, seven (7) days a week. The building is protected against unauthorized access, unauthorized use of equipment, or removal of storage media and listings. Employees have clearances through background checks and are provided badges.

ED's Security Safeguards

ED's centralized processing facility, which will move from Meriden, Connecticut, to Plano, Texas in the fall of 2007, has a high level of security. Access within the processing facility is controlled by a computerized badge reading system, while other areas are controlled by cipher locks with combinations that are changed monthly. All employees must display a photo ID upon entering the building.

The perimeter of the both the Meriden and the Plano facilities are monitored periodically and the main entrances are monitored continuously by a third-party security force. Access to all doors, as well as to the data center's main corridors, is monitored by 12

CCTV cameras that can pan, zoom, and record the perimeter premises. Each facility monitors access 24 hours a day, 7 days a week. The CCTV cameras can record access at random or at a specific camera location. The cameras are connected to two VCRs for recording purposes. Videotapes are retained for one month before being recycled by physical security administration.

ED limits access to the information received from the USCIS and maintained in the VIS database to those individuals responsible on a "need-to-know" basis. Individuals with a "need-to-know" are authorized ED employees and ED contractors who make use of the data to determine eligibility for Title IV Student Financial Assistance Programs and communicate with students, their families and Financial Aid Administrators at postsecondary institutions. Access to this information is controlled in accordance with a strict set of security procedures documented in the VIS System Security Plan, Section 4.0 Technical Controls. An automated audit trail is maintained for all personal interactions within the VIS. Additionally, all changes made by authorized users of the VIS to the Free Application for Federal Student Aid (FAFSA) data in a new transaction also have a specified audit trail. All authorized users of the VIS are issued unique user IDs with personal identifiers, which are mandatorily changed every month.

The Federal Information Security Management Act of 2002 requires all agencies to report security incidents to a Federal incident response center. The Center (US-CERT) is located within the DHS. All incidents involving personally identifiable information (PII) will be reported to US-CERT within one hour of discovering the incident in electronic or physical form and will not distinguish between suspected and confirmed breaches. US-CERT will forward all agency reports to the appropriate Identity Theft Task Force point-of-contact also within one hour of notification by an agency.

N. RECORDS USE, DUPLICATION AND REDISCLOSURE RESTRICTIONS

ED and USCIS agree to safeguard PII that is exchanged between the agencies or their agents in accordance with the restrictions under the provisions of the Privacy Act.

USCIS agrees to provide safeguards as outlined under section 121 of the IRCA, which states that, "such system shall not be used by the USCIS for administrative (non-criminal) immigration enforcement purposes". Further, the law provides for immigration status verification without regard to the "sex, color, race, religion, or nationality of the individual involved."

ED and USCIS agree not to duplicate, re-disclose or disseminate any records from the other party pursuant to this matching agreement except where it is essential to conduct the matching program, i.e., to verify the immigration status of Applicants for the Title IV Student Financial Assistance Programs administered by ED (including follow-up actions), or where authorized by law, e.g., for necessary law enforcement investigations or prosecutions by ED and DHS, as appropriate, if the match uncovers activity that warrants such action (e.g., evidence of fraudulent claims or the use of fraudulent immigration documents).

O. RECORDS ACCURACY ASSESSMENT

USCIS maintains its records to a standard of accuracy that will reasonably assure fairness in any eligibility determination made on the basis of the record.

USCIS currently estimates that information within its VIS database is 90-95% accurate in reflecting immigration status, but continues to undertake various actions to further improve the quality of the VIS database. In addition, in cases where status is not confirmed through VIS, Automated Additional Confirmation and Manual Additional Verification procedures are used, which allow USCIS to check all necessary indices and files before providing ED or the institution with immigration status information. This process includes procedures for USCIS to correct any errors detected in the immigration status information.

During the 2005-2006 award year, in which there were approximately 751,752 Applicants for Title IV Student Financial Assistance Programs that were sent to USCIS to be matched, ED received no reports of discrepant data records.

P. COMPTROLLER GENERAL ACCESS

The GAO (Comptroller General) may have access to all of ED and the USCIS match result records as necessary in order to verify compliance with this agreement.

Q. EFFECTIVE DATE

This agreement will become effective 40 days after a report concerning the computer matching program has been transmitted to the Office of Management and Budget (OMB) (unless a request to OMB for a ten-day waiver is approved), and transmitted to the Congress along with a copy of the agreement, or 30 days after publication of a computer matching notice in the Federal Register, whichever is later.

The agreement (and matching activity) will expire 18 months from the effective date, unless within three months prior to the expiration of this agreement, the Data Integrity Boards approve a one-year extension of this agreement pursuant to 5 U.S.C. 552a(o)(2)(D).

R. SIGNATURES

The undersigned are officials of the USCIS and ED who are authorized to represent their agencies for purposes of this agreement.



Date: 9/18/07 USCIS

Date: _____ ED

for David Bounds
Chief
Benefits Operations
Verification Division
United States Citizenship and Immigration
Services

Lawrence A. Warder
Acting Chief Operating Officer
Federal Student Aid
U.S. Department of Education

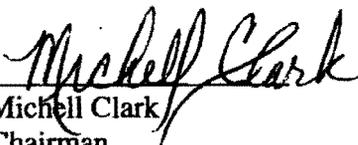
S. AGENCY DATA INTEGRITY BOARD APPROVALS

Date: Sept. 18, 2007

Approval: 

Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security

Date: 9/18/07

Approval: 

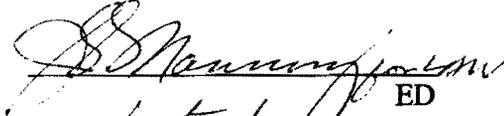
Mitchell Clark
Chairman,
Data Integrity Board
U.S. Department of Education

R. SIGNATURES

The undersigned are officials of the USCIS and ED who are authorized to represent their agencies for purposes of this agreement.

USCIS
Date: _____

David Bounds
Chief
Benefits Operations
Verification Division
United States Citizenship and Immigration
Services



ED
Date: September 18, 2007

Lawrence A. Warder
Acting Chief Operating Officer
Federal Student Aid
U.S. Department of Education

S. AGENCY DATA INTEGRITY BOARD APPROVALS

Date: _____

Approval: _____

Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security

Date: _____

Approval: _____

Michell Clark
Chairman,
Data Integrity Board
U.S. Department of Education



USCIS/DHS - ED Data Matching Agreement Cost/Benefit Analysis Award Year 2005-06 Data

The eligibility requirements of section 484 (a)(5) of the Higher Education Act of 1965, as amended (HEA), and 34 CFR 668.33 (a) of the Student Assistance General Provisions regulations require, in part, a student to be a citizen or national of the United States or to provide evidence from the United States Citizenship and Immigration Services (USCIS), Department of Homeland Security (DHS), that the student is a permanent resident of the United States or is in the United States for other than a temporary purpose with the intention of becoming a permanent resident.

Prior to the USCIS/U.S. Department of Education (ED) data match, institutions of higher education were required to verify and document all eligible noncitizen applicants' citizenship status in order to determine if they were indeed in the "eligible noncitizen" category. However, in January of 1989 a data match was developed and implemented between USCIS and ED for the purpose of verifying eligible noncitizen status. As a result of the data match, burden has been reduced on institutions.

Applicant records whose status are "eligible noncitizens" are sent from ED's Central Processing System (CPS) to the USCIS database. For those applicants whose status is confirmed via the USCIS/ED matching program, institutions do not need to collect additional documentation to further verify the applicant's immigration status. The institution has the authority to rely on the Student Aid Report (SAR) as proof that these applicants are eligible noncitizens. However, for those applicants whose status cannot be confirmed via the match (i.e., the eligible noncitizen applicant record from the CPS was not in the USCIS data base), institutions are required to verify and document, if needed, the applicant's immigration status.

The following are the steps used to estimate the costs and savings associated with performing the USCIS data match during the 2005-06 application processing cycle and award year using various organizations. Costs are broken out by USCIS, ED, and institutions of higher education. Savings are broken out by ED and by institutions. At each step, the process used to estimate cost or savings is described in narrative and then summarized in a series of bullets showing each component calculation of the step.

A. Costs of USCIS Data Match

There are three main categories of costs associated with the USCIS match: costs to USCIS, costs to ED, and the costs to institutions of higher education.

I. United States Citizenship and Immigration Services Costs

USCIS is expected to incur on-going costs for processing all applicant records that are transmitted to USCIS by ED. One-time costs are not included in this analysis because the one-time costs were incurred when the match was put in place in 1989. The following are the costs that USCIS has provided to ED during the eighteen-month processing:

• USCIS personnel costs including fringe benefits and overhead	\$185,281
• USCIS contractor costs	\$61,887
• Verification Information System (VIS) program funding	\$26,329
• VIS Data Base	<u>+ \$36,454</u>
Total	\$309,951

II. U.S. Department of Education Costs

ED will incur several costs for performing the match with USCIS: the cost of processing the records at the CPS, the cost of leasing telephone lines for transmitting the match data to and from USCIS, and the cost of administering the match. Each of these categories of costs are presented below.

CPS Processing Cost

The CPS will incur costs for the ongoing processing of the records that will be sent to USCIS. Only those records that meet the following criteria will be transmitted to USCIS for data match processing purposes:

- Alien registration number is in the range of A000000001 through A059999999 or A070000000 through A999999999;
- Date of birth is non-blank;
- Last name and first name are non-blank; and
- USCIS flag is not equal to Y (i.e., not already verified).

751,752 applicant records were sent to USCIS during the 18-month 2005-06 processing cycle. The incremental cost to ED for processing and transmitting these applicant records for the USCIS match, is estimated by ED operations

staff to be \$0.01 per record transmitted. Therefore, the total cost for processing application records for the USCIS match is:

• Records sent to USCIS	751,752
• Processing cost per record	<u>x \$0.01</u>
Total	\$7,518

Currently, schools require applicants who are not identified in the match as being eligible noncitizens (i.e., records which were transmitted for data matching purposes resulted in a "No" match) to have the applicant records reprocessed (history corrections). In 2005-06, 123,239 records transmitted to USCIS resulted in a "No" match (from CPS Table MTC-07). It is assumed that approximately 25% of these "No" match records, or 30,810, were reprocessed. The cost of reprocessing each record is \$.084. Therefore, the total cost to reprocess the history corrections for records with a "No" match results is 30,810 x \$0.084 = \$2,588.

• "No" match records	123,239
• Percent returning as corrections	<u>x .25</u>
• Total corrections	30,810
• Processing cost per record	<u>x \$0.084</u>
Total	\$2,588

The CPS processing cost is \$10,106, which represents the total cost of processing original records plus the cost of processing history corrections:

• Application record processing	\$7,518
• History correction processing	<u>+\$2,588</u>
Total	\$10,106

Cost of Leasing Telephone Line

ED leases a dedicated telephone line for electronically transmitting the match files to and from USCIS. The cost of leasing this telephone line for the purpose of performing the USCIS match during the 2005-06 eighteen-month processing cycle was \$9,432.

Lease telephone line cost per month	\$524
Multiplied x 18 processing months	<u>x 18</u>
Total cost of leased telephone line	\$9,432

ED Administrative Costs

ED staff is involved in monitoring the match and evaluating its effectiveness. A number of ED staff are involved, none on a full-time basis. For the purpose of this analysis, they are averaged into the level of effort required by one full-time employee at a GS-13, step 1 grade level which equates to a salary of \$79,397 per year (Office of Personnel Management GS Schedule for Washington-Baltimore

area). The level of effort required for the USCIS match is estimated to be approximately one-quarter person to perform the duties of the match during the 18 month application processing cycle. The total ED administrative cost is \$32,751 ($\$79,397 \times .25 = \$19,849 + (\$79,397/2 \times .25 = \$9,925) = \$29,774$, which is then increased by 10% to account for fringe benefits and overhead costs, for a total cost of \$32,751.

Total ED Costs

The total costs to ED for processing the records, leasing telephone lines, and administrative costs is \$52,289:

• ED record processing	\$10,106
• Leased telephone line	\$9,432
• ED administration	<u>+\$32,751</u>
Total	\$52,289

III. Institutional Costs

As mentioned previously, institutions of higher education are required to verify and document all applicants whose immigration status cannot be confirmed via the match.

Current data indicates that in 2005-06 the USCIS match resulted in 123,239 records reporting a "No" match result. Applying the program eligibility (.581) and the show-up rate reductions (.764) to this figure results in the estimated number of institution match records of 54,704.

To calculate the institutions' costs, it is assumed that the equivalent of a full-time employee at a GS-9 step 1 grade level (OPM hourly rate of \$22.06) is assumed to take about one quarter-hour (15 minutes) to verify and document each record for whom a match did not occur. This amount is increased by 10% to account for fringe benefits and overhead to \$24.27. The hourly amount is then divided by 4 to obtain the amount for one-quarter hour, or \$6.07. The institutions' total cost of verifying and documenting the 54,704 "No" match result records times \$6.07, labor cost for 15 minutes effort, for a total of \$332,053.

• GS-9 hourly salary step 1	\$22.06
• Fringe benefits and overhead rate	<u>x 110%</u>
• Annual employee cost	\$24.27
• Time to process USCIS match record	<u>÷ 4</u>
• Hourly cost to process USCIS match	\$6.07
• Institution USCIS match records	<u>x 54,704</u>
Total	\$332,053

IV. Total USCIS Data Match Costs

The total costs to USCIS, ED, and institutions of the USCIS data match are \$694,293.

• USCIS cost	\$309,951
• ED cost	\$52,289
• Institutions' cost	<u>+ \$332,053</u>
Total	\$694,293

B. Savings Attributable to USCIS Data Match

There are two categories of savings that can be attributed to performing the data match between ED and USCIS: the cost avoidance by the Federal government of not disbursing Title IV student aid to ineligible applicants, and the reduction in burden for institutions by having to confirm the citizenship/immigration status on a much smaller pool of students (i.e., those that did not match with the USCIS file). The savings attributable to each of these categories is described below.

I. Government Cost Avoidance

By matching the Title IV applicants to the USCIS files, ED is able to improve its ability to identify students who attempt to fraudulently receive Federal student aid under a false immigrant status. Thus, the government will avoid the cost of disbursing Title IV aid funds to individuals who would otherwise receive aid had the match not existed. As shown above, 123,239 students who indicated they were eligible noncitizens or who reported Alien Registration Numbers were subsequently found not to be in the USCIS files (i.e., records for which a "No" match result was received from USCIS). It is necessary to calculate how many of these "No" match students would have been student aid recipients in any case, and how many will be eliminated from eligibility because they cannot provide satisfactory documentation proving their eligibility. Thus, an estimate of eligibility for student aid programs and receipt of aid is required.

For this analysis, the 2005-06 rate of qualification of all students applying for the Federal Pell Grant Program is 58.1%. Thus, the 123,239 "No" match records were multiplied by the Pell Grant eligibility rate of 58.1%, resulting in an estimated 71,602 "No" match records qualifying for (but not necessarily receiving) Federal student aid. This number must be reduced to account for the number of eligible students who actually receive Federal student aid. The 2005-06 show-up rate for the Pell Grant Program eligible applicants is 76.4%. Applying this percent to the 71,602 eligible students with a "No" match, results in an estimated 54,704 students who would have become recipients of some sort of Federal student aid.

Some of these students, however, knowing they are not eligible to receive Federal student aid, will be dissuaded from actually attempting to receive aid by the prospect of verifying their immigration status. Others, during the process of

verifying their status at the institution, will be found not to be eligible. No hard data exists concerning the number of “No” match students identified by USCIS who are subsequently found not to be in compliance. It is reasonable to assume, however, that the vast majority of these “No” match students are not in compliance and potentially could receive aid. For this analysis, only 1% of “No” match students who would otherwise receive aid will be found not to be in compliance, and therefore not receive aid, or $54,704 \times 1\% = 547$. Even this conservative estimate yields significant savings. It is assumed that these noncompliant students would have received student aid at levels similar to all other aid recipients. Multiplying the number of students not in compliance times the average aid received by all students yields the estimate of cost avoidance savings.

The estimated average amount of Federal Title IV student aid received is \$6,883. The total savings to the government as a result of the match is $547 \times \$6,883 = \$3,765,001$.

• Number of “No” match result students	123,239
• Eligibility percent	<u>x 58.1%</u>
• Total eligible	71,602
• Show-up rate	<u>x 76.4%</u>
• Total recipients before compliance adjustment	54,705
• Percent of recipients not in compliance	<u>x 1%</u>
• Potential recipients not in compliance	547
• Average federal student aid received	<u>x \$6,883</u>
Total	\$3,765,001

II. Institutions’ Savings

Institutions are required to verify and document all applicants whose immigration status cannot be confirmed by the USCIS match. If the match was not in effect, any student reporting a status of eligible noncitizen or reporting an Alien Registration Number on the application would be required to verify their status at the institution. Performing a match with USCIS significantly reduces the number of students that institutions must verify, and therefore reduces the burden and administrative costs that institutions would otherwise incur. Without the match, all 751,752 students earmarked for the USCIS match would have to be verified at the institutions. From the analysis above, it costs institutions approximately \$6.07 per record to process a USCIS verification. The total cost to institutions, then, if no USCIS match existed, would be $751,752 \times \$6.07 = \$4,563,135$. As described above, the estimated cost to institutions with the USCIS match in place is \$332,053. Therefore, the total savings to institutions by having a USCIS match is $\$4,563,135 - \$332,053 = \$4,231,082$.

• Number of applications sent to USCIS	751,752
• Cost to process single student	<u>x \$6.07</u>
• Total institutions’ cost without match	\$4,563,135

• Total institutions' cost with match	<u>-\$332,053</u>
Total	\$4,231,082

III. Total USCIS Data Match Savings

The total savings attributable to the USCIS data match is:

• Government cost avoidance	\$3,765,001
• Institutions' savings	<u>+\$4,231,082</u>
Total	\$7,996,083

IV. Cost/Benefit Ratio

The ratio of total costs to total benefits is the sum of measurable cost divided by the sum of measurable benefits is:

• Total Cost	\$694,293
• Total Benefits	\$7,996,083
 Cost to Benefit Ratio	 0.0868

4000-01-U

DEPARTMENT OF EDUCATION

Privacy Act of 1974; Computer Matching Program

AGENCY: Department of Education

ACTION: Notice - Computer Matching between the Department of Education and the Department of Homeland Security, United States Citizenship and Immigration Services, formerly the Immigration and Naturalization Service.

SUMMARY: Pursuant to the Office of Management and Budget (OMB) Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, (54 FR 25818 (June 19, 1989)) and OMB Circular A-130, Appendix I (65 FR 77677 (December 12, 2000)) notice is hereby given of the computer matching program between the Department of Education (ED) (the recipient agency), and the Department of Homeland Security, United States Citizenship and Immigration Service (USCIS), (the source agency).

In accordance with the Privacy Act of 1974 (5 U.S.C. 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, and OMB Circular A-130, the following information is provided:

1. Names of Participating Agencies.

The U.S. Department of Education and the U.S. Department of Homeland Security, USCIS.

2. Purpose of the Match.

The matching program entitled "Verification Division USCIS/ED" will permit ED to confirm the immigration status of alien applicants for, or recipients of, financial assistance under Title IV of the Higher Education Act of 1965, as amended (HEA), as authorized by section 484(g) of the HEA; 20 U.S.C. 1091(g). The Title IV programs include: the Federal Pell Grant Program; the Academic Competitiveness Grant Program; the National Science and Mathematics Access to Retain Talent Grant Program; the Federal Perkins Loan Program; the Federal Work-Study Program; the Federal Supplemental Educational Opportunity Grant Program; the Federal Family Education Loan Program; the William D. Ford Federal Direct Loan Program; the Leveraging Educational Assistance Partnership Program; and the Gaining Early Awareness and Readiness for Undergraduate Programs.

3. Authority for Conducting the Matching Program.

The information contained in the USCIS data base is referred to as the Verification Information System (VIS), and is authorized under the Immigration Reform and Control Act of 1986 (IRCA), Pub. L. No. 99-603. ED seeks access to

the VIS database for the purpose of confirming the immigration status of applicants for assistance, as authorized by section 484(g) of the HEA, 20 U.S.C. 1091(g), and consistent with the Title IV student eligibility requirements of section 484(a)(5), 20 U.S.C. 1091(a)(5) of the HEA. USCIS is authorized to participate in this immigration status verification under section 103 of the Immigration and Nationality Act, as amended, 8 U.S.C. 1103.

4. Categories of Records and Individuals Covered.

The records to be used in the match and the roles of the matching participants are described as follows: Through the use of user identification codes and passwords, authorized persons from ED will transmit electronically data from its Privacy Act system of records entitled, "Federal Student Aid Application File (18-11-01)" to USCIS. The data will include the alien registration number, the First and Last Name, date of birth, current Social Security Number and the answer to the question, "Are you male or female?" of the alien applicant for, or recipient of, Title IV assistance. This action will initiate a search for corresponding data elements in a USCIS Privacy Act system of records entitled "Verification Information System Records Notice (DHS-2007-0010)." Where there is a match of records, the system will add the following data to the

record and return the file to ED: the Primary or Secondary Verification Number, a code indicating whether the student was confirmed to be an eligible non-citizen or if a determination could not be made, the date of entry into the U.S., country of birth, and the USCIS status code of the alien applicant or recipient. In accordance with 5 U.S.C. 552a(p), ED will not suspend, terminate, reduce, or make a final denial of any Title IV assistance to such individual, or take other adverse action against such individual, as a result of information produced by such a match, until

- (1) (a) ED has independently verified the information; or
- (b) the Data Integrity Board of ED determines in accordance with guidance issued by the Director of the OMB that (i) the information is limited to identification and amount of benefits paid by ED under a Federal benefit program; and (ii) there is a high degree of confidence that the information provided to ED is accurate;

(2) the individual receives a notice from ED containing a statement of its findings and informing the individual of the opportunity to contest such findings by submitting documentation demonstrating a satisfactory immigration status within 30 days of receipt of the notice; and (3) 30 days from the date of the individual's receipt of such notice has expired.

5. Effective Dates of the Matching Program.

The matching program will become effective 40 days after a copy of the computer matching agreement, as approved by the Data Integrity Board of each agency, is sent to Congress and OMB, unless the requested ten-day waiver is approved by OMB or unless OMB objects to some or all of the agreement, or 30 days after publication of this notice in the Federal Register, whichever date is later. The matching program will continue for 18 months after the effective date and may be extended for an additional 12 months thereafter, if the conditions specified in 5 U.S.C. 552a(o) (2) (D) have been met.

6. Address for Receipt of Public Comments or Inquires.

Ms. Marya Dennis, Management and Program Analyst, U.S. Department of Education, Federal Student Aid, Union Center Plaza, 830 First Street, NE., Washington DC 20002-5345. Telephone: (202) 377-3385. If you use a telecommunications device for the deaf (TDD), you may call the Federal Relay Service at 1-800-877-8339.

Individuals with disabilities may obtain this document in an alternative format (e.g., Braille, large print, audiotape or computer diskette) on request to the contact person listed in the preceding paragraph.

Electronic Access to This Document

You may view this document, as well as all other documents of this Department published in the Federal Register, in text or Adobe Portable Document Format (PDF) on the Internet at the following site:
www.ed.gov/news/fedregister.

To use the PDF you must have Adobe Acrobat Reader, which is available free at this site. If you have questions about using PDF, call the U.S. Government Printing Office (GPO), toll free, at 1-888-293-6498; or in the Washington, DC, area (202) 512-1530.

Note: The official version of this document is the document published in the Federal Register. Free Internet access to the official edition of the Federal Register and the Code of Federal Regulations is available on GPO access at: <http://www.gpoaccess.gov/nara/index.html>

AUTHORITY: 5 U.S.C. 552a; Pub. L. No 100-503.

