



Privacy Impact Assessment
for the

Compliance Tracking and Management System

May 22, 2009

Contact Point

**Claire Stapleton
Privacy Branch Chief
Verification Division**

Reviewing Official

**Donald Hawkins
Chief Privacy Officer
United States Citizenship and Immigration Services
(202) 272-8000**

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



Abstract

The Verification Division of the United States Citizenship and Immigration Services (USCIS) operates the Compliance Tracking and Management System (CTMS). CTMS collects and uses information necessary to support monitoring and compliance activities for researching and managing misuse, abuse, discrimination, breach of privacy, and fraudulent use of USCIS Verification Division's verification programs, the Systematic Alien Verification for Entitlements (SAVE) and E-Verify. This is a new system that requires publication of a Privacy Impact Assessment and System of Records Notice.

Overview

The United States Citizenship and Immigration Services (USCIS) Verification Division supports two congressionally authorized programs, the Systematic Alien Verification for Entitlements (SAVE) and E-Verify programs.¹ Congress mandated SAVE to provide government agencies with citizenship and immigration status information for use in determining an individual's eligibility for government benefits. The SAVE program allows federal, state, and local government benefit-granting agencies, as well as licensing bureaus and credentialing organizations to confirm the immigration status of non-citizen applicants, by submitting to SAVE certain information supplied by the benefit applicant. Congress mandated E-Verify for use by employers to determine whether an employee is authorized to work in the United States at the time that he or she begins working.² The E-Verify program allows participating employers to verify the employment eligibility of all newly hired employees, by submitting to E-Verify specific information supplied by the employee.³

The SAVE and E-Verify programs rely on the Verification Information System (VIS) as the underlying technical infrastructure as described in the VIS system of records notice (SORN) and Privacy Impact Assessments PIAs.⁴ As part of the mandate to implement the SAVE and E-Verify programs, Congress imposed various legal and operational requirements including requirements to insulate and protect the privacy and security of collected information, to prevent unauthorized disclosure of personal information, and to have safeguards against the system resulting in unlawful discrimination. In order to ensure that these requirements are met, the Verification Division created the Monitoring and Compliance Branch (M&C) which, as one might imagine, will be responsible for two distinct set of tasks: monitoring and compliance. M&C will monitor the verification transactions within VIS to identify potential cases of misuse, abuse, discrimination, breach of privacy, or fraudulent use of SAVE and E-Verify. When M&C identifies certain defined anomalous activities through these monitoring efforts they may take additional

¹ The specifics of the SAVE and E-Verify programs can be found on the DHS web site and in the Verification Information System (VIS) System of Records Notice (SORN) and Privacy Impact Assessments (PIA).

² Authority for SAVE can be found in the Immigration Reform and Control Act of 1986 (IRCA), Public Law (P.L.) 99-603, The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), P.L. 104-193, 110 Stat. 2168, and in Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub. L. 104-208, 110 Stat. 3009. Authority for E-Verify can be found in Title IV, Subtitle A, of IIRIRA, Pub. L. 104-208, 110 Stat. 3009, and the Basic Pilot Extension Act, Pub. L. No. 107-128 (2002); and Basic Pilot Program Extension and Expansion Act, Pub. L. No. 108-156 (2003).

³ In most cases, E-Verify queries are only to be conducted on new employees. However, there are certain categories of employers who may verify their current workforce. Executive Order 13466, amending Executive Order 12989 [73 FR 33286 (June 11, 2008)], and the Secretary of Department of Homeland Security designation of June 13, 2008 together require all Federal contractors to verify existing employees through E-Verify. A regulation requiring federal contractor use of E-Verify for existing employees is pending promulgation.

⁴ The Verification Information System SORN, DHS-USCIS-004, December 11, 2008, 73 FR 75445 and PIAs associated with VIS and the SAVE and E-Verify programs can be found at www.dhs.gov/privacy.



compliance steps to verify and correct these activities. These activities are referred to as noncompliant behaviors.

The M&C Branch is developing detailed procedures for both monitoring the verification transactions in VIS and for performing compliance activities on defined non-compliant behaviors. For example, one type of behavior is associated with the misuse of SSNs. For this behavior M&C will identify when a single SSN is used multiple times for employment authorization verifications through E-Verify. It would not be uncommon for a single individual to be verified several times through E-Verify as one person may hold multiple jobs or change jobs frequently, but it would be unusual for a single individual to hold 30 or 40 jobs simultaneously. M&C has developed procedures for identifying when a certain threshold number of verifications of a single SSN would be likely to indicate some type of misuse. If this threshold is met then M&C would conduct certain specific compliance activities that may involve collecting or looking at information from outside of VIS. This might include contacting or visiting an employer to research the issue and determine if there is: a system problem which the Verification Division needs to correct; if there is a user misunderstanding which requires additional training for the employer, or potentially fraudulent activity which may need to be reported to law enforcement agency.

In most cases compliance activities will be undertaken based on monitoring defined behaviors in VIS. However, there are some behaviors which may not necessarily be indicated by monitoring VIS. For example, employers are required to conspicuously post notification of their participation in E-Verify to their employees. This notification provides the employees with information concerning their rights and responsibilities regarding E-Verify, including contact information. Obviously there is no information in VIS that would indicate whether an employer had actually posted these notices. Compliance activities around the non-compliant behavior of failing to post the required notices would most likely occur based on a complaint/hotline report or during a compliance visit researching another potential behavior. M&C might also identify potential non-compliant behaviors from media reports or tips for law enforcement agencies.

The management of compliance activities and storage of the supporting information will be handled by the Compliance Tracking and Management System (CTMS) the subject system of this PIA. The basic capabilities of CTMS include: monitoring and compliance activity tracking, data and document collection and storage, incident management tracking and incident history searching, reporting, and workflow management.

CTMS will be developed in increments. Initially, it will be based on existing and new consumer-off-the-shelf (COTS) technology products required to meet basic capabilities. This includes database and analysis technologies that are currently available in the Verification Division, and new data storage and business process workflow systems. It is anticipated that CTMS will also grow to include additional and more sophisticated analytic and information management functionality. As the system develops, USCIS will update the SORN and PIA as appropriate.

Initially, CTMS will be used to support a range of monitoring and compliance activities, which include researching and documenting the following non-compliant agency or employer categories of behaviors:

- Fraudulent use of Alien-Numbers (A-Numbers) and SSNs by E-Verify users;
- Termination of an employee because he receives a tentative non-confirmation (TNC)⁵;

⁵ A tentative non-confirmation (TNC) occurs when E-Verify is unable to match the information provided by the employer with the information in DHS records. Employees can choose to contest the TNC by contacting either SSA or DHS and following the established procedures.



- Failure of an employer to notify DHS, as required by law, when an employee who receives a final non-confirmation (FNC) is not terminated;
- Verification of existing employees (as opposed to new hires);
- Verification of job applicants, rather than new employees (pre-screening);
- Selectively using E-Verify or SAVE for verifications based on foreign appearance, race/ethnicity, or citizenship status;
- Failure to post the notice informing employees of participation in E-Verify;
- Failure to use the E-Verify, consistently or at all, once registered;
- Failure of SAVE agency to initiate additional verification when necessary;
- Unauthorized searching and use of information by a SAVE agency user; and
- Fraudulent use of visas, permits, and other DHS documents by SAVE users.

MONITORING

Generally speaking these categories of behaviors, as described more fully below, will usually be identified by monitoring the information in VIS. They may also be identified based on tips received from affected individuals, various law enforcement agencies, or the media. They may be the result of a Privacy Act redress request. With regard to the behavior of failing to post appropriate notice, it could be identified during a compliance visit to an employer for research on another potential non-compliant behavior. As noted above, monitoring for behaviors is complicated by the fact that not all anomalous transactions in VIS will necessarily indicate a non-compliant behavior. Thus M&C is establishing thresholds to narrow their research to find the most likely cases of non-compliant behaviors. Once M&C has established there is likely an occurrence of a non-compliant behavior M&C will extract the minimal amount of data necessary to identify possible non-compliant behavior. The minimal amount of data necessary is only data that is directly related to making a determination about the alleged non-compliant behavior. That data is entered into CTMS to conduct compliance activities.

COMPLIANCE

Compliance activities are meant to stop misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify. These activities could result in a range of outcomes including correcting a SAVE or E-Verify system problem, providing additional SAVE and E-Verify user training or assistance to ensure correct use of these systems, turning off access to SAVE and E-Verify for individual users who continue to misuse the systems, or contacting law enforcement agencies in the case of suspected illegal activities.

Once the monitoring analyst determines a behavior meets the threshold the compliance analyst may begin researching the behavior. The specific research will vary depending on the behavior but generally could involve contacting or visiting the SAVE or E-Verify user, (a government agency or employer respectively) to notify them that they may not be in compliance with program requirements. This notification will allow the SAVE and E-Verify user to remediate or explain the issue. In some cases, if the program user is unable to remediate or explain the issue, additional research may be conducted, including collecting supporting information from other sources beyond VIS. This may include the collection of such information as E-Verify or SAVE created documents (such as an E-Verify Tentative Non-Confirmation (TNC) letter or referral letters), Forms I-9 and copies of supporting documents, employment offer or



termination letters, information collected during interviews with SAVE and E-Verify users⁶ related to program participation.

M&C efforts are focused on misuse of the E-Verify and SAVE program. M&C will concentrate compliance operations, such as interviews or document requests, directly on the users of these systems—the employers or government agencies, rather than on the individuals who are verified. M&C would only contact a SAVE or E-Verify subject directly when a compliance activity is based on a redress request or hotline tip. When appropriate, interviews will be conducted in a confidential manner. Information received during interviews and complaints will be kept confidential unless required to be released based on legal necessity. If a particular behavior is substantiated, the Verification Division will take appropriate steps to correct this behavior including requiring additional training, restricting access to SAVE or E-Verify, or referral to a law enforcement agency for further action.

Below is a brief description of each behavior, the monitoring effort associated with the behavior, and a description of the documents that might be collected during the compliance activities.