Dated:



Lawrence A. Warder
Acting Chief Operating Officer
Federal Student Aid.

COMPUTER MATCHING AGREEMENT
between the
DEPARTMENT OF HOMELAND SECURITY
and the
SOCIAL SECURITY ADMINISTRATION

This computer matching agreement sets forth the responsibilities of the Social Security Administration (SSA) and the Department of Homeland Security (DHS) with respect to disclosure of information for the purposes identified in this agreement. It is executed under the Privacy Act of 1974, 5 U.S.C. 552a, as amended by the Computer Matching and Privacy Protection Act of 1988, as amended, and the regulations and guidance promulgated thereunder.

I. LEGAL AUTHORITY, DEFINITIONS AND PURPOSE

A. Legal Authority

The Privacy Act, 5 U.S.C. 552a, as amended, regulates the use of computer matching by Federal agencies when records in a system of records are matched with other Federal, State or local government records. It requires Federal agencies involved in computer matching to:

1. Negotiate written agreements with the other agency or agencies participating in the matching programs;
2. Obtain the approval of the match agreements by the Data Integrity Boards of the participating Federal agencies;
3. Furnish detailed reports about matching programs to Congress and OMB;
4. Notify applicants and beneficiaries that their records are subject to matching; and,
5. Verify match findings before reducing, suspending, terminating or denying an individual's benefit payments.

As further detailed below, legal authority for the relevant disclosures is contained in sections 202(n) of the Social Security Act ("Act"), as amended by section 412 of Pub. L. 108-203, 1611(f), and 1614(a)(1) of the Act (42 U.S.C. 402(n)), 1382(f) and 1382c(a)(1) of the Act, and the Immigration and Nationality Act (INA), 8 U.S.C. 1611 and 1612. Section 1631(e)(1)(B) of the Act, 42 U.S.C. 1383(e)(1)(B), requires SSA to verify declarations of applicants for and recipients of SSI payments before making a determination of eligibility or payment amount. Section 1631(f) of the Act (42 U.S.C. 1383(f)) requires Federal agencies to provide SSA with information necessary to verify SSI eligibility or benefit amounts or to verify other information related to these determinations. In addition, section

202(n)(2) of the Act specifies that the "Attorney General or Secretary" [of the Department of Homeland Security] notify the Commissioner of Social Security when certain individuals are removed under specified provisions of section 237(a) or under section 212(a)(6)(A) of the INA.

B. Definitions

1. "**Act**" means Social Security Act, as amended.
2. "**INA**" means Immigration and Nationality Act.
3. "**Disclose**" and "**disclosure**" means the release of information with or without the consent of the individual, or as otherwise authorized by the Privacy Act of 1974 as amended, 5 U.S.C. 552a, by either DHS or SSA.
4. "**Removed**" means individuals who were deported from the United States under section 241(a) of INA in effect before April 1997, or removed from the United States under section 237(a) or section 212(a)(6)(A) of the INA in effect as of April 1997.
5. "**DHS**" means the Department of Homeland Security.
6. "**MBR**" means Master Beneficiary Record.
7. "**NH**" means the number holder or the owner of the social security number; i.e., the person to whom the social security number has been assigned.
8. "**RSDI**" means the Retirement, Survivors and Disability Insurance programs governed by Title II of the Act.
9. "**SSA**" means the Social Security Administration.
10. "**SSI**" means the Supplemental Security Income Program. SSI is the Federal program established under Title XVI of the Act to provide benefits to aged, blind and disabled individuals with income and resources below levels established under that title.
11. "**SSR**" means Supplemental Security Record.
12. "**SSN**" means Social Security Number.
13. "**SAVE**" means Systematic Alien Verification for Entitlements Program.
14. "**VIS**" means Verification Information System. VIS is the database utilized by the SAVE program to maintain updated information about the current immigration status of certain individuals.

15. “**DACS**” Deportable Alien Control System is the database utilized by ICE to track relevant information of aliens in removal proceedings that includes closure of case, bond information, any court action and disposition of case.
16. “**Pub. L. 108-203**” means the Social Security Protection Act of 2004.

C. Purpose of the Matching Program

The purpose of this agreement is to establish the conditions, safeguards and procedures for the disclosure of information relating to aliens for matching purposes by DHS and SSA. DHS will disclose two separate data files through a computer matching operation for SSA’s use in making federal benefit eligibility determinations as follows:

1. Aliens who Leave the United States Voluntarily

SSA will use one data file in identifying resident aliens who are SSI recipients and who have left or plan to leave the United States for any period of 30 consecutive days. DHS will disclose information from the Computer Linked Application Information Management System (CLAIMS) to SSA to identify those resident aliens who may be ineligible for benefits because they have been outside the United States for 30 consecutive days during the benefit period.

Resident aliens are entitled to SSI benefits for any month in which they reside in the United States. An individual is ineligible to continue to receive SSI benefits in the event he or she resides outside the United States for any period of 30 consecutive days. See section 1611(f) of the Act and 20 CFR § 416.1327. If an individual is absent from the United States for 30 consecutive days, section 1611(f) of the Act also provides that he/she be treated as remaining outside the United States until he/she has been in the United States for a period of 30 consecutive days.

2. Aliens Who are Removed from the United States

Section 202(n)(1)(A) of the Act prohibits payment of retirement or disability insurance benefits to number holders (NHs) who have been removed from the U.S. on certain grounds specified under section 237(a) or under section 212(a)(6)(A) of the INA. No monthly retirement and/or disability benefit may be paid to such NHs for the month after the month in which SSA is notified by the Secretary of Homeland Security that the NH has been removed or before the month in which the NH is subsequently lawfully admitted to the United States for permanent residence. SSA will use a second data file provided by DHS to determine NHs who have been removed and, thus, who may be subject to nonpayment of their Social Security retirement and/or

disability benefits or suspension of their SSI payments.

Section 202(n)(1)(B) of the Act prohibits payment of auxiliary or survivors benefits to certain individuals who are entitled to such benefits on the record of a NH who has been removed from the United States on certain grounds as specified in the above paragraph. Nonpayment of benefits is applicable for any month such auxiliary or survivor beneficiary is not a citizen of the United States and is outside the United States for any part of the month. Benefits cannot be initiated (or resumed) to such auxiliary or survivor beneficiaries who are otherwise subject to nonpayment under these provisions until the removed NH has been subsequently lawfully admitted to the United States for permanent residence. In addition, removals within this second data file may be subject to suspension of their SSI benefits under section 1614(a)(1)(B)(i) of the Act, which provides, in part, that an SSI recipient must be a resident of the United States. Further, if an SSI recipient is not a U.S. citizen, 8 U.S.C 1611 and 1612 of the INA provide that an alien who is not a qualified alien within the statutory definitions applicable to those sections is ineligible for SSI benefits, and those who are qualified aliens will have their eligibility severely restricted.

The removal file will be used to identify aliens whose SSI benefits may be subject to these eligibility requirements, and who may under these requirements, as opposed to earlier requirements in section 1614 of the Act, be ineligible for SSI as a result of their status as removals.

As the recipient agency using the results of the match in its programs, SSA will publish the required Privacy Act Notice of this matching program in the Federal Register.

The SSA component responsible for the matching activity is the Office of Income Security Programs. The SSA component responsible for alien policy questions is the Office of Income Security Programs (for voluntary absences from the United States and removals involving SSI recipients) and the Office of International Programs (for removals involving RSDI claimants and recipients). The DHS components are the U.S. Citizenship and Immigration Services (CIS), Office of Service Center Operations (OSCO), and Immigration and Customs Enforcement (ICE), Office of Detention and Removal (ODR).

II. JUSTIFICATION AND ANTICIPATED RESULTS

A. Justification

Computer matching is believed to be the most efficient and comprehensive method of collecting and comparing this information. There is no other administrative activity that could be employed to accomplish the same purpose with the same degree of efficiency or accuracy.

B. Anticipated Results

1. Aliens Who Leave the United States Voluntarily

One intent of this match is to identify those resident aliens who should have their SSI benefit payment suspended because they have voluntarily left the United States for a period of 30 consecutive days or more. Savings will result from the withholding of SSI benefits by performing this matching program. SSA expects to save \$726,500 annually from cases suspended and put into nonpayment status.

2. Aliens Who are Removed from the United States

The second intent of this match is to identify NHs whose Title II Social Security retirement and/or disability benefits (and under certain conditions the benefits of their dependents or survivors) should be stopped under section 202(n) of the Act because the NHs have been removed from the United States on certain grounds specified in section 237(a) or under section 212(a)(6)(A) of the INA.

This match will also identify individuals who, by virtue of their status as removals, may be ineligible for SSI benefits, because they no longer meet certain SSI eligibility requirements that an SSI recipient be a resident of the United States and (1) a U.S. citizen, (2) a qualified alien eligible under 8 U.S.C. 1611, or (3) for periods prior to the effectiveness of 8 U.S.C. 1611 and 1612, an alien meeting the criteria under section 1614(a)(1)(B)(i) of the Act that an alien be lawfully admitted for permanent residence or otherwise permanently residing in the United States under color of law. SSA expects to save \$7.8 million in overall RSDI/SSI benefits annually by performing this matching program. The expansion of section 202(n) as amended by Pub. L. No. 108-203, section 412, to apply NHs removed from the United States under section 237(a) or under section 212(a)(6)(A) will materially expand the number of individuals who are subject to nonpayment of their Social Security Title II RSDI benefits, thus enhancing the savings derived from the matching program.

3. Matching Agreement Benefits and Costs:

The benefits of this matching operation include the detection and recovery of retroactive overpayments, the avoidance of future overpayments due to changes in the recurring benefit amount.

The costs of developing the match results for Title II were \$26,125 with an annual savings of \$1,146,000, resulting in a benefit-to-cost ratio of 43.9 to 1. For Title XVI the costs were \$221,033 which provided a benefit savings of \$726,511 resulting in a benefit-to-cost ratio of 3.3 to 1. The combined annual benefit savings for Title II and Title XVI were \$1,872,500 with a total cost of

\$247,158 resulting in a benefit-to-cost ratio of 7.6 to 1. (See page 20 for the complete cost benefit analysis for this agreement.)

III. DESCRIPTION OF THE RECORDS TO BE MATCHED

A. Systems of Records and Specific Elements Used

1. Aliens who Leave the United States Voluntarily (Title XVI)

Systems of Records:

The DHS system of records used in the match is the Computer Linked Application Information Management System (CLAIMS), Justice/INS-013, most recently published at 62 FR 59734 (November 4, 1997) which is electronically formatted for transmission to SSA. SSA systems of records used in this portion of the matching program are the Master Files of Social Security Number (SSN) Holders (NUMIDENT), SSA/OEEAS 60-0058 full text published at 71 FR 1795,1815 (January 11, 2006), and the Supplemental Security Income Record and Special Veterans Benefits (SSR/SVB), SSA/ODSSIS 60-0103 full text published at 71 FR 1795,1830 (January 11, 2006).

Specific Data Elements Used:

The Data Elements Furnished by the DHS CLAIMS System (Justice/INS 013) are:

The alien's name, SSN, date of birth, alien identification number, date of departure and expected length of stay. To verify the SSN, CLAIMS data will be matched against the names, DOB, and SSNs of SSA's Numident and Alpha Index files. Verified SSNs will be stored and matched against the same elements in SSA's SSR files.

2. Aliens who are Removed from the United States (Title XVI, SSI and Title II, RSDI)

System of Records:

The DHS system of records used in the match is the Deportable Alien Control System (DACS) Justice/INS-012, full text published at 65 FR 46738, (July 31, 2000) modified at 66 FR 6672, (January 22, 2001), electronically formatted for transmission to SSA. DACS is scheduled to be replaced by the Enforce Removal Module (EREM).

SSA systems of records used in this portion of the matching program are the Master Files of Social Security Number Holders (NUMIDENT), SSA/OEEAS 60-0058 full text published at 71 FR 1795, 1815 (January 11, 2006), and the

Master Beneficiary Record (MBR), SSA/OEEAS 60-0090, full text published at 71 FR 1795, 1826 (January 11, 2006), and the SSR/SVB, SSA/ODSSIS 60-0103, full text published at 71 FR 1795, 1830 (January 11, 2006).

Under an existing Interagency Agreement (IAA) between the agencies, SSA has automated access to the DHS Systematic Alien Verification for Entitlements (SAVE) program that utilizes the Verification Information System (VIS), DHS-USCIS-004 72 FR 17569 (April 13, 2007). This system provides information on the current immigration status of aliens who have Alien Identification Numbers ("A" numbers). SSA will utilize the automated access to the SAVE program, as discussed further in the "Verification" section of the agreement, to verify current immigration status of aliens both where the immediate DACS (Justice/INS-012) match or any future claims activity indicate an alien has been deported. The parties do not consider this verification as a separate match subject to the provisions of the Computer Matching and Privacy Protection Act (CMPPA); such verifications will be conducted in compliance with the terms of the aforementioned IAA.

Specific Data Elements Used:

The data elements furnished by DACS (Justice/INS 012) are the removals name and alias (if any), SSN (if available), DOB, sex, country of birth, country to which removed, date of removal, the final removal charge code and DHS "A" number.

To verify the SSN, DACS data will be matched against SSA's Numident and Alpha-Index files (60-0058). Verified SSNs are matched against the existing MBR and SSR records to locate removals (and their dependents or survivors, if any) who have already claimed and are currently receiving RSDI and/or SSI benefits. Data verified through this matching program will also be retained on the MBR (SSA/OEEAS 60-0090), to be associated with future claims activity. (When an RSDI or SSI claim is filed on a Social Security record where DHS has previously reported a removal via this match program, a remark on the claimant's earnings record will alert operational personnel responsible for adjudicating the claim to the removal involvement).

B. Number of Records Involved

1. Aliens who Leave the United States Voluntarily

The electronic files provided by DHS to SSA will annually contain approximately 250,000 records of aliens who have left the United States voluntarily as described above in section III.A.1 and will be matched against 8.5 million records on the SSR.

2. Aliens who are Removed from the United States

The electronic files provided by DHS to SSA will annually contain approximately 63,000 records of removed aliens as described above in Section III.A.2 that will be matched against approximately 40 million records on the MBR and 7.2 million records on the SSR.

IV. PROCEDURES FOR INDIVIDUALIZED NOTICE

SSA will provide direct notice, in writing, to all applicants at the time of application for SSI or RSDI benefits that their records will be matched against those of other agencies to verify their eligibility or payment amount and similar periodic notice will be provided to all SSI and RSDI benefit recipients at least once during the life of the match. SSA notices will be provided in Spanish and English where there is a Hispanic Indicator on the MBR. The same notice printed in English is included in the mailing. This periodic notification is accomplished in a variety of ways.

For example, both of the following include computer-matching notification:

- a. The annual Cost of Living Adjustment (COLA) notice received by all RSDI beneficiaries; and,
- b. The COLA notice received annually by SSI recipients.

SSA will also publish specific notices of this matching program in the FR, in accordance with the requirements of the Privacy Act and applicable OMB guidelines.

V. VERIFICATION AND OPPORTUNITY TO CONTEST

A. Verification

1. Aliens Who Leave the United States Voluntarily

SSA will make all efforts required under 5 U.S.C. 552a(p) to verify match information pertaining to an affected person, before taking any action based on this match.

SSA will not take any action to deny, reduce, suspend or terminate SSI payments based solely on data obtained from this match. Match results indicating that an alien has notified the DHS of his intent to be absent from the country for a period of time that would make him ineligible for benefits will trigger a multi-step verification process by SSA which includes requesting a report from the individual of the information necessary to determine the alien's continuing eligibility or to determine the correct amount of benefits payable.

2. Aliens Who are Removed from the United States

SSA will not take any action to deny, reduce, suspend or terminate any benefit based solely on removal data obtained from this match. In RSDI cases where discrepant information may be produced by SSA alert development, SSA will verify status through VIS/SAVE. For instance, when necessary, SSA will request or conduct further development (including secondary verification, where appropriate) if the VIS/SAVE database and the removal report generated as part of this match are inconsistent with respect to the NH's current immigration status or there is some other indication that the removal report is incorrect or does not apply to the NH. In cases where the VIS/SAVE database or other information immediately available to SSA is sufficient to establish that suspension of RSDI benefits under the removal provisions is not warranted, benefits will continue without further development.

In SSI cases under sub-sections 1 and 2 above, SSA will make personal follow-up requests prior to suspending benefits when individuals do not respond to requests. These attempts typically include telephone contacts, inquiries with landlords and employers, service agencies, etc. The purpose of these inquiries is to obtain information on whether the individual actually departed the country, the length of his absence from the United States and whether the individual re-established residency. SSA offers assistance to the individual, as needed, to comply with information requests. Any subsequent action to adjust, suspend or terminate benefits will be based upon the outcome of these efforts.

B. Opportunity to Contest

Before taking any adverse action based on the information received from the match and SAVE verification, SSA agrees to provide all individuals for whom SSA decides such adverse action is necessary with the following information:

1. Aliens Who Leave the United States Voluntarily

- a. Where SSA has received information pertaining to the alien's absence from the United States which indicates that specified adverse action is necessary, the specific information that indicates the necessity for adverse action will be provided to the individual receiving Title XVI SSI payments.
- b. The individual receiving Title XVI SSI payments has 10 days from the date of the notice to contact SSA and contest the adverse decision. (See 20 C.F.R. § 416.1336.)
- c. Unless the individual notifies SSA otherwise within the time period specified, SSA will conclude that the data provided by DHS is correct and will make the necessary adjustment to the individual's SSI benefits.

2. Aliens Who are Removed from the United States

- a. Where SSA has received information from DHS pertaining to the alien's removal from the United States that indicates that specified adverse action is necessary, the specific information, which indicates the necessity for the adverse action will be provided to the individual receiving Title XVI SSI payments.
- b. The individual receiving Title XVI SSI payments has 10 days and the individual receiving Title II RSDI benefits has 30 days from the date of the notice to contact SSA and contest the adverse decision.
- c. Unless the individual notifies SSA otherwise within the time period specified, SSA will conclude that the data provided by DHS is correct and will make the necessary adjustment to the individual's RSDI or SSI benefits.

VI. PROCEDURES FOR RETENTION AND TIMELY DESTRUCTION OF IDENTIFIABLE RECORDS

A. Aliens Who Leave the United States Voluntarily

SSA will retain the identifiable records received from DHS only for the period of time required for any processing related to the matching program and will then destroy the records as soon as the information has served the matching program's purpose, by means of demagnetization. Information verified as a result of this program may be retained in the individual's file folders in order to meet evidentiary requirements. In the latter instance, each agency will retire identifiable records in accordance with a National Records and Archives Administration (NARA) approved record retentions schedule subject to applicable retention requirements, DHS may retain one copy of the information provided to SSA as its record of disclosure in accordance with the disclosure accounting and retention requirements of subsections (c)(1) and (c)(2) of the Privacy Act, as amended, 5 U.S.C. 552 a(c)(1) and (2).

B. Aliens Who are Removed from the United States

SSA will retain the identifiable records received from DHS only for the period of time required for any processing related to the matching program and will then destroy the records as soon as the information has served the matching program's purpose, by means of demagnetization. Under applicable legal retention requirements, SSA will retain the identifiable records verified through this matching program on the MBR unless, SSA deletes them because:

1. It is established that the DHS/SSA data match was incorrect and the NH on the SSA record is not the same person as the individual reported by DHS to

have been removed or,

2. Documentation is submitted to establish the NH was lawfully admitted to the United States for permanent residence subsequent to the removal. When necessary, removal information will be retained in the individual's file folders in order to meet evidentiary requirements. In the latter instance, each agency will retire evidentiary records in accordance with a NARA approved record retentions schedule subject to applicable retention requirements.

Subject to applicable retention requirements, DHS will retain one copy of the information provided to SSA as its record of disclosure in accordance with the disclosure accounting and retention requirements of Privacy Act, as amended, 5 U.S.C. 552a(c)(1) and(2).

VII. PROCEDURES FOR SECURITY

Both SSA and DHS agree to comply with the requirements of the Federal Information Security Management Act (FISMA) (Pub. L. 107-347, title III, section 301) and OMB M-06-16 as they apply to the electronic storage and transport of records, especially those records containing Personally Identifiable Information (PII), between agencies and the internal processing of records received by either Agency under the terms of this agreement. Both SSA and DHS reserve the right to conduct onsite inspections to monitor compliance with FISMA and OMB M-06-16 requirements during the life of this agreement. DHS agrees to uphold SSA's Information and Systems Security Guidelines for Federal, State and Local agencies receiving electronic information from SSA. The DHS official responsible for the DHS systems security and oversight of this agreement is listed under Section XV – DHS Systems Contacts.

The SSA will use the DHS data supplied in the manner prescribed by this agreement and will maintain proper safeguards to prevent unauthorized release or use of all data supplied. These safeguards include:

A. Administrative Safeguards

Access to the records matched and to any records created by the match will be restricted to only those authorized employees and officials who need it to perform their official duties in connection with the uses of the information authorized in this agreement. Further, all personnel who will have access to the records matched and to any records created by the match will be advised of the confidential nature of the information, the safeguards required to protect the records and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.

B. Physical Safeguards

The records matched and any records created by the match will be stored in a

physically secure environment in which entry is restricted and security surveillance is constant. Access to the record storage area is limited to authorized personnel who must display a photo-identification pass or confidential electronically coded magnetic strip identifier prior to entry. The electronic data record storage area is maintained to required standards of temperature and humidity.

Only authorized personnel will transport the records matched and created by the match. Such transport shall be under appropriate safeguards consistent with the manner in which the records are stored and processed.

C. Technical Safeguards

The records matched and any records created by the match will be processed under the immediate supervision and control of authorized personnel in a manner which will protect the confidentiality of the records so that unauthorized persons cannot retrieve any such records by means of computer, remote terminal, or other means

Systems personnel must enter personal identification numbers (PINs) when accessing data on the system. In addition, they must possess prior clearance through the TOP SECRET electronic security system for any areas which are accessed. Authorization is strictly limited to those electronic record areas required by the work of the authorized analyst.

D. Safeguarding and Reporting Responsibilities for Personally Identifiable Information (PII)

1. SSA will encrypt all data on mobile computers/devices which carry agency data. Data encryption shall meet National Institute of Standards and Technology (NIST) standards.
2. SSA will allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.
3. SSA will use a "time-out" function for remote access and requiring user re-authentication after 30 minutes inactivity.
4. SSA will log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All data erasures shall meet NIST standards.
5. SSA will establish procedures to ensure that when an SSA employee becomes aware of the possible or suspected loss of PII, they will notify the Systems Security contact immediately following the discovery of the incident.

E. Application of Policy and Procedures

SSA shall also utilize policies and procedures to ensure that information contained in records used or created in the matching operation shall be used solely as provided in this agreement. DHS reserves the right to make arrangements with SSA for onsite inspections or for other appropriate arrangements for auditing compliance with the terms of this agreement.

F. Onsite Inspection

The Data Integrity Board (DIB) of each party to this agreement reserves the right to monitor compliance of systems security requirements and to make onsite inspections for purposes of auditing compliance, if needed, during the lifetime of the agreement or any 12-month extension of this agreement.

VIII. RECORDS USAGE, DUPLICATION AND REDISCLOSURE RESTRICTIONS

SSA agrees to the following limitations on the access to and disclosure of Information provided pursuant to this agreement:

- A. That the files provided by DHS as part of the matching program will remain the property of DHS, and will be handled as indicated in section VI of this agreement once any processing under this matching program is complete.
- B. That the data supplied by DHS and the records created by the match will be used and accessed by SSA only for the purposes of, and to the extent necessary, in the matching program created by this agreement.
- C. That SSA will not duplicate or disseminate the data provided by DHS unless essential to the conduct of the matching program or required by law. Prior to making such redisclosure, SSA will give notice to DHS and obtain approval of DHS's DIB. SSA must specify in writing what records are being disclosed and to whom and identify the statutory authority requiring redisclosure or explain how the redisclosure meets the "essential" standard established under the Privacy Act and interpreted in OMB guidance.
- D. Other than for purposes of a particular match under this program, no file will be created that consists of information concerning only matched individuals.

IX. ACCURACY ASSESSMENTS

Based on internal consistency checks, annual accuracy studies, comprehensive development and evidentiary documentation conducted prior to creation of a payment record, and ongoing information from the client population, it has been determined that the SSA systems of records used in the matching program are more than 99 percent accurate. DHS maintains complete and accurate data through a

process of data reconciliation that ensures data integrity.

X. ACCESS BY THE COMPTROLLER GENERAL

The Government Accountability Office (Comptroller General) may have access to all SSA and DHS records, as necessary, in order to verify compliance with this Agreement.

XI. ADDITIONAL FUNCTIONS TO BE PERFORMED

There are no additional functions to be performed.

XII. REIMBURSEMENT

Due to the nominal costs of services associated with providing data to SSA under this agreement, DHS waives recovery of the costs pursuant to the Economy Act (31 U.S.C. 1535).

XIII. EFFECTIVE DATE; DURATION AND MODIFICATION OF AGREEMENT

This agreement shall be effective no sooner than 30 days after SSA publishes a Computer Matching Notice in the Federal Register or 40 days after notice of this matching program is transmitted to Congress and the Office of Management and Budget, whichever occurs later. This agreement may be renewed at the end of 18 months for a period of time not to exceed 12 months, subject to the requirements of the Privacy Act, as amended, including the requirement that each agency must certify to the responsible DIB that: (1) the matching program will be conducted without change; and (2) the matching program has been conducted in compliance with the original agreement. If either agency does not want to renew this agreement, it should notify the other of its intention not to renew at least 90 days before the end of the agreement period. This agreement may be modified by written modification to this agreement that satisfies both parties and is approved by the DIB of each agency. This agreement may be terminated at any time with the consent of both parties. Either party may unilaterally terminate this agreement upon written notice to the other party, in which case the termination shall be effective 90 days after the date of the notice or at a later date specified in the notice.

XIV. INTEGRATION

This agreement constitutes the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties or promises made outside of this Agreement. This agreement shall take precedence over any other documents that may be in conflict with it.

XV. PERSONS TO CONTACT

Department of Homeland Security Contacts:

Matching Program Issues - ICE

Susan M. Mathias, Attorney
Immigration Customs Enforcement (ICE)
OPLA
Department of Homeland Security
Room 6100
425 I Street N.W.
Washington D.C. 20536
(202) 514-9697 (Tel)
(202) 514-8044 (Fax)
Email: Susan.Mathias1@dhs.gov

Systems Issues - USCIS

Jeff Conklin
Chief Information Officer
Office of Information Technology
United States Citizenship and Immigration Services
Suite 5000
111 Massachusetts Ave, NW
Washington, DC 20529
(202) 272-1700
Jeff.Conklin@dhs.gov

Michael Aytes
Associate Director Domestic Operations
United States Citizenship and Immigration Services
20 Massachusetts Avenue, NW
Washington, DC 20529
(202) 272-1710
Michael.Aytes@dhs.gov

DHS Privacy Office POC

Ken Hunt
Secretary, Data Integrity Board
Privacy Office
Department of Homeland Security
Washington, DC 20528
(703) 235-0762 (Telephone)

(703) 235-0442 (Fax)

ken.hunt@dhs.gov

Legal Issues – DHS General Counsel

Mike Russell

Deputy Associate General Counsel, General Law Division

Office of the General Counsel

Department of Homeland Security

Washington, DC 20528

(202) 447-3526 (Telephone)

(202) 447-3111 (Fax)

mike.russell@dhs.gov

Social Security Administration Contacts:

Agreement and Computer Matching Issues

Ashley Siguenza

Office of Income Security Programs

Social Security Administration

RRCC #0080

6401 Security Blvd.

Baltimore, MD 21235

(410) 965-9877 (Telephone #)

(410) 597-0841 (FAX)

Email: ashley.siguenza@ssa.gov

Policy and Program Issues

Aliens Leaving the United States Voluntarily

Mary Dougherty

Office of Income Security Programs

Social Security Administration

RRCC #0104

6401 Security Boulevard

Baltimore, MD 21235

(410) 965-5999 (Telephone #)

(410) 597-0146 (FAX)

Email: Mary.Dougherty@ssa.gov

Jim D. Anderson
Office of Income Security Programs
Social Security Administration
RRCC #0205
6401 Security Boulevard
Baltimore, MD 21235
(410) 966-3661 (Telephone #)
(410) 966-5366 (FAX)
Email: Jim.D.Anderson@ssa.gov

Aliens Removed (who Leave Involuntarily) from the United States

Cecilia M. Bramford
Office of International Programs
Social Security Administration
West High Rise
6401 Security Boulevard
Baltimore, MD 21235
(410) 965-7383 (Telephone #)
(410) 966-7025 (FAX)
Email: Cecilia.M.Bramford@ssa.gov

Systems Issues

Mark Dailey, Branch Chief
Office of Systems Analysis
Social Security Administration
3402 Operations Building
6401 Security Boulevard
Baltimore, MD 21235
(410) 966-7849 (Telephone #)
(410) 966-3147 (FAX)
Email: Mark.Dailey@ssa.gov

AUTHORIZED OFFICIAL'S SIGNATURE

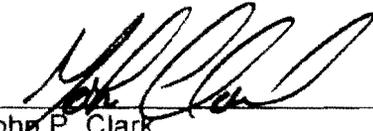
[Signature]

OFFICIAL SECURITY ADMINISTRATION

[Signature]

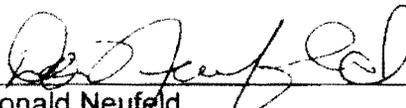
[Signature]

DEPARTMENT OF HOMELAND SECURITY

BY 

John P. Clark
Deputy Assistant Secretary,
Immigration and Customs Enforcement

Date 6-12-07

BY 

Donald Neufeld
Acting Associate Director, Domestic Operations,
Citizenship and Immigration Services

Date 6/11/07

BY 

Hugo Teufel III
Chairman, Data Integrity Board
Department of Homeland Security

Date June 8, 2007

Attachment

Cost Benefit Analysis (CBA) for the Computer Matching Operation (Match #1010) Between SSA and the Department of Homeland Security (DHS)

Number of Alerts Released in FY 2006: (Title II ... REMOVED 305)
(Title XVI ... LEFT THE U.S. 1,697 AND REMOVED 52)

<u>Benefits</u>	<u>Title II</u>	<u>Title XVI</u>	<u>Combined</u>
<u>Left the U.S. for 30+ Days:</u>			
<u>Retroactive Overpayments</u>			
Percent of Alerts with Retroactive Overpayments	12%		12%
Number of Alerts with Overpayments	204		204
Average Overpayment	\$ 1,763		\$ 1,763
Total Overpayment (Projected)	\$359,652		\$359,652
Amount Expected to Recover (60%)	<u>\$215,791</u>		<u>\$215,791</u>
<u>Suspension of Monthly Payment Amount</u>			
Percent of Alerts with Suspension of Monthly Payment	7%		7%
Average Suspended Monthly Payment Amount	\$600		\$600
Total Suspension of Ongoing Monthly Payments Projected for 6 months	\$ 71,400		\$ 71,400
	<u>\$428,400</u>		<u>\$428,400</u>
<u>Removed from the U.S.:</u>			
<u>Suspension of Monthly Payment Amount</u>			
Percent of Alerts with Suspension of Monthly Payment	45.3%	26.9%	42.6%
Average Suspended Monthly Payment Amount	\$ 692	\$ 490	\$ 673
Total Suspension of Ongoing Monthly Payments Projected for 12 months	\$ 95,496	\$6,860	\$102,356
	<u>\$1,145,952</u>	<u>\$82,320</u>	<u>\$1,228,272</u>
Total Benefits	\$1,145,952	\$726,511	\$1,872,463
	<u>Title II</u>	<u>Title XVI</u>	<u>Combined</u>
<u>Costs</u>			
Systems Costs (Office of Systems)	\$10,110	57,969	\$ 68,079
PSC/FO Alert Development Costs	\$16,015	\$152,144	\$168,159
Overpayment Development/Recovery/Processing Costs		\$ 10,920	\$ 10,920
Total Costs	<u>\$26,125</u>	<u>\$221,033</u>	<u>\$247,158</u>
Benefit-to-Cost Ratio	43.9:1	3.3:1	7.6:1

COMPUTER MATCHING AGREEMENT
BETWEEN
THE UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES (CIS)
AND
THE NEW YORK DEPARTMENT OF LABOR

PART I: GENERAL TERMS AND CONDITIONS

A. PURPOSE AND DESCRIPTION

This memorandum constitutes an Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and the New York Department of Labor (NY-DOL). The purpose of this Agreement is to provide the NY-DOL with electronic access to immigration status information contained within DHS-USCIS' Verification Information System (VIS) that will enable the NY-DOL to determine whether an applicant is eligible for benefits under the Unemployment Compensation (UC) program administered by the NY-DOL.

This Agreement describes the respective responsibilities of USCIS and the NY-DOL for verifying immigration status, preserving the confidentiality of, and safeguarding information received from the other party pursuant to the verification procedures. The requirements of this Agreement will be carried out by authorized employees and/or contractor personnel of DHS-USCIS and the NY-DOL.

B. FUNCTIONS TO BE PERFORMED

DHS-USCIS agrees to make available and maintain, as part of the Verification Division Systematic Alien Verification for Entitlements Program (SAVE), an immigration status verification system, which provides information on aliens' immigration status.

DHS-USCIS agrees to provide NY-DOL through the automated system, the following information on each alien inquiry as appropriate: DHS-USCIS generated verification number, last name, first name, date of birth, country of birth, date of entry, immigration status data, and, in some cases, certain other biographical data that may relate to the alien number or work authorization.

DHS-USCIS agrees to provide NY-DOL with instructional materials required for the use of DHS-USCIS' verification system, a sufficient number of primary verification user codes to assure the effective implementation of the verification procedures, and instructions for obtaining necessary system access codes.

DHS-USCIS agrees to provide assistance to the NY-DOL on policies and procedures for use of the system including technical instructions for accessing the system, requirements for safeguarding information contained in the system, and restrictions on disclosure of system information. DHS-USCIS also agrees to provide the NY-DOL with the name, address and telephone number of an appropriate point of contact (POC) within DHS-USCIS, or its contractor organization, who can be contacted regarding any billing questions or problems which arise in connection with the NY-DOL's participation in the Verification program.

The NY-DOL agrees to provide the alien number of the applicant seeking a benefit from the NY-DOL for the purposes of primary (automated access) verification. If an alien's records are not initially located as a result of primary verification, DHS-USCIS will send a message seeking additional verification data from the NY-DOL. The additional/secondary verification process requires the agency to submit a copy of the applicant's immigration documentation along with a Document Verification Form G-845 or provide an electronic description of the applicant's immigration document which may further assist an Immigration Status Verifier in checking all necessary indices and DHS files before providing the NY-DOL with immigration status information. This data may include the type of document presented by the applicant to the NY-DOL, the expiration date of the document, document description, last name, first name, middle name, and or also known as a/k/a of the applicant, applicant's date of birth, I-94 (DHS arrival/departure document), applicant's employment history data, NY-DOL case number and/or other special comments.

The NY-DOL agrees to provide a liaison with DHS-USCIS to resolve any questions regarding this Agreement and to provide assistance to DHS-USCIS to facilitate the provisions of accurate immigration status verification information.

C. SAFEGUARDS REGARDING THE USE AND DISCLOSURE OF INQUIRY DATA

The VIS shall be used in a manner that protects the individual's privacy to the maximum degree possible, and shall not be used in a manner that will allow for discrimination based on race, color, creed, national origin, sex, or disability.

The parties agree to comply with applicable Privacy Act (5 U.S.C.552a, et. seq.) restrictions and requirements in the conduct of the verification procedures under the Agreement, as well as, in the safeguarding, maintenance and disposition of any information received under this Agreement. The NY-DOL also agrees to protect information regarding non US citizens and/or non Lawful Permanent Residents (LPRs) in accordance with New York State Public Officers Law, Article 6-a (the "Personal Privacy

Protection Law”), New York State Labor Law §537 and, to the maximum extent applicable, the provisions of the Privacy Act. The NY-DOL also agrees to comply with any additional requirements that may be imposed by other applicable Federal benefit program regulations.

The NY-DOL agrees not to delay, deny, reduce, or terminate any applicant/recipient’s UC benefits because of that individual’s immigration status based solely on a response received from the DHS-USCIS Verification Division’s primary (automated) system or based upon any additional verification check that may be pending. No adverse action shall be taken unless the NY-DOL has received a response from the DHS-USCIS Verification Division that “additional verification” procedures were conducted and indicate that the applicant does not have the type of immigration status that makes him or her eligible for the benefit and the individual has been afforded the opportunity to refute any adverse information as provided in PART II of this Agreement.

DHS-USCIS reserves the right to use information received by it from the User Agency for any purpose permitted by law, including but not limited to the prosecution of violations of Federal criminal law.

DHS-USCIS may terminate this MOU without prior notice if deemed necessary because of a requirement of law or policy, upon a determination by DHS-USCIS that there has been a breach of system integrity or security by the User Agency, or a failure by the User Agency to comply with established procedures or legal requirements.

The NY-DOL agrees to immediately notify the SAVE Program whenever there is cause to believe an information breach has occurred as a result of User Agency action or inaction pursuant to Office of Management and Budget (OMB) Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” which concerns safeguarding and responding to the breach of personally identifiable information.

Nothing in this MOU is intended, or should be construed, to create any right or benefit, substantive or procedural, enforceable at law by any third party against the United States, its agencies, officers, or employees.

PART II: COMPUTER MATCHING ACT REQUIREMENTS

INTRODUCTION

The purpose of this section of the Agreement is to comply with the Computer Matching and Privacy Protection Act of 1988 (CMPPA), Public Law 100-503, 102 Stat. 2507 (1988), which was enacted as an amendment to the Privacy Act of 1974 (5 U.S.C. 552a,

et. seq.). The requirements of this Section pertain only to alien applicants for, or recipients of, benefits administered by the NY-DOL who have been accorded lawful permanent resident status by DHS-USCIS and to United States citizens whose records are included in VIS, as described in Section H below. Pursuant to the Department of Homeland Security's Privacy Policy Guidance Memorandum 2007-1, to the extent practicable, privacy protections afforded to US Citizens and LPRs shall be afforded to non LPRs and non citizens.

The CMPPA applies when computerized comparisons of Privacy Act records contained within a Federal agency's databases and the records of another organization are made in order to determine an individual's eligibility to receive a Federal benefit. The CMPPA requires the parties participating in a matching program to execute a written agreement specifying the terms and conditions under which the matching program will be conducted.

DHS-USCIS has determined that the status verification checks to be conducted by the NY-DOL using the VIS database is a "computer matching program" as defined in the CMPPA.

A. TITLE OF MATCHING PROGRAM

The Title of this matching program as it will be reported by Department of Homeland Security, to Congress, and the Office of Management and Budget is as follows: Verification Division DHS-USCIS/NY-DOL.

B. MATCHING AGENCIES

1. Source Agency: Department of Homeland Security: United States
Citizenship and Immigration Services
2. Recipient Agency: New York Department of Labor

C. PURPOSE AND LEGAL AUTHORITIES

Section 121 of the Immigration Reform and Control Act (IRCA) of 1986, Public Law 99-603, as amended by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), Public Law 104-193, 110 Stat. 2168 (1996), requires DHS to establish a system for the verification of immigration status of alien applicants for, or recipients of, certain types of benefits as specified within IRCA, and to make this system available to state agencies that administer such benefits. Section 121(c) of IRCA, amends Section 1137 of the Social Security Act and certain other sections of law that pertain to Federal entitlement benefit programs and requires state agencies administering these programs to use DHS-USCIS' verification system in making eligibility

determinations in order to prevent the issuance of benefits to those alien applicants who are not entitled to program benefits because of their immigration status. The VIS database is the DHS-USCIS system which has been established and made available to the NY-DOL and other covered agencies for use in making these eligibility determinations.

The NY-DOL seeks access to the information contained in DHS-USCIS' VIS database, for the purpose of confirming the immigration status of alien applicants for, or recipients of, benefits it administers, in order to discharge its obligation to conduct such verifications pursuant to Section 1137 of the Social Security Act and New York Unemployment Insurance Law Article 18, Title 7, section 590.

D. JUSTIFICATION AND EXPECTED RESULTS

It has been determined by the parties that a computer matching program is the most efficient and expeditious means of obtaining and processing the information needed by the NY-DOL to verify the immigration status of alien applicants for, and recipients of, entitlement benefits. It is expected that this matching program will enable the NY-DOL to rapidly confirm the benefit eligibility of alien applicants/recipients with proper immigration status, to identify those applicants who require further checks to confirm proper eligibility status, and to identify and prevent improper payments to those applicants whose immigrant status does not entitle them to receive the benefits administered by the NY-DOL.

It has been determined that available alternatives to the use of a computer matching program for verifying immigration status would impose a much greater administrative burden (i.e., be much more labor intensive), would result in higher annual administrative costs, and would protract the average query response time. The anticipated savings to be derived from the use of the electronic verification program including administrative costs and savings derived by eliminating fraudulent benefit payments is \$2,406,972.00 based on FY 2006 savings. Using a computer matching program, the NY-DOL is able to process, in an extremely expeditious manner, a higher volume of queries with reduced overall labor demands. DHS-USCIS will provide once daily responses to NY-DOL batch inquiries.

Additionally, because of the rapid response capability provided by this computer matching program this program will have a greater deterrent effect on applicants seeking to fraudulently receive entitlement benefits administered by the NY-DOL, as compared to a much slower mail-in procedure. One of the major objectives of IRCA, to reduce incentives for illegal aliens to come to and remain in the United States, is furthered by this matching program's deterrent effect. Finally, this system also supports efforts to curb waste, fraud, and abuse within Federally funded entitlement programs.

E. RECORDS DESCRIPTION

1. Records to be matched:
 - a. Records in the DHS-USCIS VIS database which contain information on the status of aliens and other persons on whom DHS-USCIS has a record as an applicant, petitioner or beneficiary. See Systems of Records Notice, 72 F.R. 17569.
 - b. the NY-DOL records pertaining to alien applicants for, or recipients of, entitlement benefit programs administered by the NY-DOL.
2. Data elements:
 - a. Data element contained within the NY-DOL's records to be matched with DHS-USCIS VIS database:
 1. Alien Registration Number
 - b. Data elements contained within DHS-USCIS' records to be matched the NY-DOL data may consist of the following:
 1. Alien Registration Number
 2. Last Name
 3. First Name
 4. Date of Birth
 5. Country of Birth (not nationality)
 6. Social Security Number (if available)
 7. Date of Entry
 8. Immigration Status Data
 9. Employment Eligibility Data
3. Number of records: On a monthly basis, approximately 13,000 records from the NY-DOL will be matched against DHS-USCIS VIS database which consists of more than 110 million records.
4. Duration of the program: Eighteen months from the effective date of this Agreement.

F. NOTICE PROCEDURES

DHS-USCIS agrees to publish in the Federal Register a notice of this matching program as specified in the CMPPA and the Office of Management and Budget CMPPA

implementing guidance.

As required by 5 U.S.C. 552a(o)(1)(D) the NY-DOL will provide periodic notice to applicants for and recipients of financial assistance or payments under the Federal benefit program(s) covered by this Agreement that any information they provide may be subject to verification through matching programs.

In New York, individuals can file a new UI claim either by calling the Telephone Claims Center's toll-free number or by filing through the Department of Labor's website, www.labor.state.ny.us.

For those individuals who file a claim by telephone, the first step in the process is automated. The individuals answer a series of questions by either using the key-pad on their telephone or speaking their answers into the telephone receiver. After this automated portion is completed, the call is transferred to a claims representative who verifies the name and address of the claimant and the last employer and any other required information.

Those who file on-line enter answers to questions that appear on the computer screen. When the individual has provided all requested information, he/she submits the claim by selecting the "Submit Claim" button. All individuals who file a claim on-line are shown a confirmation page. If the claim cannot be completed on-line, the confirmation page advises the individual to call the Telephone Claims Center to speak to a claim representative to complete the application.

Regardless of whether a claim is completed on line or by telephone, a monetary determination is mailed to the claimant on the next business day. Also, on the following business day, an Unemployment Insurance Information for Claimants handbook is mailed to the individual. This handbook specifically advises the claimant that their immigration status will be verified by matching against the DHS-USCIS database.

G. VERIFICATION PROCEDURES

1. The NY-DOL may not suspend, terminate, reduce, or make a final denial regarding the Federal benefit program eligibility of an applicant covered by this part based on that individual's immigration status, or take other adverse action against such individual as a result of information produced by the matching program until information has been independently verified. The DHS-USCIS' "additional verification procedures" as described in its M-300 SAVE Users Manual, a copy of which is provided to each user upon execution of this Agreement.
2. Furthermore, the NY-DOL may not suspend, terminate, reduce, or make a final denial regarding the Federal benefit program eligibility of any individual described in paragraph 1, or take other adverse action against such individual as a result of

information produced by this matching program unless: (a) such individual has received notice from the NY-DOL containing a statement of the findings of the immigration status check; and (b) until the subsequent expiration of any notice period provided by such program's law or regulations, or 30 days, whichever is later. Such opportunity to contest may be satisfied by the notice, hearing, and appeal rights governing the Federal benefit program and the applicant has been provided the opportunity to refute any adverse status information as a result of this verification inquiry. The exercise of any such rights shall not affect any rights available under this section.

H. RECORDS RELATING TO UNITED STATES CITIZENS

This Agreement authorizes the NY-DOL to use the Verification Division's system for the purposes of verifying the immigration status of alien applicants for UC benefits. Nothing in this Agreement authorizes the NY-DOL to use the DHS-USCIS system for the purposes of verifying the status of any individual claiming United States citizenship by birth. However, in addition to records relating solely to aliens, VIS contains records relating to former lawful permanent resident aliens who have become naturalized United States citizens. It is possible that applicants for UC may on occasion, through fraud or error, present documentation identifying themselves as lawful permanent resident alien without informing the NY-DOL that they have become a United States citizen, thereby resulting in a NY-DOL inquiry in VIS.

In the event that DHS-USCIS receives a request for a verification of a NY-DOL applicant who is a LPR or a United States Citizen, the request will be referred to a DHS-USCIS Immigration Status Verifier for additional verification procedures. All safeguards and protections provided by CMPPA, Privacy Act, and this Agreement regarding the use, disclosure, and security of DHS-USCIS records apply to DHS-USCIS records regarding United States citizens to the same extent as to the DHS-USCIS records relating to lawful permanent resident aliens. Pursuant to the Department of Homeland Security's Policy, privacy protections afforded to United States Citizens and LPRs shall be afforded to non LPRs and non citizens.

I. DISPOSITION OF MATCHED ITEMS

Matching records that the NY-DOL receives from DHS-USCIS will be retained for a period of 60 days beyond the completion of all actions relating to the verification process (including any such necessary related actions as reviews, appeals, investigations, prosecutions, overpayment recoupments, etc.) and then will be destroyed by NY-DOL. All matching records that DHS-USCIS receives from the NY-DOL will be returned with any of DHS-USCIS records that are matched after automated disclosure accounting audit records have been generated. The parties agree that information generated through the match will be destroyed as soon as possible after it has served the matching program's

purposes and all applicable legal retention requirements, i.e., applicable requirements of the UC program for the NY-DOL, and applicable requirements of the Privacy Act for DHS-USCIS.