BEHAVIORS

Fraudulent use of A-Numbers and SSNs by E-Verify users

Congress mandated that E-Verify prevent misuse of the verification process. Further, other various legal mandates prohibit the fraudulent use of government identification documents.⁷

Monitoring

M&C will begin monitoring to identify fraudulent use of SSNs and A-numbers which may be indicated by repeated use of the same SSN or A-number. This behavior could also be identified by a tip from an associated individual such as a fellow employee, law enforcement source, or media source. For example, this behavior could be identified by examining transactional records in VIS and detecting a large number of identical SSNs or A-numbers. Because a single SSN or A-number may legitimately be used multiple time for verification purposes M&C will establish thresholds over which further research would be conducted. Once the most likely cases of fraudulent use have been identified, M&C could research additional information in VIS such as whether the name and birth date are identical. After a monitoring analyst has determined that there is potential fraud and that they have exhausted their research in VIS they may refer the information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that demonstrate the source of a particular SSN or A-number. These may include the Form I-9 and copies of its supporting documents as listed on the Form I-9.

Termination of an employee based on receiving a tentative non-confirmation (TNC)

Congress mandated that employers using E-Verify neither terminate nor discriminate against an employee based on a TNC.⁸ If an employee receives a TNC from E-Verify, the employer must inform the

⁶ An E-Verify user is anyone in a company/agency enrolled with E-Verify, who actually uses E-Verify to verify other individuals, or others who have a relationship/association with E-Verify such as a designated point of contact or Memorandum of Understanding (MOU) signatory. Similarly, SAVE users are deemed to be individuals who actually use SAVE to verify other individuals, or others who have a relationship/association with SAVE. Users do not include individuals who have no relationship with SAVE or E-Verify except that they may have been verified through these programs.

⁷ Immigration and Nationality Act, §274C., Identity Theft and Assumption Deterrence Act of 1998, §003 (d)(3), Immigration Reform and Control Act, §103(a)(1), Social Security and Benefits Act, Identity Theft and Assumption Deterrence Act of 1998, §003 (d)(3).



employee about the TNC and ask them if they want to contest. If the employee chooses to contest the TNC, the employer must give them a referral letter generated by the E-Verify system and refer them to the Social Security Administration (SSA) or DHS, as appropriate, to correct any discrepancies in his or her record. Employers are prohibited from terminating the employee on the basis of the TNC unless the employee chooses not to contest the TNC. Terminating the employee during the time between the TNC and a final determination of either Employment Authorized (EA) or a Final Non-confirmation (FNC), on the basis of a TNC, is a violation of the employee's rights and a misuse of the system, and may indicate discrimination by the employer.

Monitoring

M&C will monitor for this behavior in VIS by examining such things as VIS transactional records where there a particular employer has a large number of uncontested TNCs. Transactional analysis could potentially indicate that an employer did not offer employees the opportunity to resolve the TNCs, and instead terminated them. This behavior could also be indicated by a tip from an associated individual such as a fellow employee, law enforcement source, or media source. Once a monitoring analyst has determined that there is a potential inappropriate termination, they may refer this information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that demonstrate that an employee was actually terminated. These may include the Form I-9 and copies of its supporting documents and employment offer and termination letters. Additional documents to be collected or reviewed include E-Verify produced documents such as the employer's copy of the TNC or referral letter.

Failure of an employer to notify DHS when an employee who receives a final non-confirmation (FNC) is not terminated

Congress mandated that employers using E-Verify should notify DHS if they decide to retain an employee who has received an FNC.⁹ That is, while an employer may not terminate or take any adverse employment action against the employee on the basis of TNC, if an employee receives an FNC, the employer may terminate the employee or they may choose to retain the employee and notify DHS of their decision or action. The process for DHS notification consists of selecting "employee not terminated" as the closure code during the verification process. This option to retain and notify is an important safeguard should an employer have knowledge that a mistake has been made in the verification process.

Monitoring

M&C will monitor for this behavior in VIS by examining transactional records in VIS where there is no closure, or a significant amount of time has passed before closures are made to verification cases that resulted in FNCs. Such transactions could potentially indicate an employer is retaining employees who have received FNCs but is not notifying DHS about the retention as required by law. This behavior could also be indicated by a tip from an associated individual such as a fellow employee, or a law enforcement or media source. Once a monitoring analyst has determined that there is potential inappropriate retention they may refer this information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that demonstrate that an employee was actually terminated, such as copies of termination letters. Additional documents to be

⁸ IIRIRA §403(a)(4)(B)(iii)

⁹ IIRIRA §403(a)(4)(C)(i)



collected or reviewed include E-Verify produced documents such as the employer's copy of the TNC or referral letter.

Verification of existing employees

Congress mandated that E-Verify be used to verify work authorization for new hires within three days of their hire date. Employers are not allowed to verify existing employees.¹⁰ Verification of existing employees could lead to selective verification and possible discrimination. There are certain instances where verification of existing employees may be authorized by law. This will be considered during the monitoring activities.

Monitoring

M&C will monitor for this behavior in VIS by examining such things as transactional records where the Verification Date is inappropriately well beyond the hire date, or where there are multiple verifications for one employee, or even where there are a large number of verifications considering the employer's size and business. These types of transactions could potentially indicate employer verifying of existing employees. This behavior could also be identified by receiving a tip from an affected individual, or a law enforcement or media source. Once a monitoring analyst has determined that there is potential existing employee verification they may refer this information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that demonstrate when an employee was actually hired. These include the Form I-9 and employment offer letters.