J. SECURITY SAFEGUARDS

DHS-USCIS agrees to safeguard information it receives from the NY-DOL in connection with status verification inquiries in accordance with the Privacy Act of 1974 (5 U.S.C. 552a), the Immigration Reform and Control Act of 1986, other applicable statutes, and the requirements of this Agreement between the parties.

DHS-USCIS agrees to safeguard the information provided by the NY-DOL in accordance with DHS-USCIS disclosure standards and to provide the name of DHS-USCIS program inspector responsible for compliance with these standards. Individuals who wish to obtain copies of records pertaining to themselves resulting from queries submitted to DHS-USCIS, may do so by following the Freedom of Information Act and Privacy Act procedures that can be found at www.uscis.gov. DHS-USCIS also agrees to limit access to NY-DOL provided information to individuals responsible for the verification of the alien's immigration status or who require access to the information to perform necessary support functions or follow-up actions.

The contractor data facility where the NY-DOL and DHS-USCIS information is stored complies with requirements of the Department of Homeland Security, National Security Systems Policy Directive 4300B. It is a secure facility accessed only by authorized individuals with properly coded key cards, authorized door keys or access authorization. There is a security guard force on duty 24 hours a day, 7 days a week. The building is protected against unauthorized access, unauthorized use of equipment, or removal of storage media and listings. Employees at the facility have undergone background checks in order to be granted clearance and are provided access badges.

The NY-DOL agrees to safeguard information it receives from DHS-USCIS under the verification process in accordance with the requirements of the Privacy Act (5 U.S.C. 552a), and applicable Federal and state entitlement benefit program record retention and disclosure requirements.

The NY-DOL also agrees to limit access to information to those individuals responsible for the verification of the alien's immigration status or who require access to the information to perform necessary support functions. The NY-DOL will restrict further dissemination of the information unless required in connection with state or the Federal entitlement program law enforcement responsibilities.

The NY-DOL has taken measures to secure information received from DHS-USCIS for

purposes of the matching program in accordance with applicable State and Federal entitlement program rules procedures. The NY-DOL's offices are located in secure buildings, and access to premises is by official identification. All records are stored in government controlled buildings which are locked during non-duty office hours. Many records are stored in cabinets or machines which are also locked during non-duty office hours. Access to automated records is controlled by user identification and passwords.

The computer security systems used by both DHS-USCIS and the NY-DOL offer a high degree of resistance to tampering and circumvention. Multiple levels of security are maintained within their computer system control program. Both security systems limit access to authorized personnel strictly on a "need-to-know" basis, and control an individual user's ability to access and alter records within the system. All users are given a unique ID with personal identifiers and interactions with the system are recorded.

K. RECORDS USE, DUPLICATION AND REDISCLOSURE RESTRICTIONS

The parties agree to comply with the data maintenance and disclosure control requirements specified within Part I of this Agreement. The parties agree not to duplicate or disclose any records received from the other party pursuant to this matching agreement, except where it is necessary to verify the immigration status of alien applicants for, or recipients of, the UC benefit programs administered by the NY-DOL (including follow-up actions). Additionally, if the matching program uncovers evidence of fraudulent claims or the use of fraudulent immigration documents, the parties may redisclose the records as necessary to conduct law enforcement investigations or prosecutions or as otherwise required by law.

L. RECORDS ACCURACY ASSESSMENT

DHS-USCIS currently estimates that information within its VIS database is 90-95% accurate in reflecting immigration status, but continues to undertake various actions to further improve the quality of the VIS database. In addition, in cases where immigration status is not confirmed through VIS, additional verification procedures are used, which allows DHS-USCIS to check all necessary indices and files before providing the NY-DOL with immigration status information. This process includes procedures for DHS-USCIS to correct any errors detected in the immigration status information.

M. COMPENSATION

The User Agency shall pay the standard billing rates in accordance with the terms of the reimbursement Memorandum of Agreement (MOA) addendum to the MOU and arrange the obligations, processes and methods related to the payment of required fees to DHS-USCIS and/or its authorized agents.

The current standard billing rates are attached to the MOA. The standard billing rates and methods of payment are subject to change upon prior written notification to the User Agency.

N. COMPTROLLER GENERAL ACCESS

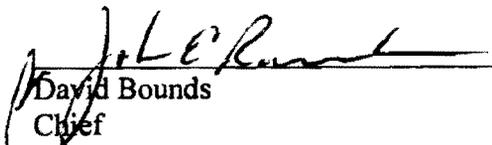
The GAO (Comptroller General) may have access to all of the matching records of the NY-DOL and DHS-USCIS necessary to verify compliance with the requirements of the CMPPA.

O. EFFECTIVE DATE

This Agreement will become effective 40 days after a report concerning the computer matching program has been transmitted to the Office of Management and Budget (OMB) and transmitted to Congress along with a copy of the Agreement, or 30 days after publication of a computer matching notice in the Federal Register, whichever is later. The Agreement (and matching activity) will continue for 18 months from the effective date, unless within 3 months prior to the expiration of this Agreement, the Data Integrity Board approves a one-year extension pursuant to 5 U.S.C. 552a (o)(2)(D).

P. SIGNATURES

The undersigned are officials of DHS-USCIS and the NY-DOL who are authorized to represent their agencies for purposes of this Agreement.


David Bounds
Chief
Benefits Operations
Verification Division
United States Citizenship and Immigration
Services


Mario Musolino
Executive Deputy Commissioner
New York State
Department of Labor

Date: 10/21/08

Date: 9/15/08

Q. DEPARTMENT OF HOMELAND SECURITY
DATA INTEGRITY BOARD APPROVAL

Approved 
Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security

Date 1-16-09

“Computer Matching Agreement between the United States Citizenship and Immigration Services (DHS-USCIS) and the New York Department of Labor (NY-DOL).”



Privacy Impact Assessment
for the

Information Sharing Fellows Program

April 14, 2008

Contact Point

Rob Riegle

**Director, State and Local Programs
Intelligence and Analysis**

Reviewing Official

Hugo Teufel III

Chief Privacy Officer

**Department of Homeland Security
(703) 235-0780**

Abstract

Pursuant to Section 512 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (the Act), Public Law No. 110-53, the Department of Homeland Security has established the Homeland Security Information Sharing Fellows Program. Under the program, State, local, and tribal law enforcement (LE) officers (LEOs) and intelligence analysts will be detailed to DHS to participate in the work of the Office of Intelligence and Analysis (I&A). The Act requires the Department to complete a concept of operations (CONOPS) for the program, including a privacy impact assessment (PIA). The CONOPS must also include a Civil Liberties Impact Assessment, which will be conducted by the DHS Office for Civil Rights and Civil Liberties.

Introduction

The Secretary, acting through the Under Secretary for Intelligence and Analysis and in consultation with the Department's Chief Human Capital Officer, Chief Privacy Officer, and Civil Rights and Civil Liberties (CRCL) Officer, is tasked with establishing the Homeland Security Information Sharing Fellows program.

The purpose of the program is to detail State, local and tribal LEOs and intelligence analysts to the Department to participate in the work of I&A in order to become familiar with both the relevant missions and capabilities of the Department and other Federal agencies, and the role, programs, products, and personnel of I&A. In addition, the program is designed to promote information sharing between the Department and State, local, and tribal LEOs and intelligence analysts by assigning such officers and analysts to:

- (1) serve as a point of contact in the Department to assist in the representation of State, local, and tribal information requirements;
- (2) identify information within the scope of the information sharing environment (ISE) that is of interest to State, local, and tribal LEOs, intelligence analysts, and other emergency response providers;
- (3) assist Department analysts in preparing and disseminating products derived from information within the scope of the ISE that are tailored to State, local, and tribal LEOs and intelligence analysts, and designed to prepare for and thwart acts of terrorism; and
- (4) assist Department analysts in preparing products derived from information within the scope of the ISE that are tailored to State, local, and tribal emergency response providers, and assist in the dissemination of such products through appropriate Department channels.

While the Fellows program seeks to promote and enhance information sharing between DHS and State, local, and tribal governments, the Fellows will not share information with their parent jurisdictions. Information sharing under the purview of the program will continue through established DHS processes, which are subjected to prior privacy agreements.

Eligible fellows must be currently employed as a LEO or intelligence analyst and have homeland security-related responsibilities. Fellows will be detailed to DHS in accordance with the Intergovernmental Personnel Act (IPA) (5 USC 3371-3375; 5 CFR 334). Fellows will be under the

direct supervision of DHS management and subjects them to applicable Federal laws and regulations, including those related to the protection of individual privacy. The Fellows will be required to complete appropriate privacy and civil liberties training, as designated by DHS, prior to beginning fellowship duties. Additionally, as the Fellows will be either LEOs or intelligence analysts, this training will augment their existing privacy and civil liberties training, including compliance with 28 CFR 23, Criminal Intelligence Systems Operating Policies as well as the Intelligence Oversight and US Person handling procedures.

This program has been designed to minimize privacy concerns. The Fellows are brought on to review DHS intelligence programs and identify ways and types of information that can improve sharing with State, local, and tribal LE partners. The privacy concern that arises when building such a program is that information will be shared inappropriately and informally between the Fellow and the respective parent jurisdiction. This risk has been mitigated in two ways:

- (1) Clearly stating that the Fellows must follow all the roles and responsibilities current I&A employees. This includes making the Fellows fully aware of the privacy requirements under the law and under DHS Policy, and regularly reminding the Fellows of these requirements.
- (2) I&A has set up the program so that Fellows will review minimal Personally Identifiable Information (PII), and instead will review other types of information.

This PIA will be updated to reflect any relevant changes in the Information Sharing Fellows program over time. In addition, DHS will issue a report on the privacy and civil liberties impact of the program, not later than one year after the program is implemented.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002, Section 222(a)(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. These principles first appeared in the Secretary's Advisory Committee on Automated Personal Data Systems within the Department of Health, Education, and Welfare ("HEW Report"), which was the basis for the passage Privacy Act. The FIPPs account for the nature and purpose of the information being collected, maintained, used, and disseminated in relation to DHS' mission to preserve, protect, and secure. They are: Transparency; Individual Participation; Purpose Specification; Minimization; Use Limitation; Data Quality and Integrity; Security; and Accountability and Auditing.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that the Homeland Security Information Fellows Program is a program rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs.

1. Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). Technologies or systems using PII must be described in a system of record notice (SORN) and PIA, as appropriate. There should be no system the existence of which is a secret to the general public.

The Homeland Security Information Sharing Fellow program, as described in the CONOPs will not change the way PII is gathered, collected, used, maintained, or disseminated by DHS. It is recognized that, during the tenure of the Fellowship, a Fellow could identify information collection types that would enhance the cooperation with State, local, and tribal homeland security and LE partners and are outside the scope of the I&A SORN. In this case, I&A, in coordination with the DHS Privacy Office, will review the existing privacy documentation to ensure that appropriate notice has been provided that the information can be shared in this manner. If documentation needs to be updated to provide sufficient notice, DHS will update the appropriate documents prior to the commencement of sharing of the information.

Information collected, used, maintained, or disseminated by I&A to meet its mission requirements under the Homeland Security Act has been described with appropriate routine uses in the existing Homeland Security Operations Center (HSOC) database SORN. (DHS/IAIP-001, April 18, 2005, 70 FR 20061).

2. Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS' use of PII.

As noted above in Principle 1, the Information Sharing Fellows Program will not change the way information is gathered, collected, used, maintained, or disseminated by I&A or DHS. The Fellow will review the general practices of I&A to identify areas where appropriate sharing with State, local, and tribal homeland security and LE partners could be more effective.

As a matter of policy and practice, individuals can submit a formal Privacy Act request for their information. Although certain records in the system of records were exempted from

certain provisions of the Privacy Act, DHS will review each request to ensure that the information meets the requirements of the exemptions of the Privacy Act.

Generally, the information collected, used, maintained, and disseminated by I&A is exempted from the Privacy Act requirements of access, correction, and redress. The exemptions are appropriate because providing access could inform the subject about the existence of an investigation or other lawful exercise of departmental authority. Access to the records could permit the individual who is the subject of a record to impede an investigation and avoid detection or apprehension. Additionally, information held by I&A may include properly classified information, the release of which would pose a threat to national security and/or foreign policy.

3. Purpose Specification

Principle: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purposes for which the PII is intended to be used.

The information gathered, collected, used, maintained, or disseminated by I&A or DHS is done so consistent with its statutory authority, and will not be impacted by the Information Sharing Fellows Program. As noted above, fellows will review the general practices of I&A to identify areas where appropriate sharing with the State, local, and tribal homeland security and LE partners could be more effective.

I&A through its SORNs specifies its authority for gathering and collection of information, and states the purposes that the information will serve.

4. Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish specific lawful purpose(s) and only retain PII for as long as necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

As a member of the Intelligence Community under Executive Order 12333, I&A must minimize U.S. Person information in both collection and ongoing maintenance. I&A must review its holdings of PII regularly to ensure that the information is properly collected and still needs to be maintained. When sharing information, I&A must minimize the U.S. Person information to comply with both EO 12333 and the Privacy Act so that only individuals with a “need to know” are provided access to the PII.

While I&A is minimizing the information it maintains, I&A has exempted its system of records from requirements of the Privacy Act that require agencies only to collect information that is relevant and necessary.¹ This exemption is necessary because it is not always possible for DHS to know in advance what information is relevant and necessary in the course of its intelligence, counterterrorism, or investigatory efforts. In the context of the authorized intelligence,

¹ 5 USC 552(a)(e)(1).

counterterrorism, and investigatory activities undertaken by DHS personnel, relevance and necessity are questions of analytic judgment and timing, such that what may appear relevant and necessary when acquired ultimately may be deemed unnecessary upon further analysis and evaluation. For this reason, the review and deletion process are an important aspect of DHS' privacy program. Constraining the initial acquisition of information included within I&A could discourage the appropriate receipt of and access to information, which could impede DHS efforts to fulfill its mission.

Notwithstanding this claimed exemption, which would permit the acquisition and temporary maintenance of records whose relevance to the purpose of the ERS may be less than fully clear, DHS will only disclose such records after determining whether such disclosures are consistent with published Privacy Act routine uses.

5. Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose that complies with the purpose for which the PII was originally collected.

The Information Sharing Fellow will not change the way information is used by I&A or DHS. The Fellows will consider the types of information that are currently not available to State, local, and tribal partners and could be used more effectively. In considering recommendations, I&A will work with the Privacy Office to determine the best course of action to ensure that only appropriate information is shared for compatible purposes.

6. Data Quality and Integrity

Principle: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

As noted above in Principle 1, the Information Sharing Fellow will not change the way information is gathered, collected, used, maintained, or disseminated by I&A or DHS. As also noted under Principles 2 and 4, I&A has exempted itself from certain aspects of the Privacy Act as it relates to data quality and integrity. I&A, as required by EO 12333, has specific policies and processes in place that require I&A to review the information regularly to ensure that the information meets the legal requirements of I&A.

7. Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

As noted above in Principle 1, the Information Sharing Fellow will not change the way

information is gathered, collected, maintained, used, or disseminated by I&A or DHS. Therefore, the protocols around securing the information are not impacted.

8. Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The Information Sharing Fellows will not change the way information is gathered, collected, used, maintained, or disseminated by I&A or DHS; however, it will be incumbent upon DHS and I&A to ensure that Fellows are fully trained and understand the rules for the period of time they are detailed to I&A. Fellows will receive appropriate privacy and civil rights and civil liberties training before beginning their detail to DHS, and regularly throughout their tenure.

Additionally, at the completion of their detail to I&A, Fellows will be reminded of their ongoing duties to protect any information in the appropriate required de-briefing.

Conclusion

I&A has designed the Information Sharing Fellows Program in such a way as to minimize the impact on privacy. The Information Sharing Fellow will not change the way information is gathered collected, used, maintained, or disseminated by I&A or DHS. The only discernible privacy risk with the program is that the Fellow will share information informally and inappropriately with his employer. This risk will be mitigated with initial and ongoing privacy training.

Responsible Officials

Program Manager:
Rob Riegle
Director, State and Local Programs
Intelligence and Analysis



Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security



Privacy Impact Assessment
Organizational Shared Space (OSS)
May 1, 2008

Contact Point

(b)(6)

**Program Executive Officer
Information Sharing and Knowledge Management Division
Intelligence and Analysis
Department of Homeland Security**

(b)(6)

Reviewing Official

**Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780**

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION. AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.



Abstract

The Department of Homeland Security (DHS), Intelligence and Analysis' (I&A) Organizational Shared Space (OSS) is a virtual protected area on the Joint Worldwide Intelligence Communications System (JWICS) network. OSS is used for the retention of intelligence products and their dissemination to other Intelligence Community (IC) consumers. I&A has conducted this privacy impact assessment (PIA) because some of the documents stored on the OSS contain personally identifiable information (PII).

Introduction

Background

The OSS project was initiated via a grant from the Director of National Intelligence (DNI) to facilitate the move of the DHS website from the IC Enterprise Services (ICES) Office (formerly the Intelink Management Office) to a DHS-owned and managed hosting solution.

I&A Mission and Requirements

DHS's role within the IC is to facilitate information sharing and conduct appropriate research and analysis to support information sharing between DHS components, DHS partners, and the IC. I&A has implemented OSS to facilitate its information sharing mission responsibilities per Title II of the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004.

I&A will use OSS to store and retain intelligence products developed by DHS intelligence personnel. OSS will also be used as the primary mechanism to disseminate those products to the IC and intelligence elements within DHS. The OSS will serve as the primary DHS JWICS presence that will be exposed to other intelligence providers. Initially, the OSS portal will host an internally and externally accessible repository of finished DHS intelligence products. As new mission applications are deployed, the portal will be used to provide access control for both internal and external users to those classified DHS-managed applications. This means that OSS will be the gateway for I&A users to access other applications to which they have access. Pantheon, which has a previously issued PIA, is currently expected to be made available through the OSS. A final timeline has yet to be finalized. Other applications, however, may precede Pantheon.

OSS Structure

The OSS Portal manages access to I&A's intelligence products (b)(2) High
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]



(b)(2) High
[Redacted text block]



- [REDACTED] (b)(2) High

[REDACTED]

Information Handling Guidelines and Protocols

OSS is a National Security System operating at the TS/SCI level. [REDACTED] (b)(2) High

[REDACTED] All I&A personnel accessing the system are required to attend annual training in security and intelligence oversight policy which includes specialized training on the legal uses of US Persons data and the protection of individual privacy when handling PII. Each I&A employee has signed documents acknowledging the penalties for violation of the rules for handling classified or sensitive information. As such, all I&A users of this data are aware that misuse of the data may result in termination of employment, monetary fines, or incarceration.

There are no specialized training requirements for non-DHS OSS users. However, all IC agency personnel that access the JWICS network, and OSS, which resides therein, conduct regular security, including information security, training, as well as regular training in the principles of Intelligence Oversight and any locally applicable regulations or procedures implementing the requirements of Executive Order 12333.

Because OSS supports intelligence operations and is required to execute on classified networks, the physical and IT security standards are rigorous. [REDACTED] (b)(2) High

[REDACTED]

[REDACTED]



(b)(2) High

Section 1.0 Characterization of the Information

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

(b)(2) High

[Redacted]

[Redacted]

In order to enable the role-based access control provided by the directory infrastructure and PKI, the OSS

(b)(2) High

- [Redacted]

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

The sources of the information contained within the finished DHS intelligence products posted to OSS

(b)(2) High



(b)(2) High Information in OSS may also be received, from organizations and individuals who receive I&A intelligence products, in the form of feedback to the DHS intelligence product. Information can be generally summarized as information related to people, places, things, and events within the statutory purview of I&A.

While the specific origin of the data contained within the intelligence products cannot be quantified, the DHS Chief Intelligence Officer is committed to the quality and accuracy of the posted products. The quality control of these products is managed via a comprehensive pre-publication vetting process that facilitates further critical review of the format and content of a finished DHS intelligence product. Products not meeting these standards are not approved for release.

(b)(2) High [Redacted]

[Redacted]

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

The information which appears within DHS intelligence products that are posted on the OSS is acquired for purposes consistent with DHS and I&A authorities and responsibilities under the Homeland Security Act, and in furtherance of the I&A mission of information sharing. Properly collected and acquired information is posted on the OSS for the purpose of information sharing within and among the elements of the DHS intelligence enterprise, and other federal components, including the larger IC.

(b)(2) High [Redacted]

1.4 How is the information collected?

(b)(2) High [Redacted]



(b)(2) High

[Redacted]

(b)(2) High

1.5 How will the information be checked for accuracy?

The information is accurate to the best knowledge and belief of the reporting officer. To ensure accuracy

(b)(2) High

Moreover, DHS intelligence personnel employ best efforts to ensure that information is accurate;

(b)(2) High

however, a complete description of intelligence and analytic tradecraft is beyond the scope of this document. Finally, all finished DHS intelligence products undergo a thorough vetting process prior to release.

(b)(2) High

Information is subject to the normal Intelligence Oversight processes so it is periodically reviewed

(b)(2) High

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

Legal authority for the collection of information located in OSS is found in the Homeland Security Act of 2002, Public Law 1007-296, §§ 201-202, and Executive Orders 12333 and 13284 (making DHS I&A a part of the IC). In exercising its responsibilities under the Homeland Security Act, I&A is specifically authorized by statute to access and receive (collect) intelligence, law enforcement, and other information from Federal, State, and local agencies and private sector entities, including any relevant reports, assessments, analyses, and unevaluated intelligence that may be collected, possessed, or prepared by any agency of the Federal Government, for purposes of further analysis, integration, and other uses by the Department, and to disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland or

national security, and to agencies of State and local governments and private sector entities with such responsibilities.

In carrying out these activities, I&A must consult with the Director of National Intelligence, other appropriate intelligence, law enforcement, or other elements of the Federal Government, State and local governments, and the private sector, to ensure appropriate exchanges of information are being made. Furthermore, I&A must ensure that any material it receives is protected from unauthorized disclosure and that any intelligence information is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947.

Finally the Homeland Security Act assigns to I&A the responsibility for coordinating support to the elements and personnel of the Department, other agencies of the Federal Government, State and local governments, and the private sector, that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

In addition to relevant provisions of the Homeland Security Act and Executive Order 12333, as amended, the following authorities, arrangements, and agreements also help to define the collection of information which may appear in OSS: Executive Order 13311 (authority of DHS to prescribe and implement classified and unclassified homeland security information sharing procedures); the Memorandum of Understanding Between the IC, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing of March 4, 2003 (framework and guidance to govern homeland security, terrorism, and other related information sharing, use, and handling between DHS and the larger federal community); Homeland Security Presidential Directives/HSPDs 5 (designating the Secretary of DHS as the principal Federal official for domestic incident management under a National Response Plan) and 7 (responsibility of DHS to coordinate and establish systems for sharing homeland security information concerning the protection of critical national infrastructure and key resources); and Executive Order 13388 and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), (which call for the implementation of a terrorism information sharing environment).

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

The amount of PII contained in an intelligence product is the minimum amount of data consistent with mission need. [REDACTED]

(b)(2) High

[REDACTED]

[REDACTED]



(b)(2) High

(b)(2) High

This prevents misuse of data and the propagation of inaccurate data.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

Information stored in the OSS is used:

- To publish finished intelligence products to the JWICS network for use by authorized DHS intelligence personnel and other intelligence agencies with access to JWICS, as appropriate.
- To retrieve and analyze topic specific feedback information on intelligence products. This capability extends the window for vetting to ensure that I&A products meet customer need continuously.
- To authorize users to access applications and services consistent with their level of clearance and administrative access.