Verification of job applicants, rather than new employees (Pre-screening)

Congress mandated that E-Verify be used to verify the employment status of new employees, and was specifically not authorized to be used to screen applicants.¹¹ Verifying employees rather than applicants minimizes the opportunity for an employer to engage in the practice of rejecting applicants for improper reasons including discrimination on the basis of the appearance of foreign nationality, ethnicity/race, citizenship status, or perceived work authorization status. It also eliminates the problem of an employer pre-screening applicants and then rejecting applicants on the basis of receiving TNCs without giving them a fair chance to update their records with SSA and/or DHS.

Monitoring

M&C will monitor this behavior in VIS by examining such things as inconsistencies or abnormalities in transactional records in VIS. For example, an unusually high number of "invalid" closure codes or "blank" codes per user or employer could indicate either a potential procedural error or pre-screening attempt that was interrupted by an employer action. This behavior could also be identified by receiving a tip from an affected individual, or a law enforcement or media source. Once a monitoring analyst has determined that there is an instance of potential pre-screening they may refer this information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that demonstrate when an employee was actually hired. These include the Form I-9 and employment offer letters. Additional documents to be collected or reviewed include E-Verify-produced documents such as the employer's copy of the TNC or referral letter.

¹⁰ IIRIRA §403(a)(3)(A)

¹¹ IIRIRA §404(d)(4)(B)



Selectively using E-Verify or SAVE for verifications based on foreign appearance, race/ethnicity, or citizenship status

Congress mandated that SAVE and E-Verify be used to verify immigration status of benefit applicants and employees. The programs were authorized to be used to verify all individuals, and cannot be used to selectively verify individuals. Verifying all applicants and employees minimizes the opportunity for a benefit provider or employer to engage in discrimination on the basis of the appearance of foreign nationality, ethnicity/race, citizenship status, or perceived work authorization status.

Monitoring

M&C will monitor for this behavior in VIS by examining such things as inconsistencies or abnormalities in transactional records in VIS. For example, an unusually high number of country codes from one country by one employer could indicate selective verifications for the SAVE program. Because M&C would not have access to the information necessary to monitor selectivity based on foreign appearance and race/ethnicity, this would more likely be indicated by a tip from an associated individual such as a fellow employee, a law enforcement or media source. Once a monitoring analyst has determined that there is a potential selective verification they may refer this information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that demonstrate that verification has been done selectively. These may include the Form I-9 and employment offer letters or benefit application information. Additional documents to be collected or reviewed include E-Verify and SAVE produced documents.

Failure to post the notice informing employees of participation in E-Verify

Congress mandated that E-Verify be used to verify the employment status of all new employees of E-Verify participants. In order to ensure that new employees are aware of this process and of their rights and obligations under E-Verify, the Verification Division requires that all E-Verify employers conspicuously post this information as provided by the Verification Division. Posting this information minimizes the employer's opportunity to engage in selective verification which is prohibited under law.¹²

Monitoring

M&C would not be able to monitor this behavior in VIS. This behavior could be identified by receiving a tip from an affected individual, or a law enforcement or media source, but would most likely be found as an adjunct to research of another potential behavior. M&C would open a compliance case indicating that a potential case of failing to provide notice has been identified.

Compliance

During the compliance activities M&C would probably not collect documents. This behavior would be noted through visual inspection or from information provided by others.

Failure to use E-Verify, consistently or at all for employees, once registered

Congress mandated that E-Verify be used to verify the employment status of all new employees, and was specifically not authorized to be used selectively.¹³ Inconsistent verification of employees could suggest that an employer is engaging in the practice of terminating employees for improper reasons including discrimination on the basis of the appearance of foreign nationality, ethnicity/race, citizenship status, or perceived work authorization status.

¹² IIRIRA §404(d)(4)(A) and (C)

¹³ *Id.*



Monitoring

M&C may be able to monitor for this behavior in VIS by examining such things as inconsistencies or abnormalities in transactional records in VIS, such as significantly lower number of verifications than expected for a particular type of employer. This behavior could also be identified by receiving a tip from an affected individual, or a law enforcement or media source. Once a monitoring analyst has determined that there is a potential inconsistent use of E-Verify they refer this information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that demonstrate when an employee was actually hired. These may include the Form I-9 and employment offer letters.

Failure of SAVE agency to initiate additional verification when necessary

SAVE verification queries that are not automatically verified return a response to the SAVE user that additional manual verification is required. Congress mandated that no benefit could be refused based on response from SAVE until the verification subject is given a chance to establish their identity. The Verification Division is interested in identifying when a SAVE agency does not conduct appropriate additional verification, which could thereby deny the verification subject the benefit to which they were applying.

Monitoring

M&C will monitor for this behavior in VIS by examining VIS data for large numbers of verification queries that result in response of requiring additional verification, but which no additional verification process takes place. This behavior could also be identified by receiving a tip from an associated individual, or a law enforcement or media source. Once a monitoring analyst has determined that a SAVE user potentially did fail to initiate additional verification when needed they refer this information to a compliance analyst.

Compliance

During compliance activities M&C may review and collect documents that would confirm whether the behavior had occurred. These may include any document offered by the SAVE user to demonstrate the application or request that required the verification in the first place- these may include an application for a particular benefit or credential, in addition to any supporting documents including copies of the specific government documents. Additional documents to be collected or reviewed include E-Verify and SAVE produced documents.

Unauthorized searching and use of information by a SAVE agency user

The Verification Division is interested in identifying inappropriate uses of the SAVE program such as running multiple verifications of information not for actual SAVE purposes, but in order to determine if certain information is real and this could be used for such purposes as identity theft.

Monitoring

M&C will monitor for this behavior in VIS by examining VIS data for large numbers of verification queries that result in a response of requiring additional verification, but which no additional verification process takes place. This behavior could also be indicated by receiving a tip from an associated individual, or a law enforcement or media source. Once a monitoring analyst has determined that a SAVE user potentially is running false verifications they may refer this information to a compliance analyst.

Compliance

During the compliance activities M&C may review and collect documents that would confirm whether the behavior had occurred. These may include any document offered by the SAVE user to



demonstrate the actual use of a particular government document – such as an application for a particular benefit or credential, in addition to any supporting documents including copies of the specific government documents. Additional documents to be collected or reviewed include SAVE produced documents.

Fraudulent use of visas, permits, and other DHS documents by SAVE users

Congress mandated that SAVE prevent misuse of the verification process, and various other legal mandates prohibit the fraudulent use of various government documents.¹⁴ M&C will identify repeated use of the same government documents (to include such things as visas, DHS and Department of State issued benefit documents, and passports), as it may indicate fraudulent use of these documents.

Monitoring

M&C will monitor for this behavior in VIS by examining such things as transactional records in VIS where a large number of identical government document numbers appear. These types of transactions could potentially indicate fraudulent use of these identification numbers. This behavior could also be identified by receiving a tip from an associated individual, or a law enforcement or media source. Once a monitoring analyst has determined that a SAVE user potentially fraudulently misused a DHS document for verification purposes they may refer this information to a compliance analyst.

Compliance

During compliance activities M&C may review and collect documents that would confirm whether the behavior had occurred. These may include any document offered by the SAVE user to demonstrate the actual use of a particular government document – such as an application for a particular benefit or credential, in addition to any supporting documents including copies of the specific government documents. Additional documents to be collected or reviewed include SAVE produced documents.

Section 1.0 Characterization of the Information

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

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

Once M&C has established there is likely an occurrence of a non-compliant behavior, M&C will extract the minimal amount of data relevant to the possible non-compliant behavior and enter the data into CTMS.

Monitoring

For monitoring purposes CTMS may contain any data element in VIS that suggests the occurrence of a non-compliant behavior. However, only the relevant data elements that actually suggest the non-compliant behavior will be transferred into CTMS. This information includes individual's name; birth information; citizenship and nationality information; DHS and Department of State immigrant/non-

¹⁴ Immigration and Nationality Act, §274C., Identity Theft and Assumption Deterrence Act of 1998, §003 (d)(3), Immigration Reform and Control Act, §103(a)(1), Social Security and Benefits Act, Identity Theft and Assumption Deterrence Act of 1998, §003 (d)(3).



immigrant information (e.g., arrival and departure information); identification information such as SSN, A-Number, passport and visa information; and SAVE and E-Verify user contact information such as phone numbers, email addresses, physical addresses.

In addition, CTMS will contain information from complaints, questions, and tips from SAVE and E-Verify users and individuals subject to immigration status verification or employment authorization verification provided by callers to the Verification Call Center, or redress requests directly from verification subjects, or law enforcement tips, or media leads, any of which might suggest the occurrence of a non-compliant behavior. This information might include any of that information listed in the preceding paragraph already contained in VIS, as well as information describing the reported non-compliant behavior and the verification subject's contact information such as phone number, email address, or physical address.

Compliance

For compliance purposes CTMS will utilize all the information described above for monitoring. In addition it will contain information collected during compliance activities including, but not limited to: SAVE and E-Verify created documents such as TNC, referral, or compliance letters; Forms I-9 and supporting documents, employment offer and termination letters, benefit and credential applications and supporting documents, SAVE and E-Verify user interviews, and interviews with the verification subjects in the case of a redress request or hotline tip submitted by a verification subject.

This system contains personally identifiable information (PII) on four categories of individuals, any of whom may be either U.S. citizens or non-U.S. citizens. These include:

1. Verification Subjects: Individuals who are the subject of E-Verify or SAVE verifications and whose employer is subject to compliance activities,
2. E-Verify or Save Program Users: Individuals who use, are enrolled users, or have an agency or employment responsibility associated with the SAVE or E-Verify programs,
3. Complainants: Individuals who have contacted the Verification Division or publicly reported potential cases of misuse, abuse, discrimination, breach of privacy, and fraudulent use of Verification Division's verification programs, the Systematic Alien Verification for Entitlements (SAVE) and E-Verify, and
4. DHS Employees: Verification Division employees or contractors who are involved in SAVE and E-Verify monitoring and compliance activities.