Anticipated routine uses by I&A of the products maintained in OSS are consistent with the applicable routine uses published last in the Homeland Security Operations Center Database (HSOC) System of Records Notice (SORN), published as DHS/IAIP-001 on April 18, 2005, and available at 70 Fed. Reg. 20156, and the recently completed draft notice for the I&A Enterprise Records System (ERS) SORN which is expected to be published in the near future. The ERS SORN will replace the HSOC SORN as the governing system of records notice for all I&A systems. Covered routine uses include those which would permit the use of PII for user account holder registration for authorized administrative and auditing purposes.

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

(b)(2) High

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

OSS is simply the repository for finished I&A intelligence products. (b)(2) High



(b)(2) High
Any inquiries into the sources of I&A intelligence products would have to be made to the product originator via the content administrator.

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.

Personnel responsible for creating and publishing finished DHS intelligence products to OSS are assigned authorized analytical tasks and their performance is closely monitored by I&A branch and division chiefs. These individuals are required to attend annual training in the protection and safeguarding of U.S. Persons and privacy related information as part of a mandatory training program on the I&A Information Handling Guidelines and I&A policies concerning Intelligence Oversight. Intelligence products represent the best collective judgment of the DHS intelligence professional. As such, the DHS Chief Intelligence Officer takes a personal interest in ensuring intelligence products posted to JWICS for use by other DHS intelligence personnel and members of the IC reflect well upon the Department and are consistent with DHS intelligence authorities and responsibilities. The comprehensive pre-publication vetting process facilitates further critical review of the format and content of a finished DHS intelligence product. Products not meeting these standards are not approved for release.

(b)(2) High
[Redacted]

[Redacted]

Section 3.0 Retention

3.1 What information is retained?

All of the information described within Section One is retained within OSS.

3.2 How long is information retained?

I&A is in the process of establishing a formal retention schedule with the I&A and DHS Records Officer. As a baseline information is retained in accordance with existing I&A guidelines for information retention. Since this system is intended to be used as a research resource archive for DHS Intelligence personnel and personnel from other intelligence agencies with authorized access, longer term data storage, consistent with I&A information handling guidelines and the requirements and limitations imposed upon records retention



generally under applicable federal law, is required to support historical searches of the data set. Current I&A Intelligence Oversight policies and associated I&A Information Handling Guidelines require review of any U.S. Person information placed on the system by DHS on an annual basis to determine if the information can continue to be retained. When the specified period for retention under law has elapsed, or where the continued retention of U.S. Persons information is not justified, that information is removed and destroyed. DHS Intelligence personnel responsible for creating the record or maintaining the information in the system must complete the required annual review. (b)(2) High

[Redacted]

[Redacted]

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

No, although once a retention schedule is established with the DHS Records Officer a formal submission to NARA will be made.

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

(b)(2) High

[Redacted]

That said, DHS Intelligence personnel perform annual reviews of U.S. person information in OSS and delete the U.S. Person information for which continued retention under applicable information handling guidelines and oversight policies is no longer justified or appropriate. This helps to mitigate the risk that PII will be retained longer than needed.

(b)(2) High

[Redacted]



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?

Intelligence products are shared with other DHS intelligence personnel that have JWICS access. DHS intelligence personnel include personnel assigned to intelligence elements of the United States Coast Guard (USCG), Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), Citizenship and Immigration Services (USCIS), United States Secret Service (USSS), and Transportation Security Administration (TSA). (b)(2) High

DHS Intelligence products are shared as a resource for other DHS intelligence personnel in each of the organizational elements listed in the preceding paragraphs, above, to use for purposes of research and further analysis of intelligence topics and for other intelligence related activities.

User account information is not shared with those organizations via OSS.

4.2 How is the information transmitted or disclosed?

(b)(2) High

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.

The risks to privacy introduced by sharing the data within DHS are appropriately mitigated. Information in OSS is intelligence information maintained entirely on a classified (TS/SCI) system for the primary purpose of being shared among DHS personnel for the performance of their homeland and national security related responsibilities. The intelligence products are specifically prepared and tailored to communicate threat information among DHS intelligence personnel. To the extent U.S. Persons identifying information is included in OSS records, it is because a determination has been made that it is necessary for the potential recipient(s) to understand, assess, or act on the information provided in the record.

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?

(b)(2) High



(b)(2) High

The intelligence products are specifically published to the web for the use of all DHS Intelligence personnel and member elements and personnel of the national IC having a need to know the information in the course of their duties and responsibilities, and the particular missions of their organizations.

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.

DHS Intelligence products are shared in accordance with the HSOC SORN, published as DHS/IAIP-001 on April 18, 2005, and available at 70 Fed. Reg. 20156 (SORN) and, once published, the ERS SORN with other intelligence agencies. The use of the products will be consistent with each receiving agency's authorities and policies concerning the receipt, handling and use of information, for purposes of communicating threat information to those agencies for enabling them to plan a response to those threats, and for research and further analysis of intelligence topics or other authorized national intelligence activities. User account information is not shared with those organizations.

(b)(2) High

There is no specialized training requirements for those non-DHS personnel to whom access to OSS will be granted. However, it is understood that all IC agency personnel that access the JWICS network, and OSS, which resides therein, conduct regular security, including information security, training, as well as regular training in the principles of Intelligence Oversight and any locally applicable regulations or procedures implementing the requirements of Executive Order 12333.

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

(b)(2) High



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

The risks to privacy introduced by sharing of data from OSS with the identified organizations external to DHS are very low. This is finished intelligence information, vetted by senior DHS Intelligence leadership prior to publication, being maintained entirely on a classified (TS/SCI) system for the purpose of being shared with and among intelligence professionals, including personnel belonging to non-DHS organizational elements of the national IC for the performance of their national security related responsibilities. The intelligence products are specifically prepared and tailored to communicate threat and other information to intelligence personnel. To the extent U.S. Persons identifying information is included in any OSS records released to external organizations, it is because a determination has been made that it is necessary for the potential recipient(s) to understand, assess, or act on the information provided in the record in accordance with the procedures outlined in Executive Order 12333.

In addition, access controls ensure that only those users with the required clearances are permitted to view the classified products. Moreover, (b)(2) High This information sharing construct is common across all agencies of the IC and represents one of the principal means by which I&A executes its DHS Intelligence mission.

Section 6.0 Notice

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

(b)(2) High

we are not in a position to address the notice, if any at all, that may be provided directly to that source or subject individual to whom the record pertains. Given the sensitive methods and sources through and from which most intelligence information, including that which potentially identifies U.S. Persons information, is acquired, as well as the sensitive purposes for which that acquired information is used, it would not be appropriate to speculate in this document how, if at all, notice may otherwise be provided to individuals identified in the system.

However, notice generally concerning all intended uses of information by DHS Intelligence systems overseen by I&A is provided in the HSOC SORN, published as DHS/IAIP-001 on April 18, 2005, and available at 70 Fed. Reg. 20156, and the recently completed draft I&A ERS SORN. The ERS SORN will publish in the near future. The ERS SORN will replace the HSOC SORN as the governing system of records notice for all I&A controlled record systems.

Information provided by users for the purposes of establishing user accounts for access to OSS is collected by the user's respective parent intelligence organization, which provides notice on the uses of the information and other restrictions on the use of the JWICS network, on which the OSS resides. For example, in DHS, a written notice on JWICS rules of behavior, Privacy Act usages, and an express notification that all access may be monitored is provided to every user who applies for an account.



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

Persons named in intelligence products have no opportunity to decline to provide information inasmuch as they do not provide that information themselves, and are otherwise not on notice that the particular information has been collected and acquired by I&A. (b)(2) High

[Redacted]

[Redacted]

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

Individuals named in intelligence products do not have the right to consent to the particular uses of the information in OSS. Information published in intelligence products, however, complies in all respects with internal I&A Information Handling Guidelines, and, as specifically concerns the collection, retention, and dissemination of information that identifies U.S. persons, complies fully with I&A policies on Intelligence Oversight, including compliance with all applicable Executive Orders, Director of National Intelligence policies and directives, and other Departmental policies.

(b)(2) High

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.

(b)(2) High

This may represent a risk to privacy, however the limits placed on access to the information and information handling training under EO 12333 provided to the I&A personnel using the data are factors mitigating this privacy risk.

Section 7.0 Access, Redress and Correction

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

Because OSS contains classified and sensitive unclassified information related to intelligence, counter terrorism, homeland security, and law enforcement programs, activities, and investigations, records within it have been exempted from requests for access or amendment by covered individuals to their own information within it, to the extent permitted by the Privacy Act subsection (k) (Sec. 552a of Title 5 of the U.S. Code). Notwithstanding applicable exemptions, DHS reviews all such requests on a case-by-case basis. Where such a request is made, and compliance would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of I&A, and in accordance with procedures and points of contact published in the applicable SORN.

The procedures for submitting FOIA requests for OSS are available in 6 C.F.R. Part 5.

Assistant Secretary Office of Intelligence & Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528
Attn: FOIA Officer
E-mail: FOIAOPS@DHS.GOV

Holders of user accounts can update their information via the JWICS. This community resource updates contact information and PKI certificates.

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

Sometimes erroneous information is published in a finished intelligence product. When incorrect information is discovered, a revised product is published to correct the information or to note the questionable fact or content. The OSS uses **(b)(2) High** content management to maintain version control of the published intelligence products.

As noted above, any requests from the public for information in OSS will be reviewed on a case by case basis in light of the reasons OSS is exempted from certain provisions of the Privacy Act.

OSS user account holders are responsible for the integrity of the data they enter. Should erroneous information be entered, the user is required to correct their entry immediately. **(b)(2) High**



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

Formal notice of the fact that PII may be resident on I&A applications, such as OSS, is provided generally through the HSOC SORN.

For purposes of I&A systems privacy related records, the HSOC SORN will soon be replaced by a new ERS SORN that is currently in draft form under the title "DHS Office of I&A Enterprise Records System."

The procedures for correcting user account information are published to the Intelink Passport web site. Users may also contact their local help desk or system administrator for assistance in correction their account information.

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

Informal redress is provided to an individual requester on a limited basis where compliance with a request would not hinder I&A or DHS operations, the supported activities of other agencies, or otherwise jeopardize a sensitive national or homeland security, law enforcement, or other intelligence investigation.

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

Given the classified nature of the underlying system and the OSS application, a robust program to permit access, review and correction of the raw intelligence data cannot be provided. While this lack of direct access and formal redress mechanisms may represent a theoretical risk to individual privacy, that risk is linked with the heightened sensitivity of and potential harm that could result to the government activities supported, and are mitigated considerably given the inherent information system security protections and controls unique to classified information system within which OSS resides and the applicable policies and mandatory procedures governing the access, collection, retention, use, and dissemination of the PII by I&A personnel.

OSS Portal users are informed as to the uses of their user account information. Multiple methods are available to correct user account information.

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?

(b)(2) High
[Redacted content]



(b) (7) (C) [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

8.2 Will Department contractors have access to the system?

DHS employs contract analysts from several vendors to assist in the analysis of data and preparation of intelligence products and those contractors will have access to the system. In addition, contractors will have access to the system for development, operation and maintenance purposes. Contracts contain proprietary information and are available to authorized personnel via the Office of Procurement Operations.

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

OSS users receive DHS privacy and security training annually and system specific training upon gaining their system accounts. Individual DHS intelligence professionals responsible for publishing finished DHS intelligence products, receiving products and reporting for posting into OSS, and otherwise authorized access to them for later use are each required to attend annual training in the protection and safeguarding of U.S. Persons and privacy related information as part of a mandatory training program on the I&A Information Handling Guidelines and I&A policies concerning Intelligence Oversight.



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

OSS was designed to meet FISMA requirements (b)(2) High

[Redacted]

[Redacted]

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

(b)(2) High

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?

The security controls in place provide adequate protection of privacy, therefore, the privacy risks for this category are considered low. The primary privacy risks associated with the system were related to unauthorized access to the system and improper maintenance and dissemination of information. The systems access risk was mitigated (b)(2) High

[Redacted]

The information maintained within OSS is classified and sensitive and subject to the information handling requirements identified in Executive Order 12333. The mitigation of improper distribution or maintenance of this information is accomplished by the I&A analysts' mandatory annual information handling and intelligence oversight training.

Section 9.0 Technology

9.1 What type of project is the program or system?

OSS is an operational project which provides a virtual protected area that hosts the DHS JWICS website. The site provides a platform upon which intelligence products may be retained or disseminated through authorized access mechanisms to other IC consumers

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

The I&A development contractor, (b)(2) High created the system:

(b)(2) High
[Redacted text block]

The I&A development contractor, (b)(2) High OSS has been deployed and is undergoing its Security Test and Evaluation. OSS was assessed by the I&A Information Technology Review Board and after that evaluation the product acquisition, accreditation and deployment activities were permitted to continue.



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

(b)(2) High

Responsible Officials

(b)(6)
Program Executive Officer
Office of Intelligence & Analysis
Department of Homeland Security

(b)(6)

(b)(6)
Project Manager

(b)(6)

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

John Kropf
Acting Chief Privacy Officer
Department of Homeland Security



Privacy Impact Assessment
for the

Pantheon

Request for Information Management System

December 20, 2007

Contact Point

(b)(6)

**Program Executive Officer
Office of Intelligence & Analysis
Department of Homeland Security**

(b)(6)

Reviewing Official

**Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780**

Abstract

As a member of the Intelligence Community (IC), the Department of Homeland Security Office of Intelligence & Analysis has developed an information technology system called Pantheon. Pantheon’s mission is to enable the Department of Homeland Security (DHS) to share intelligence-based information with DHS components and Communities of Interest (COIs) (i.e. Federal, state, local, tribal, territorial, private sector, intelligence community, and international partners) by implementing a technology solution for responding to requests for information (RFIs) received by I&A. I&A has conducted this privacy impact assessment (PIA) because Pantheon will involve the collection and use of personally identifiable information (PII).

Introduction

DHS’s role within the IC is to facilitate information sharing between DHS components, COIs, and the IC. The Office of Intelligence and Analysis (I&A) has developed Pantheon to facilitate this information sharing requirement.

(b)(2) High

[Redacted]

Pantheon intelligence information, data, and/or products may potentially contain Personally Identifiable Information (PII).

(b)(2) High

[Redacted]

In the future, I&A will evaluate other automated systems and “backbones” for possible adaptation to support the RFI process.

(b)(2) High

Typical Transaction

(b)(2) High

(b)(2) High

(b)(2) High

Use and Handling of Personally Identifiable Information

Even though I&A cannot know when and how PII will be encountered, DHS and I&A have strict protocols as well as IC requirements, which protect any PII associated with an intelligence product. (b)(2) High

I&A can retain control over how PII is labeled and processed. This arrangement complies with the provisions of Executive Order (EO) 12333, *United States Intelligence Activities*, as amended, Intelligence Community Directives (ICDs) 153, *Process for Developing Interpretive Principles and Proposing Amendments to Attorney General Guidelines Governing the Collection, Retention, and Dissemination of Information Regarding U.S. Persons*, 501 Policy on the Use of Dissemination Controls for Intelligence Information, and DHS Management Directive 8202, *Procedures Governing Activities of the Office of Intelligence and Analysis that Affect United States Persons*. These documents along with DHS implementing procedures, define the varied responsibilities, authorities, and limitations within the federal government for the conduct of intelligence activities.

In many ways these procedures mirror privacy laws, and in most instances, EO 12333 and ICD 153 are more restrictive than current privacy laws because they strictly define the boundaries within which IC members can acquire, retain, and utilize U.S. person information.¹ Moreover, prior to disseminating any properly acquired and retained U.S. Person information, I&A personnel must undertake a “minimization” process, whereby the U.S. Person information or identity is evaluated in the context of the request and/or the intended recipient for determining whether disclosure of that specific identifying information is necessary for an understanding of the product. Where such disclosure is not necessary, the identity information will be “masked” by replacing it with “a U.S. Person” (“USPER”). When an I&A product includes U.S. person identifying information, that information will be properly marked as “a U.S. Person” or “USPER,” as appropriate, and the product itself will carry a warning stating that “This document contains U.S. Person Information and should be handled in accordance with E.O. 12333”.

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?

(b)(2) High

may have PII contained within

¹ The definition of a U.S. Person includes a U.S. citizen, an alien known by the intelligence agency to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S. (except for a corporation directed and controlled by a foreign government or governments) Source: E.O 12333, as amended by E.O. 13284, Part 3; Sec. 3.4, Subsec, (g)(5) (i).

them, but the PII related to U.S. Person (USPER) information must be submitted in conformance with applicable executive orders and laws, including EO 12333 and the Privacy Act. PII may include name, date of birth, aliases, and any other information relevant to intelligence activities.

1.2 From whom is information collected?

The information contained in Pantheon may be collected from DHS components and COI partners, including the IC.

1.3 Why is the information being collected?

The information within the Pantheon is being collected to ensure that appropriate information is disseminated to the appropriate agencies in a timely and efficient way and in accordance with the Homeland Security Act, the information sharing environment, the Privacy Act, and any other applicable law or regulation.

1.4 How is the information collected?

(b)(2) High

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

In exercising its responsibility under the Homeland Security Act of 2002, as amended, the National Security Act of 1947, as amended, and Executive Order 12333, as amended, I&A is authorized to disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities. In carrying out this responsibility, I&A must also consult with the Director of National Intelligence, other appropriate intelligence, law enforcement, or other elements of the Federal Government, State and local governments, and the private sector, to ensure appropriate exchanges of information. Furthermore, I&A must ensure that any material it receives is protected from unauthorized disclosure and that any intelligence information is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947. Finally, it is the responsibility of I&A under the Homeland Security Act to coordinate support to the elements and personnel of the Department, other agencies of the Federal Government, State and local governments, and the private sector, that provide information to the Department, or are consumers of information provided by the Department,

in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department. The system called Operational Shared Space (OSS) will directly support all of these activities.

Among the legal authorities, arrangements and agreements that define the information collection are:

The **Homeland Security Act of 2002** (P.L. 107-296), as amended, directs DHS to access, receive and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, state and local government agencies (including law enforcement agencies), and private sector entities; to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center, to aid in terrorism-related analysis; to consult with the Director of National Intelligence and other appropriate intelligence sources to establish priorities and strategies; to appropriately disseminate collected information; to establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence; to have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government; to integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))); and to make available, within the Department and to other departments and agencies of the Federal Government, as appropriate, information provided by State, local, and tribal governments and the private sector, and reviewed and analyzed by the Department.

Executive Order 13311 U.S. Intelligence Activities delegates authorities for prescribing and implementing homeland security and related terrorism information sharing procedures.

Homeland Security Presidential Directive 7 (HSPD-7) Critical Infrastructure Identification, Prioritization, and Protection (2003) orders the Secretary of Homeland Security to establish appropriate systems for the sharing of relevant Homeland security information within and among the identified critical infrastructure sectors.

The Intelligence Reform and Terrorism Prevention Act (IRTPA)(P.L. 108-458) grants authority to Federal agencies for terrorism information sharing, but preserves the authority of the Department with regard to the dissemination of information to state, local and private entities.

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.**

I&A minimizes the amount of PII on Pantheon as required for intelligence products. For intelligence products containing PII on USPERS collected and retained in Pantheon, I&A applies internally developed procedures which implement the Intelligence Oversight requirements of Executive Order 12333, ICD 153, and MD 8202. Prior to the dissemination or external release of that information, I&A employs the process of “minimization” to reduce or, whenever possible, eliminate the need to release any PII, thereby reducing any privacy risks to these individuals. Thus, consistent with its obligations as a member of the Intelligence Community operating under Executive Order 12333, ICD 153, MD 8202 and in accordance with the “Information Handling Guidelines for the Office of Information Analysis” it adopted on Oct. 5, 2005, I&A reviews each intelligence product prior to its dissemination to determine whether the release of information identifying a USPERS is, when evaluated in the context of the request and/or the intended recipient, necessary for an understanding of the product. Where such disclosure is not necessary, the identity information will be “masked” by removing and replacing it with “U.S. Person” or “USPER.” Where an I&A product includes USPER identifying information, that information will be properly marked or otherwise tagged as “USPER.” Further, the product itself will carry a warning stating that “This document contains U.S. Person Information (USPER) and should be handled accordingly,” or words to that effect.

(b)(2) High
I&A will ensure that any information shared or distributed via Pantheon complies with Constitutional, statutory, regulatory, and all other policy requirements as appropriate. This will include applicable privacy and civil liberties standards.

(b)(2) High

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.

(b)(2) High

(b)(2) High

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

(b)(2) High

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

(b)(2) High

(b)(2) High

(b)(2) High

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.

As explained in the introduction (b)(2) High. This ensures Pantheon is being used appropriately not only as a system, but also the information being exchanged is used appropriately. (b)(2) High

(b)(2) High

dissemination of information regarding USPERS as specified in EO 12333, ICD 153, ICD 501, ICD 701, DHS PD 002, and MD 8202. The applicable protections and controls on the treatment and handling of personally identifying information is a core principle of intelligence oversight, upon which US Person information may be collected, retained, and disseminated by I&A personnel only when: 1) it is relevant for the performance of the DHS mission and I&A's responsibilities therein and 2) it properly falls within one of the pre-defined categories of collectability.

Minimization, as a process, occurs only after the initial and proper application of the principles, above, and then only in the event that the information sought by an entity outside I&A would contain USPER information if released in response to a proper request.

(b)(2) High

[Redacted]

With these controls in place, the privacy impact in this category is assessed as low.

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?

Data and information determined to be useful and correct is maintained in the system in accordance with EO 12333, ICD 153, ICD 501, ICD 701, MD 8202, DHS PD 002, DHS Memorandum, and Intelligence Oversight Basics, dated March 27, 2006; and in the Information Handling Guidelines for the Office of Information Analysis, dated October 5, 2005 and other governances as appropriate. This guidance includes reviewing U.S. person information placed in the system by DHS on an annual basis to verify if it is still needed and, if not, the deletion of such information.

(b)(2) High

This system is intended to be used as a research resource for I&A and other intelligence agencies.

(b)(2) High

[Redacted]

[Redacted]

(b)(2) High

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

No. DHS Records Retention has submitted the schedule to NARA but has not received a final approval decision as of the date of this PIA.

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

(b)(2) High

I&A performs annual reviews of U.S. person information and deletes the information if it is no longer needed or permissible to retain under applicable information handling guidelines and oversight policies. This helps to mitigate the risk that personally identifiable information will be retained longer than needed.

User account information is needed to maintain user accounts and provide access to authorized individuals.

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?

Intelligence information, data, and products are shared with DHS components, COIs, the IC, and other entities possessing JWICS access. Specifically, internal DHS components that submit and respond to RFIs are: Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), Customs and Border Protection (CBP), Transportation Security Administration (TSA), and the United States Coast Guard (USCG).

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

RFIs and responses to RFIs are shared with DHS components pursuant to that component's authority to receive the information.

4.3 How is the information transmitted or disclosed?

(b)(2) High

(b)(2) High

[Redacted]

[Redacted]

[Redacted]

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

The risk to privacy is that information will be shared with a component that does not have the authority to collect the information. This risk is mitigated by the fact that [Redacted] (b)(2) High

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?

I&A will receive and task DHS components and other agencies with RFIs. I&A will provide the response to RFIs back to the requesting agency. [Redacted] (b)(2) High

5.2 What information is shared and for what purpose?

RFIs and responses to RFIs are shared with agencies outside DHS pursuant to that agency's authority to receive the information.

5.3 How is the information transmitted or disclosed?

(b)(2) High

[Redacted]

(b)(2) High

[Redacted]

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?

Yes. The MOU is the Memorandum of Understanding between the IC, Federal Law Enforcement and the Department of Homeland Security Concerning Information Sharing, paragraph 3, g, (iii). This is the Homeland Security information Sharing Agreement between DHS, the AG, and the IC, of March 4, 2003 – while limited to terrorism and other defined information, it does provide the proper scope of information shared with other entities and for the appropriate purposes.