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

The information in CTMS comes primarily from the following four sources:

1. Information from VIS that suggests non-compliant behavior. This information could include name and date of birth on SAVE and E-Verify subjects and user transactional information;
2. Information from SAVE and E-Verify subjects who submit tips or redress requests including the contents of those requests;
3. Information from media or law enforcement organizations referrals or requests; and
4. Information collected from compliance reviews undertaken by the M&C staff which has been provided by the E-Verify employer or SAVE user regarding the compliance review.



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

Information is collected, used, disseminated, and maintained to support monitoring and compliance efforts to verify and remedy patterns of irregular use that might indicate misuse, abuse, discrimination, breach of privacy, or fraudulent use of SAVE and E-Verify. Monitoring and compliance activities can combat fraud and misuse by ensuring the integrity of E-Verify and SAVE by detecting, deterring, and remedying improper use of the system, safeguarding PII, preventing the fraudulent use of counterfeit documents, and referring instances of fraud, discrimination, and illegal or unauthorized use of the system to enforcement authorities.

1.4 How is the information collected?

Information will be collected from VIS and placed into CTMS from the monitoring and compliance analysis of user interactions with Verification programs and from research conducted on potential occurrences of defined behaviors. Information will be collected from VIS based on specified queries regarding defined behaviors. Information will be collected from E-Verify and SAVE users (employers or government clients, respectively) based on inquiries or site visits to the E-Verify employers and SAVE agencies for the investigation of a prohibited behavior as described in Section 1.3 above. The information collected from compliance activities will be collected by requesting information directly from E-Verify and SAVE users, by reviewing documents related to verification, or by interviewing individuals such as verification users, and in the case of a redress request or hotline tip, the verification subjects. Information will be collected from tips of occurrences of a prohibited behavior from Verification Call Center, law enforcement agencies, and the media. The information collected from the Call Center will be collected as part of the Call Center normal activity of collecting information from callers.

1.5 How will the information be checked for accuracy?

One of the fundamental purposes of M&C is to review information to determine whether it is accurate and in doing so, whether the information will indicate whether a non-compliant behavior has occurred. The information is collected into CTMS from VIS and is verified, by comparing it with the actual documents submitted for the original verification. In addition, interviewing users and verification subjects can determine if there are inconsistencies in the information.

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

The Verification Division has the authority to prevent misuse, abuse, discrimination, breach of privacy, and fraudulent use of the verification process, under the following specific laws: the Immigration Reform and Control Act of 1986 (IRCA), Public Law (P.L.) 99-603; The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), P.L. 104-193; Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), P.L. 104-208; 18 U.S.C. § 3291, and Immigration and Nationality Act (INA) Title 8 United States Code.



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

CTMS will consist of information authorized for the protection of the integrity of E-Verify and SAVE, including protection of individual rights, civil liberties, and privacy. It is intended that the information collected and used in CTMS will be the minimal amount of information needed to confirm or disprove an identified, suspected occurrence of a prohibited behavior. The amount of information collected cannot always be identified before research begins; however, the monitoring and compliance activities are being defined in standard operating procedures (SOPs) that include procedures to limit the collection of information to only the information required. Furthermore, the Verification Division Privacy Branch will work closely with the Monitoring and Compliance Branch to ensure that the monitoring and compliance activities are developed with a goal of minimizing data collection.

Section 2.0 Uses of 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.

The Verification Division will use the information in CTMS to support both monitoring and compliance activities associated with potential misuse, abuse, discrimination, breach of privacy, and fraudulent use of USCIS Verification Division's verification programs—SAVE and E-Verify. Initially, the information will be used to identify and mitigate against a selection of prohibited behaviors. As technological and operational procedures and systems develop, additional behaviors will be approved for monitoring and compliance. The immediate monitoring and compliance activities will focus on the following prohibited categories of behaviors:

- Fraudulent use of Alien-Numbers (A-Numbers) and SSNs by E-Verify users;
- Termination of an employee because he receives a tentative non-confirmation (TNC);
- Failure of an employer to notify DHS, as required by law, when an employee who receives a final non-confirmation (FNC) is not terminated;
- Verification of existing employees (as opposed to new hires);
- Verification of job applicants, rather than new employees (pre-screening);
- Selectively using E-Verify or SAVE for verifications based on foreign appearance, race/ethnicity, or citizenship status;
- Failure to post the notice informing employees of participation in E-Verify;
- Failure to use the E-Verify, consistently or at all, once registered;
- Failure of SAVE agency to initiate additional verification when necessary;
- Unauthorized searching and use of information by a SAVE agency user; and
- Fraudulent use of visas, permits, and other DHS documents by SAVE users.



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

Data is analyzed to identify behaviors that indicate misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify systems. This consists of searching for pre-defined patterns and data irregularities and applying thresholds against this data which may indicate that a particular non-compliant behavior has occurred. These are described more fully in the Overview section of this PIA.

2.3 Does the system use commercial or publicly available data? If so, please explain why and how it is used.

CTMS will contain some publicly available data, such as information gathered as a result of monitoring and compliance analysis of news reports that might indicate a potential misuse or abuse of the verification process or publicly related information related to employment statistics prepared by federal state and local agencies. The Verification Division does not use commercial data aggregators at this time.