5.5 How is the shared information secured by the recipient?

Information shared is secured in accordance with standard USG, DHS, IC standard policy procedures, directives, and memorandums. (b)(2) High

[Redacted]

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

(b)(2) High

[Redacted]

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

The risk to privacy is that information will be shared with an agency that does not have the authority to collect the information. This risk is mitigated by the fact that (b)(2) High [Redacted] to ensure that the requesting agency has the authority to make a request and receive the substantive response.

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?

The purpose of Pantheon is to improve the capability of DHS to collect, retain, and disseminate information, in order to protect the United States from terrorism and other threats to national security, while ensuring its activities are carried out in manner that protects the legal rights, civil liberties, and privacy interests of USPERS. EO 12333 provides that agencies within the IC are authorized to collect, retain, and disseminate information concerning USPERS only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General (AG) (e.g. the Memorandum of Understanding between the IC, Federal Law Enforcement and the Department of Homeland Security Concerning Information Sharing).

All DHS components, partners, and COIs maintain some information sharing request capability; however, each partner possesses different rules, objectives, sources, methods, and standards. Pantheon faces unique challenges responding to RFI's due to these differences.

(b)(2) High

Formal notice of the fact that PII may be resident on I&A applications, such as Pantheon, is provided generally through the Homeland Security Operations Center Database System of Records Notice published April 18, 2005 at 70 FR 20156.

For purposes of I&A systems privacy related records, the HSOC SORN will soon be replaced by a new ERS System of Records Notice (SORN) that is currently in draft form under the title "DHS Office of Intelligence & Analysis (I&A) Enterprise Records System." This SORN has not yet been published to the Federal Register.

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

Persons named in intelligence products have no opportunity to decline to provide information.

(b)(2) High

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?

Individuals named in intelligence products are not provided with a means to limit the use of the information.

(b)(2) High

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

Because Pantheon contains classified and sensitive unclassified information related to intelligence, counter terrorism, homeland security, and law enforcement programs, records within it have been exempted from notification to the extent permitted by subsection (k) of the Privacy Act. Any residual risks to privacy, however low, and which are incapable of being addressed as a result of these applicable exemptions, are nevertheless mitigated by I&A's intelligence oversight framework and obligations there under.

I&A, as a member of the National Intelligence Community, also conducts its mission in conformance with the requirements of Executive Order 12333, as amended, "United States Intelligence Activities," dated December 4, 1981. Section 2.3 of Executive Order 12333 requires that each agency head within the IC establish procedures to govern the collection, retention, and dissemination of information concerning U.S. Persons in a manner which protects the privacy and constitutional rights of U.S. Persons.

Specifically within I&A, intelligence personnel may acquire information which identifies a particular U.S. Person, retain it within or disseminate it from ERS, as appropriate, only when it is determined that the personally identifying information is necessary for the conduct of I&A's functions and otherwise falls into one of a limited number of authorized categories, each of which reflects discrete activities for which information on individuals would be utilized by the Department in the overall execution of its statutory mission.

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?

Because Pantheon contains classified and sensitive unclassified information related to intelligence, counter terrorism, homeland security, and law enforcement programs, records within it have been exempted from access by covered individuals to their own information, to the extent permitted by subsection (k) of the Privacy Act. Notwithstanding applicable exemptions to access, DHS reviews all such requests received on a case-by-case basis. Where a request for access to any specific record in Pantheon is made, and compliance would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived.

Holders of user accounts can update their information within Pantheon.

7.2 What are the procedures for correcting erroneous information?

Sometimes erroneous information is published in a finished intelligence product. (b)(2) High

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Because Pantheon contains classified and sensitive unclassified information related to intelligence, counter terrorism, homeland security, and law enforcement programs, records within it have been exempted from requests for access or amendment by covered individuals to their own information within it, to the extent permitted by subsection (k) of the Privacy Act. Notwithstanding applicable exemptions, DHS reviews all such requests on a case-by-case basis. Where such a request is made, and compliance would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived.

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

Formal notice of the fact that privacy identifying information may be resident on I&A applications, such as Pantheon, is provided generally through the Homeland Security Operations Center Database System of Records Notice published April 18, 2005 at 70 FR 20156.

For purposes of I&A systems privacy related records, the HSOC SORN will soon be replaced by a new ERS System of Records Notice (SORN) that is currently in draft form under the title “DHS Office of Intelligence & Analysis (I&A) Enterprise Records System.” This SORN has not yet been published to the Federal Register.

Because Pantheon contains classified and sensitive unclassified information related to intelligence, counter terrorism, homeland security, and law enforcement programs, records within it have been exempted from notice, access, and amendment by covered individuals to their own information within it, to the extent

permitted by subsection (k) of the Privacy Act. Therefore, no formal procedures exist to allow individuals to correct their information. Notwithstanding applicable exemptions and the absence of formal procedures, DHS will nevertheless review all such requests on a case-by-case basis.

(b)(2) High

Users may also contact their local help desk or system administrator for assistance in correcting their account information.

7.4 If no redress is provided, are alternatives available?

Redress is provided on a limited basis where compliance with a request would not impede I&A operations.

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.**

Notwithstanding DHS' willingness to receive and address requests in writing for notification, access, and amendment by individuals of any non-exempt records in Pantheon which pertain to them, there is no right of redress for individuals named in Pantheon records. Because Pantheon contains classified and sensitive unclassified information related to intelligence, counter terrorism, homeland security, and law enforcement programs, access, correction, and redress rights are not provided in as much as doing so could interfere with or adversely affect the national or homeland security of the United States or sensitive investigatory activities. Nevertheless, DHS attempts to provide as much redress as possible by reviewing such requests on a case by case basis. However, in the intelligence environment redress and access requests are generally not granted.

Users are informed as to the uses of their user account information (b)(2) High

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?

(b)(2) High

[Redacted content]

- [REDACTED] (b)(2) High
[REDACTED]
[REDACTED]

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

DHS I&A contractors will have access to the system [REDACTED] (b)(2) High
[REDACTED]
[REDACTED]

Contracts contain proprietary information and are available to authorized personnel via the Office of Procurement Operations.

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

[REDACTED] (b)(2) High

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

[REDACTED] (b)(2) High
[REDACTED]

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

[REDACTED] (b)(2) High
[REDACTED]

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

[REDACTED] (b)(2) High
[REDACTED]
[REDACTED]
[REDACTED]

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

Pantheon users receive annual Intelligence Oversight and security training. Intelligence Oversight training includes specific instruction pertaining to the handling of personally identifiable information and USPER

data. Upon gaining their system accounts, system specific training is available to users by appointment by calling the I&A Help Desk.

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

Yes. Pantheon was designed to meet FISMA requirements and the associated security requirements. Pantheon is currently going through the security Certification and Accreditation process and has obtained an Interim Authority to Test (IATT). The IATT is required prior to allowing the servers to be connected to a TS/SCI network. Now that the IATT has been issued, Pantheon can complete the Security Test and Evaluation (ST&E) plan required for a full Approval to Operate (ATO).

(b)(2) High

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

The security controls in place provide adequate protection of privacy. (b)(2) High
Information communicated over I&A information technology may be classified. For these reasons, user privileges, user access, and information security were primary interests in the development of Pantheon. Any privacy risks for this category have been significantly mitigated.

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?

(b)(2) High

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

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

(b)(2) High

[Redacted]

9.3 What design choices were made to enhance privacy?

Privacy enhancements include the following design features:

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

- Pantheon is not intended to be a Privacy Act system of records for intelligence information. Pantheon limits the retention of intelligence information, data, and products attached to RFI Responses in accordance with established DHS policies and procedures.



Responsible Official

(b)(6)

Program Executive Officer
Office of Intelligence & Analysis
Department of Homeland Security

(b)(6)

Project Manager

(b)(6)

(b)(6)



Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security



Privacy Impact Assessment

Pathfinder

April 17, 2008

Contact Point

(b)(6)

Program Executive Officer

Information Sharing and Knowledge Management Division

Intelligence and Analysis

Department of Homeland Security

(b)(6)

Reviewing Official

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780

FOR OFFICIAL USE ONLY

~~THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION. AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.~~

Abstract

The Pathfinder Web (Pathfinder) system is an integrated product owned and operated by the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A). Pathfinder is an integrated text search, retrieval, display, and analytic tool suite used to analyze intelligence community (IC) message traffic directed or otherwise addressed to DHS. I&A has conducted this PIA because message traffic analyzed in Pathfinder may contain personally identifiable information (PII).

Overview

I&A Mission and Requirements

DHS's role within the IC is to facilitate information sharing and conduct appropriate research and analysis to support information sharing between DHS components, Communities of Interest (COIs), and the IC. I&A has implemented Pathfinder to facilitate its duties to analyze and research law enforcement, intelligence, and other information and to integrate and organize such information in order to identify, assess, and understand potential threats, including terrorism, against the United States.

I&A plans to use Pathfinder to support the research and analytical needs of its analysts. (b)(2) High

[REDACTED]

[REDACTED] The goal of Pathfinder is to provide intelligence analysts with tools designed by analysts for analysts.

Source Data

(b)(2) High
[REDACTED]

The Pathfinder architecture was designed to be flexible such that the system will be able to accommodate new data sources by simply modifying the routines needed for its data ingestion modules. After deploying the tool operationally within I&A, I&A intends to solicit its users and partners for additional

1 (b)(2) High [REDACTED]

candidate data sources. The integration of any additional data sources within Pathfinder will be coordinated with the DHS Privacy Office and I&A Security prior to inclusion.

Pathfinder Architecture

(b)(2) High

[Redacted]

Pathfinder Search Tools

(b)(2) High

[Redacted]

Utilities included within the PF Web application Pathfinder utilize the repository data in order to provide useful information to the analysts. PF web contains five tools that are delivered to the client as Java applets:

(b)(2) High

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

PFORs are used when the subject sensitivity, speed, and sureness of delivery are important considerations.

(b)(2) High

Security and Information Handling

Pathfinder is a National Security System operating at the TS/SCI level. All personnel using the system have also been read into the Signals Intelligence (SI) and Talent Keyhole (TK), as well as the HCS and Gamma, compartments. (b)(2) High

(b)(2) High

Because Pathfinder supports intelligence operations and is required to execute on classified networks, the physical and IT security standards are quite rigorous. (b)(2) High

(b)(2) High

Section 1.0 Characterization of the Information

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

The term “collection” has a specific meaning in the intelligence community; implying a targeted tasking where human, technological, or other resources are actively used to collect information of specific interest from its originating source. (b)(2) High

(b)(2) High

The information gathered by I&A Pathfinder is limited in this initial release only to information provided (b)(2) High to DHS.

(b)(2) High

(b)(2) High

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

(b)(2) High

, as described in the Introduction and 1.1.

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

(b)(2) High

Specifically, the analysis of intelligence data and message traffic reporting, including, as appropriate, personally identifying data, is essential to DHS and the IC in fulfillment of their respective missions to protect United States national and homeland security.

1.4 How is the information collected?

Pathfinder draws on (b)(2) High

1.5 How will the information be checked for accuracy?

The information acquired by DHS (b)(2) High and otherwise included in Pathfinder is accurate to the best knowledge and belief of the original reporting officer or author of the intelligence product. (b)(2) High

(b)(2) High

(b)(2) High

, but a more complete description of the intelligence and analytic tradecraft involved is beyond the scope of this document.

(b)(2) High

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

DHS I&A's mission and responsibilities, including the authority to collect the information and intelligence from AMHS and other sources and incorporate it into Pathfinder, are derived primarily from EO 12333, as amended, the National Security Act of 1947, as amended, and the Homeland Security Act of 2002, as amended. In the context of these generally applicable authorities, I&A collects information in executing its discrete functional responsibilities, which can be understood as falling within the following categories:

- (1) Terrorist Threats. Ensuring the specific intelligence and analytical responsibilities found in Title II of the Homeland Security Act and involving a nexus to terrorist threats to the Homeland are carried out, including, among others, conducting intelligence analysis, facilitating information and intelligence sharing, and managing intelligence collection priorities;
- (2) Protective and Support Measures. Identifying priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities, where there exists a nexus either to terrorism or other threats to the Homeland.
- (3) Departmental Support. Providing intelligence and information analysis and support to other elements of the Department engaged in authorized missions.
- (4) As Directed by the Secretary. Performing such responsibilities as may be directed by the Secretary and in furtherance of a Departmental mission derived from statutory, regulatory, or other executive authorities.
- (5) As Assigned By Law or Regulation. Activities undertaken in furtherance of duties or responsibilities specifically assigned to the Under Secretary for I&A, or I&A, by statute or regulation.

Unlike most of the IC, I&A's mission has no requirement for a foreign nexus. Even purely domestic threats to the homeland may be appropriate for its analytic efforts, and therefore appropriately acquired into Pathfinder. As is the case with all I&A information "collection," (b)(2) High

so long as they conform to applicable I&A Intelligence Oversight (IO) and Information Handling guidelines.

Prior to utilizing any report or products received **(b)(2) High** or other authorized source, and identified through Pathfinder as potentially responsive to an intelligence need, I&A analysts must review any identified U.S. Person information for the purpose of assessing its relevance to the I&A mission, and for determining whether it fits into one of I&A's approved "collection" categories. As I&A personnel undertake review of any U.S. Person identifying information they encounter, they may temporarily retain it for up to 180 days for the purpose of assessing and determining whether that information may be "collected," and thus permanently retained and, where appropriate, disseminated, under applicable IO procedures to authorized homeland security partners with a need for such information. Where a conclusive determination is made at, or any time within and up to, the expiration of that 180 day period, that this information may not be permanently retained, the identifying information is destroyed immediately.

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

U.S. Person Information within I&A source systems that Pathfinder searches against have been previously assessed for collectability (as defined in relevant law, regulations and protocols as they apply to the IC) pursuant to existing DHS authorities and Intelligence Oversight principles as they apply to I&A. Moreover, all U.S. Person information contained in final products produced by I&A based upon information using Pathfinder must also be minimized pursuant to applicable Intelligence Oversight principles, to ensure that only that U.S. Person identifying information which is necessary for the intended recipient of the product to understand, assess, or act on the information is provided. Otherwise, the PII must be masked or redacted. Thus, the amount of PII actually disclosed in any Pathfinder-facilitated intelligence product is the minimum amount of such data consistent with overall mission needs.

Finally, access to the information in Pathfinder, including PII, is only granted to appropriate DHS personnel **(b)(2) High**

(b)(2) High and Intelligence Oversight training is an annual requirement for all personnel within and otherwise supporting I&A. Given these circumstances, the risks to privacy are considered low.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

Information contained in Pathfinder is to be used internally within I&A **(b)(2) High**

(b)(2) High There are no other authorized uses for the Pathfinder system.

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

Pathfinder provides tools (b)(2) High

[Redacted]

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

(b)(2) High

[Redacted]

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.

I&A personnel are assigned authorized analytical tasks and their performance is monitored by I&A branch and division chiefs.

Individual DHS intelligence professionals responsible for (b)(2) High

[Redacted]

[Redacted] are each required to attend annual training in the protection and safeguarding of U.S. Persons and privacy related information as part of a mandatory training program on the I&A Information Handling Guidelines and I&A policies concerning Intelligence Oversight.

Finally, Pathfinder is subject to regular security audits. (b)(2) High

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b)(2) High

Section 3.0 Retention

3.1 What information is retained?

(b)(2) High

3.2 How long is information retained?

Information acquired through and otherwise retained within the Pathfinder application is retained in accordance with applicable I&A guidelines for records retention, and consistent with other policies or guidelines affecting the handling or retention of specific categories of certain information, including U.S. Person's Identifying Information. (b)(2) High

(b)(2) High

Current I&A Intelligence Oversight policies and associated I&A Information Handling Guidelines also require regular I&A review (at least annually) of any U.S. Person information acquired through Pathfinder to determine if the continued retention of that information is appropriate. When the specified period for federal records retention has elapsed, that record is removed and destroyed or archived, as appropriate. Where the continued retention of particular U.S. Persons identifying information is no longer appropriate, that identifying information is removed from the record. DHS Intelligence personnel responsible for creating the record or maintaining the information in Pathfinder must complete this required annual Intelligence Oversight review.

(b)(2) High

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

No, however, the DHS Records Retention Office has proposed the following schedule: NARA N1-563-07-16 Item 9 - Requests for Information (RFI) / Data Calls - Destroy or delete 30 years after the date a record was requested. Once the schedule is approved and established with the DHS Records Officer a formal submission to NARA will be made.

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

Given that I&A, as a discrete organizational element of DHS, has been in existence for only 5 years and was preceded by no other precursor agency or element of the Federal government with similar legacy functions or responsibilities that have carried over, the relative risks of longer term data retention are currently not as significant as they might be for an agency with a longer period of existence. Nevertheless, any historical compilation of records containing personally identifying information presents added inherent risks to privacy, as both the number of records retained and authorized user access accounts issued increases over time. However, the inherent risks posed by increased volume and user access are mitigated significantly by the controlled management and oversight of user accounts and the robust information security (b)(2) High information handling, and Intelligence Oversight framework discussed in previous sections.

Moreover, given the mission of DHS/I&A in preparing for and countering the threats to national or homeland security (b)(2) High. An extended period of retention is therefore more likely, notwithstanding (though ever mindful of) the potential risks associated with privacy, (b)(2) High. For that reason, (b)(2) High and otherwise to be permitted under law and applicable retention guidelines, for continued access by DHS personnel and other authorized users (b)(2) High.

In all cases, however, DHS Intelligence professionals are required to abide by all applicable guidelines designed, specifically, to ensure the protection of individual privacy. For example, I&A personnel perform annual reviews of and, as appropriate, remove U.S. person identifying information in products for which continued retention under applicable information handling and IO guidelines is no longer justified or appropriate. This helps to mitigate the risks both that personally identifiable information will be retained any longer than needed, and that information appropriately retained for extended periods of time will be accessed and used for only those purposes considered relevant to its original collection and necessary for its intended use.

(b)(2) High

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?

(b)(2) High

DHS Intelligence products and reports are shared with authorized external recipients consistent with the applicable authorities of I&A to share, and the intended recipients to receive, handle and otherwise use that information.

(b)(2) High

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.

(b)(2) High

will be shared in accordance with the Homeland Security Operations Center Database (HSOC) System of Records Notice (SORN), DHS/IAIP-001 (April 18, 2005), and available at 70 Fed. Reg. 20156. As it applies to I&A, specifically, the HSOC SORN will soon be overtaken by an updated privacy framework covering all of I&A's information applications, including Pathfinder. To be known as the I&A Enterprise Records System (ERS), the SORN for ERS was recently submitted in final draft form to the

Privacy Office and OMB in early 2008, and is nearing final approval for publication. The ERS SORN will replace the HSOC SORN as the governing system of records notice for all I&A systems and applications. The routine uses reflected in both SORNs contemplate the sharing of such information with intelligence and other agencies in furtherance of their respective national or homeland security responsibilities. In all such cases, the use of the products will be consistent with each receiving agency's authorities and policies concerning the receipt, handling and use of that information, and especially any U.S. Person's identifying information included therein, for appropriate intelligence or other authorized activities. User account information for Pathfinder is not shared with external organizations.

(b)(2) High

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

(b)(2) High

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

(b)(2) High

any privacy risks presented by the fact of external sharing are minimal.

Section 6.0 Notice

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

Generally speaking

(b)(2) High

we are not in a position to address the notice, if any at all, that may be provided to the individual supplying the information or to whom the record pertains. Given the sensitivity of the sources and methods through and from which most intelligence information, including that which potentially identifies U.S. Persons information, is acquired, as well as the sensitive purposes for which that acquired information is used, it would not be appropriate to speculate further in this document how, if at all, notice may otherwise be provided to individuals identified in the system.

However, notice generally concerning all intended uses of information by DHS Intelligence systems, applications, or repositories overseen by I&A is provided in the HSOC and ERS SORNs, respectively, as discussed previously.

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

(b)(2) High
and therefore is seldom, if ever, in a position to provide them an opportunity to decline to provide information in the first instance. (b)(2) High

[Redacted]

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

The individual is not provided with a means to limit the authorized use of the information utilized within Pathfinder. (b)(2) High

[Redacted] There are no other regular uses for this information, and any use by I&A of such information without that individual's written consent must be consistent with one of I&A's published Privacy Act routine uses, as reflected in the governing SORN framework. Moreover, whenever the collection, retention, or dissemination of U.S. Person identifying information is undertaken by I&A without the consent of that record subject, such activities also must comply fully with I&A Intelligence Oversight policies. Beyond the obligation to meet these requirements, Pathfinder does not provide any right or opportunity for individuals to consent to particular uses of their PII within Pathfinder.

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.

Other than the general notice provided to all potential record subjects, as reflected in publication in the Federal Register of I&A's governing SORN and associated privacy framework, specific notice to individuals whose personally identifying information is in Pathfinder is not provided. Given the nature of I&A's mission and the scope of the information within Pathfinder, (b)(2) High

[Redacted]

(b)(2) High

Therefore, it is neither practicable nor, possible to provide notice to the individual that his personal data has been obtained.

This may represent a risk to privacy, however the limits and requirements that I&A places upon its collection, retention, and dissemination of information within Pathfinder, including the implementation of and mandatory training on Information Handling and Intelligence Oversight guidelines required of all I&A personnel using the data are factors which mitigate this privacy risk considerably.

Section 7.0 Access, Redress and Correction

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

Because Pathfinder contains classified and sensitive unclassified information related to intelligence, counter terrorism, homeland security, and law enforcement programs, activities, and investigations, records within it have been exempted from requests for access or amendment by covered individuals to their own information within it, to the extent permitted by subsection (k) of sec. 552a of Title 5 of the U.S. Code. Notwithstanding applicable exemptions, DHS reviews all such requests on a case-by-case basis. Where such a request is made, and compliance would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of I&A, and in accordance with procedures and points of contact published in the applicable SORN.

The procedures for submitting FOIA requests for Pathfinder are available in 6 C.F.R. Part 5.

Assistant Secretary Office of Intelligence & Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528
Attn: FOIA Officer
E-mail: FOIAOPS@DHS.GOV

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

As noted above, erroneous information is not corrected or removed from the system. (b)(2) High

[Redacted]

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

Formal notice of the fact that privacy identifying information may be resident on I&A applications, such as Pathfinder, is provided generally through the SORN applicable to I&A systems, as described previously in this document.

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

Informal redress is provided to an individual requester on a limited basis where compliance with a request would not hinder I&A or DHS operations, the supported activities of other agencies, or otherwise jeopardize a sensitive national or homeland security, law enforcement, or other intelligence investigation.

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

Given the classified nature of the underlying system and the Pathfinder application, a robust program to permit access, review and correction of the raw intelligence data cannot be provided. While this lack of direct access and formal redress mechanisms may represent a theoretical risk to individual privacy, that risk is balanced against the heightened sensitivity of and potential harm that could result to the government activities supported, and are mitigated considerably given the inherent information system security protections and controls unique to classified information system within which Pathfinder resides and the applicable policies and mandatory procedures governing the access, collection, retention, use, and dissemination of the PII by I&A personnel.

(b)(2) High

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?

(b)(2) High

8.2 Will Department contractors have access to the system?

DHS employs contract analysts and other support personnel from several vendors to assist in the analysis of data, preparation of intelligence products, and administrative and technical management of the underlying system and IT application. All authorized I&A contractors with access to Pathfinder are bound by governing policies, guidelines, directives, and procedures, as appropriate and otherwise applicable to I&A personnel.

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

All Pathfinder users within I&A receive information security and general privacy training at least annually, (b)(2) High Individual I&A professionals, including contractors, detailees, and assignees, responsible for publishing finished DHS intelligence products, receiving products and reporting for posting into Pathfinder, and otherwise authorized access to them for later use are each specifically required to attend annual training in the protection and safeguarding of U.S. Persons and privacy related information as part of a mandatory training program on the I&A Information Handling Guidelines and I&A Intelligence Oversight.

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

Yes. PATHFINDER is certified and accredited (b)(2) High

The Pathfinder system was awarded an Approval to Operate on March 27, 2007.

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

(b)(2) High

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?

The security controls in place provide adequate protection of privacy, therefore, the privacy risks for this category are considered low. The primary privacy risks associated with the system were related to unauthorized access to the system and improper maintenance and dissemination of information. The systems access risk was mitigated by two primary countermeasures. (b)(2) High

[Redacted]

The information maintained within Pathfinder is classified and sensitive, and subject to the information handling requirements identified in Executive Order 12333. The mitigation of improper distribution or maintenance of this information is accomplished by the I&A analysts' mandatory annual information handling and intelligence oversight training,

Section 9.0 Technology

9.1 What type of project is the program or system?

Pathfinder is an operational project which assists I&A analysts in the execution of the Analysis and Production phases of the intelligence cycle.

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

Pathfinder has been deployed and is in operational usage at many locations within the Intelligence Community. I&A is using Pathfinder version 5, so this is a mature COTS product that has gone through several iterations of development and revisions. Pathfinder was assessed by the I&A Information Technology Review Board and after that evaluation the product acquisition, accreditation and deployment activities were permitted to continue.

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

(b)(2) High

Approval Signature Page

Original signed and on file with the DHS Privacy Office

John W. Kropf
Acting Chief Privacy Officer
Department of Homeland Security



Privacy Impact Assessment
for the

HSIN-Intelligence Portal

January 31, 2008

Contact Points

(b)(6)

Program Manager

Office of Intelligence and Analysis

(b)(6)

(b)(6)

CIO / Deputy Director, Information Sharing and Knowledge Management Division

Office of Intelligence and Analysis

(b)(6)

Reviewing Official

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The Office of Intelligence and Analysis (I&A) in the Department of Homeland Security (DHS) is implementing the Homeland Security Information Network-Intelligence Portal. The Portal is designed to foster information sharing, specifically with state, local, tribal, and private sector stakeholders. I&A has conducted this PIA because the portal may be used to communicate personally identifiable information (PII).

Introduction

The Department of Homeland Security, Office of Intelligence and Analysis (I&A), as the departmental lead component for communicating and collaborating with internal and external stakeholders on intelligence matters, has implemented the Homeland Security Information Network (HSIN)-Intelligence secure extranet portal, hereafter referred to as HSIN-Intelligence. The platform is used to share intelligence at the controlled, unclassified information (CUI) ¹ level specifically with state, local, tribal, and private sector (SLTP) customers, and federal and international partners. The system also supports the sharing (collaboration) of intelligence within the DHS Intelligence Enterprise². I&A has conducted this privacy impact assessment because of the collection of personally identifiable information (PII) during the user registration process and the sharing of PII among users within the HSIN-Intelligence platform.

Description

HSIN-Intelligence is the centralized mechanism for the DHS Office of Intelligence and Analysis to post and share intelligence information relating to the security of the homeland and the mission of the Department with other intelligence analysts at the Federal, State and Local levels. The security and functionality features implemented to support the mission requirements ensure:

- Appropriate security for exchanging sensitive intelligence information.
- Discretionary access to intelligence information.
- Information view capabilities managed by individual user and organizational roles
- A secure, single-access point to intelligence data which authorized stakeholders may access from anywhere at any time.
- Trust-enhancing functionality (b)(2) High

¹ Controlled Unclassified Information (CUI) is the emerging term across the federal government to encompass all unclassified information that needs to be protected.

² The "DHS Intelligence Enterprise" includes all those component organizations within the Department that have activities producing raw information, intelligence-related information, and/or finished intelligence.



The implementation of this platform will involve multiple phases. Currently, implementation has entered Phase One. (b)(2) High
If this were to occur, such phases would be preceded by a revision to this privacy impact assessment.

The primary mission-driven platform configuration model is to divide the capability into two conceptually, and technically, separate areas:

- HSIN-Intelligence (General): This is the central hub for HSIN-Intelligence. (b)(2) High
Management of the I&A content provided will be overseen by the I&A Production Management (PM) Division. (b)(2) High
Subsequent and follow-on phases of implementation will address the potential need for policies and governance (b)(2) High
Modification of this PIA to support those added capabilities will be addressed appropriately.
- HS SLIC Compartment: This refers to the restricted access area self-contained within the larger HSIN-Intelligence hub. It is designed specifically for targeted dissemination to and collaboration among authorized end-users within the Homeland Security – State and Local Community of Interest (HS-SLIC). (b)(2) High
which is intended to enable participants to collaborate on the assessment of raw intelligence data and other relevant reporting, as well as the development of joint or collaborative products, that may contain the personally-identifiable information (PII) of U. S. Persons,⁵ including U.S. Citizens and other Legal Permanent Residents of the United States.

Typical Transactions on HSIN-Intelligence

HSIN-Intelligence serves as a hub through which authorized users may receive appropriately sanitized and properly vetted intelligence products or reporting disseminated by I&A, and otherwise reach the I&A-provided internal collaboration spaces, including, when appropriate, the restricted HS SLIC Compartment. Users with general authorized access to only the HSIN-Intelligence hub would access basic intelligence related information, intelligence reports and other collaborative efforts that have either been sanitized to exclude or, by rule, will not include in the first instance, any PII. Certain authorized users would, (b)(2) High access the “restricted” HS SLIC compartment for

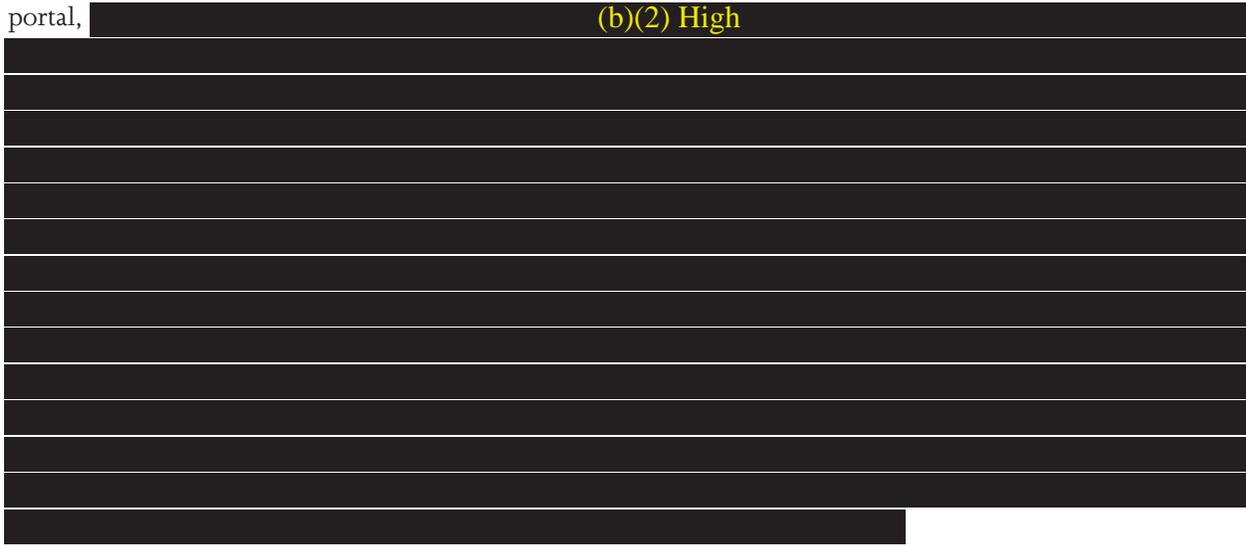
³ Intelligence Oversight is the process of ensuring that all intelligence, counterintelligence, and intelligence related activities are conducted in accordance with applicable U.S. law, Presidential Executive Orders, and DHS Management Directives and policies (b)(2) High

⁵ The definition of a U.S. Person includes a U.S. citizen, an alien known to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S. (except for a corporation directed and controlled by a foreign government).



viewing, and posting, and collaborating on intelligence products provided by, or for other authorized members of the HS SLIC.

To illustrate, when an authorized State or local agency end-user logs into the HSIN Intelligence portal, (b)(2) High



Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

Information collected includes the following:

- Intelligence, law enforcement, and other information lawfully acquired and initially provided by a federal, state, local, or tribal government agency, or the private sector, to an authorized HSIN Intelligence participant, that is relevant to one of the specific functions of I&A in the context of the broad mission and associated responsibilities of the Department, including but not limited to the prevention of terrorism; the responsibilities of legacy agencies and entities originally transferred to the Department, including those responsibilities unrelated to terrorism; the preparation, response and recovery from natural and manmade crises and disasters; and ensuring that civil rights, civil liberties, and the overall economic security of the United States are not diminished by homeland security efforts.

This information may include the PII of specific U.S. Persons, such as name, date of birth, nationality, place of birth, or some other specific PII. However, such PII shall be made visible within HSIN Intelligence, if at all, only to and by authorized members of the HS SLIC, within the restricted HS SLIC compartment, in accordance with all applicable procedures or guidelines on the collection, use, retention, and dissemination of PII, and only when necessary and relevant to the purpose for which it is to be maintained and shared within HS SLIC. While much information otherwise collected into and contained within the HSIN Intelligence portal is either derived from or, as in the case of a finished intelligence product or report re-posted from elsewhere into HSIN Intelligence, would have originally contained PII of



specific U.S. Persons, it is the policy of HSIN Intelligence that no such PII shall be visible in any intelligence, law enforcement, or other information product or report posted into the general access areas of HSIN Intelligence.

[REDACTED] (b)(2) High [REDACTED]
[REDACTED]
[REDACTED]

User registration information is also collected from nominated and approved HSIN-Intelligence end users, including those specifically nominated and approved for access within the restricted HS SLIC compartment. [REDACTED] (b)(2) High [REDACTED]

[REDACTED] Separate to the technical platform, [REDACTED] (b)(2) High [REDACTED]

[REDACTED] With respect to information providers and users within the HS SLIC compartment, such collected information will also [REDACTED] (b)(2) High [REDACTED]

1.2 From whom is information collected?

Information collected is obtained from federal, state, local, or tribal government organizations, including law enforcement agencies, participating in HSIN Intelligence. This information may include relevant information originally collected by any one of these participating organizations, consistent with their respective missions and authorities to do so, as well as by foreign government organizations and the private sector.

Registration Information: [REDACTED] (b)(2) High [REDACTED]
[REDACTED]

1.3 Why is the information being collected?

HSIN-Intelligence enables authorized end users to access, receive, analyze, and, where appropriate, disseminate relevant intelligence, law enforcement, and other information, on behalf of their represented agencies, and in accordance with all applicable laws, regulations, and guidelines. The collection of this information into HSIN Intelligence enables participating agencies at the federal, state, local, tribal, and local level to assess the information in the context of their individual agency missions and responsibilities, and to make informed decisions concerning rapidly evolving threats to homeland security by using the best data available.

Registration Information: [REDACTED] (b)(2) High [REDACTED]
[REDACTED]



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

Among the legal authorities, arrangements and agreements that define the information collection are:

- **The Homeland Security Act of 2002** (Title II – Information Analysis and Infrastructure Protection, as amended): Authorizes DHS, among other things, through the Under Secretary for I&A and Chief Intelligence Officer of the Department (collectively, I&A),: (1) to access, receive and analyze law enforcement information, intelligence information, and other information from agencies of the federal government, state and local government agencies (including law enforcement agencies), and the private sector, and to integrate such information to aid primarily in the collection, analysis, and sharing of terrorism information and related threats to the homeland; (2) to integrate relevant information in order to identify priorities for protective and support measures (including those unrelated to the prevention of terrorism) by the Department, other agencies of the federal government, state and local governments agencies and authorities, the private sector, and other entities; (3) to provide intelligence and information analysis support to other elements of DHS engaged in authorized DHS missions (including those unrelated to the prevention of terrorism); and (4) to perform such responsibilities as directed by the Secretary in furtherance of an authorized mission of DHS, as derived from statutory, regulatory, and executive authorities. Also authorizes I&A:
 - to consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, and other elements of the federal government, as well as with state and local governments and private sector entities, as appropriate, to establish priorities and strategies for the collection of relevant information, and to ensure that appropriate exchanges of that information are occurring;
 - to request additional information from other federal agencies, state and local governments, and the private sector, relating to threats of terrorism or relating to other areas of responsibility assigned by the Secretary; and
 - to establish and utilize a secure communications and information technology infrastructure, in order to access, receive, analyze, and disseminate data and information acquired by the Department, in furtherance of I&A's responsibilities therein, and to ensure information contained therein is treated in a manner which complies with applicable federal law on privacy.
- **Executive Order 12333, as amended**, recognizes I&A as a member of the National Intelligence Community (IC), and authorizes all agencies within the IC, in accordance with applicable law and other guidance, to collect information needed by the President and other Executive Branch officials for the performance of their duties and responsibilities, including but not limited to information concerning international terrorist and narcotics activities, and other hostile activities directed against the U.S. by foreign powers, persons, organizations, and their agents; and to produce and disseminate intelligence. The Order also authorizes IC agencies to collect, retain, and disseminate such information and intelligence which concerns specific and identifiable U.S. Persons, but only



in accordance with subsequently issued procedures that are both consistent with the authorities provided in law and this Order, and limited to specific types or categories of U.S. Persons information.

- This Order also authorizes IC agencies to cooperate and participate in law enforcement activities, unless otherwise precluded by law or this Order, related to counterintelligence, counterterrorism, or international counternarcotics investigations, as appropriate, and to otherwise provide, with the approval of the agency General Counsel, expert assistance, including, but only where lives are endangered, in support of local law enforcement agencies.
- **The Homeland Security Presidential Directive (HSPD-5)(February 28, 2003)** designates the Secretary of Homeland Security as the principal federal official for domestic incident management, and facilitates pertinent information sharing between the Department of Homeland Security and other agencies.
- **Homeland Security Presidential Directive 7 (HSPD-7)(2003)** orders the Secretary of Homeland Security to establish appropriate systems and mechanisms for sharing relevant homeland security information within and among the various sectors, and with those agencies and organizations primarily responsible for coordinating the protection of, our nation's critical infrastructure and key natural resources.
- **The Intelligence Reform and Terrorism Prevention Act (IRTPA)(2004), as amended**, directs the establishment of an information sharing environment, or ISE, to facilitate the sharing of terrorism, including pertinent law enforcement, weapons of mass destruction-related, and homeland security information among all appropriate Federal, state, local, and tribal entities, and the private sector, utilizing, among other things, existing systems and networks, and incorporating mechanisms (e.g., audits, authentication, access controls) for protecting the security of the information and individual's privacy and civil liberties. While the IRTPA created a government-wide program for sharing information in the ISE, it specifically preserved within DHS its existing authorities with regard to the exchange, use and dissemination of information to state, local, and private entities.
- **The Privacy Act of 1974** outlines the notice, use, access, and disclosure procedures which govern the I&A system of records within which HSIN Intelligence, and the specific intelligence and other user-related registration information containing covered PII contained therein, is maintained.

1.5 Privacy Impact Analysis

I&A posts intelligence information products and other related reporting products which contain visible PII only to those discrete restricted-access areas of the HS SLIC compartment within HSIN Intelligence where content and access management of the information in that area is either controlled exclusively by I&A or, when such control belongs to another HS SLIC member organization, where I&A has in advance determined specifically that the release of PII to that organization is authorized and otherwise consistent with I&A's obligations and procedures concerning the treatment and handling of U.S. Persons information, as discussed further below in this section. Similarly, other participating HS SLIC member



organizations post information, including that which may contain PII, into those areas of the HS SLIC compartment where content and access management of the information in that area is either controlled exclusively by that organization or, when such control belongs to another HS SLIC member organization, where that posting organization has in advance determined specifically that the release of PII into that organization's area is authorized and otherwise consistent with its own obligations and procedures concerning the treatment and handling of U.S. Persons information.

As discussed above, and consistent with the governing HS SLIC Charter, (b)(2) High

[REDACTED]

All PII posted onto the HS SLIC compartment by I&A personnel, including the purpose for which it was collected into HSIN Intelligence and the manner in which it is maintained and shared with other agencies within the HS SLIC compartment, conforms to the requirements of the Privacy Act insofar as public notice of the collection, use, and maintenance of PII by I&A has been properly published, along with specific instructions for or claimed exemptions from, *see* 6 CFR Part 5, subpart B, Access and Amendment of Covered Records by Record Subjects.

Moreover, I&A, as a member of the National Intelligence Community, also conducts its mission in conformance with the requirements of Executive Order 12333, as amended, and has established procedures to govern the collection, retention, and dissemination of information concerning U.S. Persons in a manner which protects the privacy and constitutional rights of U.S. Persons. Specifically, I&A intelligence personnel may collect information which identifies a particular U.S. Person, retain it within and or disseminate it from I&A information sharing platforms such as HSIN Intelligence, as appropriate, only when it is determined that the PII is necessary for the conduct of I&A's authorized functions and otherwise falls into one of a limited number of categories which reflect the discrete types or activities of U.S. Persons for which information on such individuals would be utilized by the Department in the overall execution of its mission. Even where the collection and retention by I&A personnel of PII within HSIN Intelligence is appropriate under these procedures, there is nevertheless an additional requirement imposed whereby, prior to disseminating or making available any such PII outside of I&A, I&A personnel must also undertake a "minimization" process; that is, evaluating whether inclusion of the specific U.S. Person information or identity within that particular intelligence product or report, in the context of the intended recipient's need for the specific PII to understand or utilize the product, is necessary. Where disclosure of the actual PII is not necessary, the identity information must be "masked" by redacting or deleting it and replacing it with "a U.S. Person," "USPER", or some similar generic identifier. When an I&A product includes U.S. person identifying information, that PII must also be properly marked or tagged as "a U.S. Person" or "USPER," as appropriate, and the product or report itself must carry a warning stating that "This document contains U.S. Person Information and should be handled accordingly," or words to that effect.

I&A "Information Handling Guidelines" further complement the protections already afforded, respectively, by I&A's Privacy Act and Intelligence Oversight frameworks, described above, by explicitly prohibiting in all circumstances the collection and maintenance of U.S. persons information "solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights



secured by the Constitution or laws of the United States.” These same guidelines also require I&A personnel to honor other restrictions/controls that may apply to information previously acquired by I&A, and which may limit or, in some cases, entirely prohibit, the use of certain information such as PII on platforms such as HSIN Intelligence. Such restrictions might include, as appropriate, classified or other sensitive information controls, statutory restrictions on the use of certain data, and 3rd party controls (e.g., ORCON, 3rd Agency Rule, Trusted Agents, etc.).

Other participating HS SLIC member organizations post information, including that which may contain PII, into those areas of the HS SLIC compartment where content and access management of the information in that area is controlled exclusively by that organization. Similar to the obligations of I&A personnel to protect information concerning U.S. Persons, State and Local HS SLIC members, whose users post intelligence and related reports into the HS SLIC compartment, have also agreed, as a condition both to participation within HS SLIC and access to relevant information containing PII, to be bound by the obligations and requirements concerning the treatment of PII applicable within “Criminal Intelligence Systems,” pursuant 28 CFR Part 23. This imposes upon them obligations to protect the privacy interests of the subjects and potential subjects of these activities. These protections are achieved by requiring, among other things, that law enforcement intelligence information which identifies an individual be collected, retained, and disseminated only when there is reasonable suspicion that the individual identified is involved in criminal conduct and the information is relevant to that conduct or activity.

Furthermore, while each State and Local member, as a matter of policy and business process within the HS SLIC compartment of HSIN Intelligence, retains originator control over its own postings and is individually responsible for its users’ compliance with the requirements of 28 CFR Part 23, as well as all other laws, regulations or directives which may apply uniquely or otherwise to that State or Locality’s activities within HSIN Intelligence, appropriate I&A personnel may nevertheless review every HS SLIC user posting and, at their discretion, request minimization of any U.S. person identifying information contained therein where it is determined to be necessary in the interest of protecting the privacy and civil liberties of individuals.

Notwithstanding the implicit protections to privacy and civil liberties contained in the applicable frameworks described above, it is important to note also that the HS SLIC Steering Group regularly steers discussion and information posting activities occurring within the HS SLIC compartment to fit current issues and concerns of its member organizations, DHS, and the Intelligence Community. Thus, in most circumstances, user posted information must, in addition to complying with the policies, procedures, and guidelines described above, be relevant to issues and concerns specifically defined by the Steering Group.

Finally, significant technical safeguards have been implemented to further ensure the consistent and constant protection of PII. Primary among them, [REDACTED] (b)(2) High

[REDACTED] This primary safeguard ensures that only those individuals actually nominated, verified and validated as authorized users are provided access to PII, as appropriate, at any time.



Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

I&A uses of HSIN Intelligence include:

- (b)(2) High [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Registration Information (b)(2) High [Redacted]

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

(b)(2) High [Redacted]



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

The information contained within HSIN-Intelligence will be provided by I&A and other authorized member organizations. Beyond those mechanisms actually in place, applied, or otherwise required by law, when the information was originally collected by the relevant agency, the information posted to HSIN Intelligence, including PII within the restricted spaces of the HS SLIC compartment, is not checked for accuracy, but assumed to be accurate as coming from a trusted system user and organization in the ordinary course

(b)(2) High
[Redacted]

(b)(2) High
[Redacted]

[Redacted]

2.4 Privacy Impact Analysis

The HSIN-Intelligence portal access and accountability controls, including those specifically designed for and implemented within the HS SLIC compartment where PII resides, are the primary guarantors of the accuracy, appropriate protection and integrity of the information stored within the system. As gatekeepers for determining who holds access and to what information, these rules and controls involve two basic components. The first of these are the technical limitations

(b)(2) High
[Redacted] Secondly, users are administratively restricted from information that they are not authorized by policy or law, or otherwise permitted, to receive.

(b)(2) High
[Redacted]

Registration Information: (b)(2) High
[Redacted]



Any user found to be falsely making such a certification will be immediately denied continued access to the portal, referred to the appropriate law enforcement or other entity responsible for investigating such misconduct, and the matter will also be referred to the user’s parent and/or sponsoring organization for consideration of any additional disciplinary or other legal actions that may be taken against that individual.

Section 3.0 Retention

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

I&A maintained data contained within HSIN-Intelligence, including any PII of U.S. persons contained within the HS SLIC compartment, is retained for periods of time in accordance with applicable law, regulation, and other directives or guidance, including relevant provisions of the Federal Records Act, and specifically with respect to PII, those rules and procedures for the retention of such information required under Executive Order 12333, and as implemented through DHS Memorandum, *Intelligence Oversight Basics*, dated March 27, 2006, discussed more fully in section 1.5, above, which requires review of U.S. person information placed into I&A’s records system, including relevant portions of HSIN Intelligence, on a periodic⁶ basis to see if the PII itself is still needed and otherwise meets the standards for its original collection, also discussed above. If not, the PII will be deleted from the record. Under these rules, the obligation to review and assess PII in I&A controlled records for continued retention belongs to each employee, contractor or other official assigned to I&A, or over whom it is determined that I&A policies and procedures concerning the treatment of PII within HSIN Intelligence will apply, and who is responsible for posting the covered content.

Data maintained, and otherwise posted into restricted HS SLIC spaces where content management is exclusively controlled by HS SLIC member organizations other than I&A, is retained in accordance with whatever retention period the individual State or locality requires – to be clear, information posted into those restricted access areas of the HS SLIC compartment control over which belongs exclusively to organizations other than I&A or other federal agency participants are not considered federal records. This is so, notwithstanding the fact that I&A or another member organization is provided access to that particular space for purposes of viewing and assessing the content.

Registration Information: (b)(2) High
[Redacted]

⁶ At a minimum, PII is to be reviewed annually to determine the need and authority for continued retention.