2.4 Privacy Impact Analysis: What types of controls are in place to ensure that information is handled in accordance with the above described uses?

CTMS is operated in a secure environment with appropriate access controls to ensure that individuals who access the system have the appropriate authority and need to see the information. Prescribed roles and responsibilities with corresponding access controls will protect the integrity of the system. In addition, the information use is monitored and logged, and all users will receive detailed training in the appropriate use of the system to ensure all procedures are followed.

Section 3.0 Retention

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

3.1 How long is information retained?

DHS will retain all the information in CTMS for 10 years, or as long as the information is part of an active and ongoing investigation or litigation by enforcement agencies, to correspond with the retention period for the primary information source system VIS. This 10-year retention period is based on the statute of limitations for most types of misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify (under 18 U.S.C. § 3291, the statute of limitations for false statements or misuse regarding passports, citizenship or naturalization documents). The information will be retained for the 10 year period regardless if it is immediately used for a particular investigation or litigation as it may be significant for future research for these limited purposes.



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

No. The Verification Division will work with NARA to gain approval for the 10-year retention schedule.

3.3 Privacy Impact Analysis: What are the risks associated with the length of time data is retained, and how are those risks mitigated?

If approved, the 10-year retention period will accommodate the legal business needs and purpose of collection. The information will be secured with a full range of technical, operational, and management controls as described below in Sections 8 and 9. Once the information is secured, there is minimal risk associated with the retention of the information as only the minimal amount of information required will be retained for the minimal amount of time necessary.

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 organization(s) is the information shared, what information is shared and for what purpose?

The Verification Division will share monitoring and compliance records associated with the referral of compliance matters with the Immigration and Customs Enforcement (ICE), the USCIS Office of Chief Counsel (OCC), the Office for Civil Rights and Civil Liberties (CRCL), enforcement offices of a DHS SAVE user (e.g., Transportation Security Administration (TSA)), the Privacy Office, and the Office of the Inspector General (OIG), as appropriate, in the event of misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify system.

4.2 How is the information transmitted or disclosed?

The Verification Division will communicate with ICE and other enforcement agencies through referral letters and other intra-departmental communications, which may include secure methods prescribed by the receiving agency. These referral letters will contain the minimum necessary information required by ICE or other recipients for investigation. The Verification Division is currently developing a standard operating procedure for referring misuse or abuse to ICE. These referrals will be sent in accordance with appropriate DHS and USCIS security and privacy controls relating to PII. These include a full array of technical, physical, and operational controls as required by DHS Security Directive 4300A, which requires security controls such as transmission and at-rest encryption, access controls, auditing, retention limits, logging of users' activities, as well as logging and management of electronic extracts per OMB Memorandum 06-16, and security certification and accreditation of CTMS. Users will be held personally responsible for handling this information appropriately.



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 Verification Division will develop procedures and create approved sharing agreements based on DHS guidance for any intra-departmental information sharing. These procedures will include specific controls for transmission and storage security, limitations on use, access controls and auditing, as well as data destruction 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 organization(s) is the information shared, what information is shared, and for what purpose?

USCIS may refer suspected incidents of misuse, abuse, breach of privacy, fraud, or discrimination to the Department of Justice (DOJ), Office of Special Counsel (OSC) for Unfair Employment Practices, and to other federal, state, and local law enforcement organizations for the purpose of responding to incidents. The referral will contain minimum necessary information from CTMS for investigation about the suspected misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify.

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.

Any information shared will be for the very purpose for which it was originally collected. These purposes include the prevention of misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify. Routine Uses A-I cover the sharing of information for these purposes.

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

Information shared outside of USCIS is shared for law enforcement, investigation, and litigation purposes or for corrective action by SAVE user agencies only. This sharing typically involves electronic data excerpts or printed hard copies from CTMS. It is shared in accordance with security procedures established to ensure that only the minimal amount of information is shared with the appropriate parties for the appropriate purposes.



5.4 Privacy Impact Analysis: What privacy risks were identified due to external sharing and were they mitigated?

The Verification Division does not intend to share any information from CTMS through system-to-system connection with external systems. The external information sharing is in the form of a referral, which will contain the minimal amount of information extracted from CTMS for research of the suspected misuse, abuse, discrimination, breach of privacy, and fraudulent use of E-Verify and SAVE. The privacy risk of inappropriate release and use of extracted information will be mitigated by administrative procedures, including the OMB Memorandum 06-16 requirements for logging and destruction of extracted data within 90 days, as well as DHS requirements for transmission and at-rest encryption of data, access controls, and policies on limiting the use of the shared data consistent with approved Routine Uses in the SORN.

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?

Notice is provided by the Federal Register publication of this PIA, the CTMS SORN, and Notice of Proposed Rulemaking, and the PIA and SORN for VIS which inform individuals that the Verification Division will collect and use information for certain purposes associated with preventing misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify information and systems. In addition, notice is provided by consent forms or applications for benefits; the SAVE and E-Verify posters and publications; and by employers, benefit issuing agencies, and user MOUs.