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

No, a records retention schedule currently has not been reviewed or approved by NARA. I&A is coordinating separately a records retention schedule for approval in parallel to this HSIN-Intelligence project. I&A, as the system owner, will default to retaining all records indefinitely (or five years in accordance with 28CFR, Part 23) until such time that the retention schedule has been approved and implemented within I&A.

3.3 Privacy Impact Analysis

The retention rules concerning information within HSIN Intelligence generally, and specifically those concerning PII posted and maintained within I&A controlled HS SLIC spaces which require, among other things, annual reviews of PII and deletion when no longer needed or permissible to retain under applicable guidelines and procedures, help to mitigate significantly the risk that personally identifiable information will be retained any longer than actually needed.

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?

Information is generally shared with any DHS component with an intelligence element (e.g., CBP, ICE, I&A, TSA, Coast Guard, etc.), and any other DHS component where the information is relevant to the performance of an official function. Since DHS intelligence information sharing and collaboration is the purpose of the HSIN-Intelligence system, and because DHS policies require the sharing of certain information in the possession of any one DHS organization – including I&A – with any other DHS organization, those DHS employees who are otherwise eligible and have validated user accounts can access information within HSIN Intelligence in accordance with applicable HSIN Intelligence rules and procedures. This internal access specifically includes access to information by both law enforcement and non-law enforcement organizations within DHS for purposes consistent with the authorized functions of those DHS organizations and personnel, and the DHS mission.

Registration Information: User registration information is not shared outside of HSIN-Intelligence or, for the HS SLIC portions, outside of the respective HS SLIC community.

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

Any information within HSIN Intelligence capable of being collected by I&A may be generally shared with any other DHS component where the information is relevant to the performance of an official function which belongs by statute or other authority to that DHS component, appropriate information security safeguards exist and are in place (e.g., system eligibility and access by the component user), and



the sharing is not itself otherwise prohibited by law. Since the scope of I&A's intelligence information sharing mission is consistent with that of the mission of DHS and all of its constituent components, the information shared with those components does not, generally speaking, differ from the type of information already described in 1.1.

4.3 How is the information transmitted or disclosed?

Authorized users with specifically assigned rights and attributes are able to access HSIN-Intelligence spaces, including, as appropriate, the restricted HS SLIC compartment, directly over an unclassified web-based (i.e., remote) secure network interface.

4.4 Privacy Impact Analysis

All HS SLIC members who access PII via the HSIN-Intelligence system must (inclusive):

- Be a full-time, current employee (government or contractor personnel) of a law enforcement, criminal justice, or homeland security Federal, State, Territorial and Protectorate, Tribal, or local government agency engaged in seeking to detect, defeat, or deter terrorist acts and thereby engaged in law enforcement activities for purposes of 28 C.F.R. Part 23; exceptions to full-time status must be approved by both the respective State HS SLIC point of contact and the DHS HS SLIC PM;
- Be a U.S. Citizen;
- Be currently employed in homeland security information and intelligence analysis functions for that government agency, as verified by (1) the DHS HS SLIC PM or their Government supervisor for federal employees, or (2) the respective State, Territory, or Urban Area HS SLIC point of contact or their designee for State and local intelligence employees;
- For State and Local members, be formally associated — either via management chain of command, Memorandum of Understanding, or some other formal mechanism — with a State and Local Fusion Center, or centralized intelligence fusion capability in the absence of a center, recognized as such by the HS SLIC Steering Group Voting Member appointed by the respective Homeland Security Advisor;
- Accept a HS SLIC user agreement that includes, to specifically include a third party non-disclosure agreement; any HS SLIC End User violating this user agreement shall have their access to the HS SLIC terminated on an immediate basis; and
- Have a government email address (or other email address approved by the State, Territory, or Urban Area POC and the HS SLIC PM).

In addition, each participating State, Territorial, or Urban Area HS SLIC Sponsoring Organizational representative is required to:

- Verify the HS SLIC eligibility status of sponsored employees (including contractors) on an annual basis, ensuring that each employee they sponsor (1) meets the eligibility requirements and (2) uses the system within these rules; and



- Maintain the user roster for the organization, and remove from the system any sponsored employee no longer eligible.

Finally, each HS SLIC member must:

- Be part of a single Sponsoring Organization approved by the associated Voting Member;
- Revalidate their position, title, and email address at least annually; and
- Change their system password and agree to user rights and responsibilities every 90 days or their access will be terminated.

The HS SLIC mitigates privacy risks caused by inappropriate access and/or sharing by limiting who has access to PII and defining proper use of system information. (b)(2) High

This ensures internal and external access to the HS SLIC restricted portion of HSIN-Intelligence is tightly controlled. Coupled with usage restrictions detailed in Section 2.0 and Section 8.0, this ensures that risks associated with internal sharing are mitigated as much as possible.

Internal and external sharing is governed by these same access, control, and accountability procedures.

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?

As of January 3, 2008, those external organizations who are members of the HS SLIC and have sponsored user accounts for eligible personnel to access the HS SLIC compartment include:

39 States:

Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, New Hampshire, New Jersey, New Mexico, New York, Ohio, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin

Federal Agencies:

DOJ, Drug Enforcement Administration
Department of Interior
Federal Bureau of Intelligence, National Security Branch
Office of Director of National Intelligence, Program Manager-Information Sharing Environment
Department of Defense, Northern Command



All users granted access to the HS SLIC compartment, who are employed by any organization (to include all listed above,) have been granted access through the eligibility criteria described in Section 4.4 above, and have accepted to be bound by the handling restrictions, HS SLIC governance policies and laws of their jurisdictions.

Users granted access to the HSIN-Intelligence (General) areas are granted via policies determined by the I&A Production Management Division for intelligence dissemination products that do not contain PII.

All HSIN-Intelligence information is stored in virtual spaces accessible only through the HSIN Intelligence portal. Individual users will be able to send external emails and alerts to other users from within the system, though emails or alerts originating on the system are retained in the system.

Registration Information: User information is contained in a global directory. Users may alter their information themselves, within the portal.

5.2 What information is shared and for what purpose?

Homeland security-related law enforcement, intelligence, and other information from federal, State and local government agencies (including but not limited to terrorism and related threat reporting, assessments of suspicious activity reports, and other reports or exchanges concerning activities that users consider germane to the homeland security mission) is shared among and between the external organizations listed above in order to enable those organizations to identify criminal and other related activities associated with terrorist actions, planning, or preparations. (b)(2) High

[Redacted]

5.3 How is the information transmitted or disclosed?

Authorized users with specifically assigned rights and attributes are able to access HSIN-Intelligence spaces, including, as appropriate, the restricted HS SLIC compartment, (b)(2) High

[Redacted]

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?

Individual HSIN-Intelligence users, including and especially those end users with access to restricted spaces within the HS SLIC compartment, must read, acknowledge, and comply with an End User Agreement that references and incorporates their obligations to comply with the laws and policies associated with their sponsoring organization, the jurisdictions in which they operate, and that of the overall HSIN Intelligence program, as applicable. In addition, and in order to enter any spaces within the HSIN-Intelligence portal, users must acknowledge an on screen system use agreement.



All organizations that are eligible and vetted for membership into the HS SLIC, in coordination with their applicable sponsoring organizations and approval authorities are initially bound, as a condition of membership, by the policies, rules and processes outlined in the HS SLIC Charter. In addition, all HS SLIC end users, as a condition of their participation in and access to the HS SLIC compartment of HSIN-Intelligence, operate under a firm “no third party dissemination without explicit authorization” handling rule – that is, each HS SLIC user organization that posts information on HS SLIC retains the right to restrict further dissemination by any other HS SLIC member to whom access has already been granted, unless and until the original provider of the information explicitly permits further dissemination to any non-HS SLIC (3rd Party) entity.

5.5 How is the shared information secured by the recipient?

HSIN-Intelligence [REDACTED] (b)(2) High [REDACTED] Once accessed, data available to the recipient is subject to the recipient’s obligation to comply with the laws and policies of their respective agency/organization and applicable jurisdiction as well as the laws and policies associated with intelligence information and the HSIN-Intelligence system rules of conduct. The HSIN-Intelligence system complies with all appropriate DHS security policies. In addition, [REDACTED] (b)(2) High [REDACTED]

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

The following training will be provided to users of this system:

- User Technical Training: The HSIN-Intelligence secure portal service vendor offers each of the users training on how to use the system. Training will be given at both HS SLIC user locations as well as through system-based training accessible from the system itself. Under section 201(d)(16) of the Homeland Security Act, DHS has a statutory responsibility “to coordinate training and other support to the elements and personnel of the Department, other agencies of the federal government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.”
- User Legal/Regulatory Training for HS SLIC: HS SLIC users granted access to PII receive formal vetting prior to physical access, and then receive training regarding the legal/regulatory predicate authorizing access to the data as also described in Section 2.4 above. DHS I&A members are subject to Intelligence Oversight training as well as other Privacy related training over the course of their assignment to the position. A majority of the HS SLIC members are State and Local authorities (or sworn Law Enforcement officers) who are bound to comply with 28 CFR Part 23, and receive the appropriate privacy training to properly conduct their duties.



5.7 Privacy Impact Analysis

HSIN-Intelligence mitigates privacy risks caused by inappropriate external access and/or sharing by prohibiting the use of PII except in certain areas of the platform, limiting who has access to HSIN-Intelligence generally, and specifically with respect to those restricted areas of the HSLIC compartment, and defining terms for the proper use of system information. This is particularly true for the HS SLIC compartment of HSIN-Intelligence, where all intelligence products containing U.S. person information or PII will reside. Through the auditing and technical measures of the system, the potential for misuse of data is minimized ((see section 8.6, below). The HSIN-Intelligence portal, in restricting the disclosure of sensitive PII information only to authorized HS SLIC members with the statutory responsibility and a mission need to know such information, further ensures the necessary privacy protections. These protections are further reinforced by the minimization process through which I&A, prior to dissemination within the HS SLIC compartment, assesses all information, including intelligence and other relevant products and reports, concerning U.S. Persons to determine whether disclosure of the PII is necessary in order for the recipients to otherwise understand and use the product or report.

Section 6.0 Notice

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?

General notice to the public of information collected, maintained, used in, and disclosed from, all platforms within the collective records system within which I&A currently operates was published in the Federal Register on April 18, 2005, under the title "HSOC Database". The collection of information into HSIN Intelligence is covered by that SORN. Publication of notice for a new stand alone Privacy Act records system framework for I&A, including notice of exemptions to be claimed, is imminent. Among other things, this new I&A SORN will reflect the intervening reorganization of offices formerly within the DHS Information and Analysis and Infrastructure Protection Directorate, including both I&A and what had previously been known as the Homeland Security Operations Center, or HSOC (the conduit through which I&A and other IAIP offices had historically exchanged information with relevant stakeholders).

The System of Records Notice for the registration information and subsequent user verification is covered by DHS ALL 004, General Information Technology Access Accounts.

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

Information collected on individuals in support of an intelligence support mission does not include an opportunity for said individuals the right to decline the collection of this information. Information may be collected arbitrary of knowledge by the individual and the collection, retention, dissemination and



destruction of that information is bound by the laws, policies and regulations described further within this Privacy Impact Assessment.

User Registration Information (b)(2) High

Additionally, authorized users may decline to provide intelligence information collected by their specific agency however the HS SLIC community strives to foster a level of trust among users, and choosing to withhold information has the potential to hinder and impact vital intelligence related collaboration.

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?

No. There does not exist a mechanism for individuals to consent or contest the uses of their personal information. The safeguards for the proper handling and protections of that information lie only within the laws, regulations and policies of the HSIN Intelligence user organization that collects the information.

6.4 Privacy Impact Analysis

General notice is provided through the published System of Records Notices, as required by the Privacy Act of 1974, and which govern the records systems within which information accessible through the HSIN Intelligence portal exist. Although individuals who may be the subject of or mentioned in a report or product may neither have been able to decline to provide information about themselves nor consent to certain uses when it was initially acquired, the HSIN-Intelligence portal mitigates privacy risk to individuals by controlling the nature of the information posted, the purposes for and manner in which it can be used and further shared, and access to it, so that only those individuals with a need-to-know that information in the performance of authorized functions, and subject to additional restrictions and limitations concerning access and use, are allowed to view it. Providing more robust notice than that discussed above would hinder the activities of the Department and its participating stakeholders in the conduct of intelligence and law enforcement investigations and other activities undertaken for the purposes of securing the homeland.

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?

Opportunities and instructions for individuals seeking access to information about them, and maintained by I&A within those restricted areas of the HSIN-Intelligence portal where PII may be present, are explained in provisions of the applicable Privacy Act System of Records Notice which covers that particular information. Additionally, any person may request access to any federal records maintained by I&A or any other federal agency through the Freedom of Information Act. The specific procedures for



submitting Privacy Act and FOIA requests for information maintained by I&A and accessible through the HSIN Intelligence portal are available in 6 C.F.R. Part 5.

Registration Information: (b)(2) High
[Redacted]

7.2 What are the procedures for correcting erroneous information?

Because personal information likely to be accessible through the HSIN-Intelligence portal, while not classified for national security purposes, includes or is based on highly sensitive intelligence or other threat reporting, no specific procedures have been established by the HSIN Intelligence program officials to allow for correction of this information. The System of Records Notice (SORN) that applies to this platform contains provisions that allow discretion in receiving PII correcting requests, if necessary. As a practice, as new information is obtained, old information accessible through HSIN-Intelligence will be updated or deleted. In addition, with respect to all information concerning U.S. Persons maintained by I&A, PII will be periodically reviewed by the poster of the information to determine if it is still needed, and if it is not, it will be removed.

State, local, and other government agency postings to the HS SLIC compartment of the HSIN-Intelligence are not maintained by I&A, nor considered to be I&A documents unless I&A chooses to re-post them into the I&A controlled spaces of the HS SLIC compartment, or in another location within I&A's system of records not accessible through the HSIN Intelligence portal. In those situations where PII is posted by a State, local, or other government organization, and into spaces whose content is under the management and control of that State, locality, or other government agency, individuals desiring to correct records which may identify them must contact that specific agency for more information on the procedures that may be available.

Registration Information: (b)(2) High
[Redacted]

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

The DHS FOIA page, available through the DHS public website, contains instructions for correcting information within DHS systems of records generally, but there are no specific provisions for correcting the highly sensitive law enforcement and related intelligence information in the HSIN-Intelligence system. Question 7.1 discusses the procedures for accessing information through the Privacy Act/FOIA process.

Registration Information: Upon completion of registration, users are informed of the correction procedures.



7.4 If no redress is provided, are alternatives are available?

Basic access and correction procedures are discussed in Sections 7.1, 7.2, and 7.3 above.

7.5 Privacy Impact Analysis

During development of the HSIN-Intelligence information sharing platform, and the processes governing its use, significant consideration was given to the impact of erroneous data on individual record subjects, including official users of the information. Since most information within the restricted HS SLIC compartment of HSIN-Intelligence, where all PII resides (b)(2) High

[Redacted]

Nevertheless, and given the sensitive nature of the information in HS SLIC and the intelligence missions it supports, (b)(2) High (b)(2) High and every effort is made to correct information and provide access to information in accordance with DHS guidance and other legal requirements, as applicable. (b)(2) High

[Redacted]

This ensures accountability for information shared and made available to others within the HSIN-Intelligence platform.

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? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

HSIN-Intelligence has a separate Program Office that generally reviews portal content; this program office also manages the HS SLIC in its entirety, including overseeing the administration of the HS SLIC Steering Group and the technical portions of both the outer HSIN-Intelligence hub, as well as the restricted spaces of the HS SLIC compartment. As explained elsewhere, all users with access only to the outer HSIN-Intelligence hub will have similar access to all communication and collaboration tools accessible and functional capabilities within that general area. Users with access to the inner HS SLIC compartment will have such access to all communication and collaboration tools and functionality as are specifically made available to them, in accordance with any additional rules, permissions, or restrictions that may apply, therein.



All HS SLIC end users who are provided access to PII via the restricted HS SLIC compartment of HSIN-Intelligence must (inclusive):

- Be a full-time, current employee (government or contractor personnel) of a law enforcement, criminal justice, or homeland security Federal, State, Territorial and Protectorate, Tribal, or local government agency engaged in seeking to detect, defeat, or deter terrorist acts and thereby engaged in law enforcement activities for purposes of 28 C.F.R. Part 23; exceptions to full-time status must be approved by both the respective State HS SLIC point of contact and the DHS HS SLIC PM;
- Be a U.S. Citizen;
- Be currently employed in homeland security information and intelligence analysis functions for that government agency, as verified by (1) the DHS HS SLIC PM or their Government supervisor for federal employees, or (2) the respective State, Territory, or Urban Area HS SLIC point of contact or their designee for State and local intelligence employees;
- For State and Local members, be formally associated — either via management chain of command, Memorandum of Understanding, or some other formal mechanism — with a State and Local Fusion Center, or centralized intelligence fusion capability in the absence of a center, recognized as such by the HS SLIC Steering Group Voting Member appointed by the respective Homeland Security Advisor;
- Accept a HS SLIC user agreement that includes, to specifically include a third party non-disclosure agreement; any HS SLIC End User violating this user agreement shall have their access to the HS SLIC terminated on an immediate basis; and
- Have a government email address (or other email address approved by the State, Territory, or Urban Area POC and the HS SLIC PM).

In addition, each participating State, Territorial, or Urban Area HS SLIC Sponsoring Organizational representative is required to:

Verify the HS SLIC eligibility status of sponsored employees (including contractors) on an annual basis, ensuring that each employee they sponsor (1) meets the eligibility requirements and (2) uses the system within these rules; and

Maintain the user roster for the organization, and remove from the system any sponsored employee no longer eligible.

Finally, each HS SLIC member must

- Be part of a single Sponsoring Organization approved by the associated Voting Member;
- Revalidate their position, title, and email address at least annually; and
- Change their system password and agree to user rights and responsibilities every 90 days or their access will be terminated.



8.2 Will contractors to DHS have access to the system?

Yes. Both the HSIN-Intelligence portal and, within it, the HS SLIC compartment, is administered by a mix of both I&A government officers and contractors and all contractor work is overseen by DHS contracting officers and assigned I&A government staff. The number of contractors is minimized to only those needed. I&A contractors, specifically, may be utilized in a role to support directly the analytical intelligence functions and activities for which this platform serves, and/or may support directly the management/administration of the platform in support of the HSIN-Intelligence system in general or directly for the HS SLIC. In addition, currently there are several technology contractors who have access to the system as they build the information network and the database. Such contractors or other information technology professionals are registered and managed using the same auditing and controls as every other HSIN-Intelligence user. All contractors are required by contract provisions to sign non-disclosure agreements, and while serving in any role are bound by the same policies, laws, rules, and obligations that apply for any other individuals that have been vetted and authorized access to the platform in addition to the limitations included or contained within the contract or Statement of Work that applies.

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

(b)(2) High

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

(b)(2) High

Sharing with foreign partners are a critical part of fulfilling our mission of defending the homeland. (b)(2) High

(b)(2) High



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

(b)(2) High
[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

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

(b)(2) High
[Redacted]

- [Redacted]
 - [Redacted]
 - [Redacted]
- [Redacted]



(b)(2) High I&A does not include U.S. person information in this metadata.

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

All DHS personnel having access to HS SLIC must conduct their activities in accordance with the guidance provided in DHS memorandum, Intelligence Oversight Basics, dated March 27, 2006. The memorandum describes core concepts related to I&A's mission, and the collection, retention, and dissemination of information about U.S. persons. DHS users also have access to system training that includes discussion of privacy aspects of the system, including required I&A annual training on EO 12333. Non-DHS intelligence professionals within the HS SLIC, who are also employed elsewhere within the Intelligence Community, have similar requirements for intelligence oversight training in accordance with Executive Order 12333. State and local authorities have their own training programs that are used to teach staff how to comply with issued guidance (see above at 5.6).

8.8 Is the data secured in accordance with FISMA requirements? If

The Certification and Accreditation process is currently being conducted. An Authority to Operate is expected to be granted before January 31, 2008. The platform will not be utilized in operational form until that approval to operate is obtained.

8.9 Privacy Impact Analysis

Access to the portions of HSIN-Intelligence containing sensitive PII is controlled and protected by a number of technical, procedural, and policy-based safeguards, including, (b)(2) High Access is role-based, and eligibility is reviewed for accuracy. Auditing is used to monitor system use. Overall, these safeguards adequately protect against inappropriate access to and use of information in the system.

Auditing was a major portion of the need for an infrastructure solution separate from the legacy HSIN technology platform. Using the (b)(2) High technology, I&A will be able to perform its mission with a robust compliment of tools to maintain user access control and ensure appropriate conduct by users on the HSIN-Intelligence platform.

Section 9.0 Technology

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

HSIN-Intelligence was developed by (b)(2) High The majority of the system was base capability provided to all (b)(2) High customers. However, the I&A secure portal Statement of Work required the contractor to build additional features.



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

System developers of HSIN-Intelligence recognized from the beginning the need to ensure the integrity, privacy, and security of the sensitive information to be collected, used, and disseminated on the system. All decisions about system design were based on the need to ensure data integrity, embed strong privacy controls, and implement robust security features. (b)(2) High

9.3 What design choices were made to enhance privacy?

(b)(2) High, in order to bolster privacy protections, HSIN-Intelligence requires that a “minimization” process be employed whereby all reports, analyses, assessments, and other products, prior to dissemination by I&A (i.e., posted onto the HS SLIC compartment), are reviewed to assess and determine whether the specific U.S. person identity information is necessary for the use of or understanding of the product by the intended recipients. Thus, for documents disseminated by I&A within the HS SLIC where the U.S. Person information or identity is not necessary to understand the product, the identity information will be “masked” by removing and replacing it with “a U.S. Person,” “USPER,” or some similar marking, as appropriate. Where an I&A product on the HS SLIC will include U.S. person identifying information, the product itself will carry a warning stating that “This product contains U.S. Person Information” or words to that effect. This is done in accordance with I&A’s Intelligence Oversight obligations and policies, and the I&A Information Handling Guidelines.

As discussed above, (b)(2) High technology was selected because it provides the program management staff the tools necessary for I&A to comply, not only with the Intelligence Community’s oversight responsibilities uniquely applicable within HSIN Intelligence to I&A, but to facilitate compliance with the Privacy framework (e.g., 28 CFR Part 23) for any other organization with access to, including the capability to post and exchange its own information within, certain portions of the portal. This was a specific design choice made to enhance accountability surrounding the possible use of personally identifiable information in the HS SLIC portion of HSIN-Intelligence.

Conclusion

HSIN-Intelligence was deployed as an Internet-based platform to ensure compatibility and interoperability among interrelated communities of users securely exchanging critical sensitive information relevant to their official domestic security missions while also ensuring that the integrity and privacy of individuals’ data was maintained consistent with their own applicable standards, laws, policies, and procedures. For the HS SLIC compartment of the portal, U.S. person identifying information is routinely minimized unless the information is required for understanding the specific intelligence report, analysis, assessment or other product. This significantly mitigates the privacy risks for information accessible through HSIN Intelligence. For those documents that do contain personally identifiable information, a number of safeguards are in place to protect the privacy and integrity of the information. The registration



protocol for HSIN-Intelligence is identified as a critical function for ensuring that members are properly validated; this is particularly true for HS SLIC compartment access, the only portion of HSIN Intelligence which contains PII. It serves as a key component in role-based access to HSIN-Intelligence and mitigates the risk of inappropriate access to information. Basic auditing capabilities are implemented in all areas of HSIN-Intelligence. I&A will continue to track developments in policy and technology that can be applied continually to improve the privacy and security of the system.



Responsible Officials

(b)(6)

Program Manager
Office of Intelligence and Analysis

(b)(6)

(b)(6)

CIO and Deputy Director for Information Sharing and Knowledge Management
Office of Intelligence and Analysis

(b)(6)



Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security