For purposes of incoming calls to the Verification Division from individuals subject to immigration status and work authorization verification, the initial information will be provided directly by the individual, and they will be made aware of the fact that the information will be collected and used. For example, an individual may call the Verification Call Center and assert that they believe they have been discriminated against by an agency through their use of SAVE. To the extent that the Verification Division collects information on one individual from another individual, employer or benefit agency user, notice is provided by the SAVE and E-Verify users' MOUs, this PIA, the CTMS SORN, and the VIS PIA and SORN.

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

The majority of the information in CTMS is not collected directly from individuals. It is collected as part of the monitoring and compliance activities associated with E-Verify and SAVE. Consequently, individuals would not have the opportunity or right to decline to provide information. However, individuals do have the opportunity and right to refuse to provide information to compliance analysts.



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 may indicate that they are providing information in confidence to the compliance analysts. Compliance analysts will attempt to adhere to an individual's request for anonymity, but will release that information if required by law. Information collected from VIS or other systems is limited to the uses consented to when the information was originally collected. Individuals do not have the opportunity or right to consent any additional uses of information in CTMS.

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.

Notice to the public is primarily given through the PIAs and SORNs associated with CTMS and VIS. Notice is given to E-verify users and SAVE users in MOUs, and for individuals who are the subject of immigration verification notice is given through the TNC or referral letters. Individuals whose information is entered into VIS which will be verified in the CTMS are given notice by SAVE and E-Verify procedures that their information is collected as part of their participation in these programs.

Section 7.0 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 that allow individuals to gain access to their information?

CTMS plans to claim an exemption pursuant to 5 U.S.C. 552a(k)(2) of the Privacy Act from certain aspects of the Privacy Act including the requirements for access. Thus, individuals may not have access to all information. However, exemptions to particular subsections of the Privacy Act are justified on a case-by-case basis to be determined at the time a request is made. Individuals may request access to their information by submitting a Freedom of Information Act (FOIA) or Privacy Act request to USCIS in writing clearly marked "Privacy Act Request" or "FOIA Request" respectively at the following addresses:

National Records Center

FOIA/PA Office

P.O. Box 648010

Lee's Summit, MO 64064-8010

Requesters must provide their identifying information, e.g. A-number, SSN, and/or full name, date, and place of birth, and return address. Commercial or governmental agencies are required to provide official address and proof of organizational identity. Each access request is evaluated and access would be allowed provided there are no applicable exemptions to access.



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

Individuals should direct all requests to contest or amend their information contained in CTMS, with appropriate proof of identity, class of admission, and other relevant identifying information, to the FOIA/PA Officer at the address provided in Section 7.1. Depending on the originating source of information, the request may be satisfied within USCIS (e.g., Central Information System (CIS)) or referred to the appropriate agency.

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

For purposes of information associated with monitoring and compliance and interactions with the Verification Division, notice is provided by means of this PIA and the SORN for CTMS.

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

Generally, formal redress is provided whenever possible. If a redress request is made for information that DHS determines it cannot release do to law enforcement purposes no redress is directly available. If the information is later used to pursue legal action against an individual they will have the opportunity to rebut the validity of the information, in the course of the legal process.

7.5 Privacy Impact Analysis: What are the privacy risks associated with the redress available to individuals and how are those risks mitigated?

USCIS offers a formal redress process for individuals, which mitigates risks posed by outdated or incorrect information. The Verification Division plans to claim exemptions from some of the access and redress requirements of the Privacy Act through a rulemaking. Not all access and redress requests will be granted, as this system may be used for certain investigations that may result in law enforcement actions. In other words, DHS is accepting the risk that redress will not be directly provided to all individuals requesting it because of the need to protect the information for law enforcement purposes.

Section 8.0 Technical Access and Security

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

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

CTMS will include authentication requirements at the individual level. Access to information will be limited for each individual depending on his or her assigned and approved role. Procedures which include passwords, restricted access, and appropriate in-place and transmission encryption are consistent



with maintaining the secure CTMS environment. These procedures are documented as part of the CTMS system administration and security documentation.

8.2 Will Department contractors have access to the system?

Verification Division contractors will have access to CTMS.

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

USCIS personnel are the users of CTMS, and they take the mandatory, on-boarding and annual DHS Information Technology security and privacy awareness training. Users will also receive role-based training to emphasize the specific concerns associated with the use of CTMS.

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

CTMS, as a subcomponent of VIS, will undergo an update to the most recent reaccreditation which occurred in April 2008. The accreditation has an expiration date of April 2011.

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

The system will have auditing and historical use tracking designed and built into the CTMS as an integral part of the functionality and maintenance of the secure CTMS environment. Users, who are all USCIS personnel, will be identifiable by their logon information and will be made aware that they are being monitored through logon warning banners. Audit logs will be reviewed when questionable activities are being researched. Auditing will ensure that users will be able to be held accountable for their handling of PII.

Technical and operational security safeguards to control the information collected from the E-Verify and SAVE sites will include: in-place and transmission encryption, access controls, use logging, input controls, media labeling, and policies and training for security policies and procedures.

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 information collected and used for monitoring and compliance can be extremely sensitive. In addition to containing significant amounts of PII, it may contain information that could be used to show that individuals, businesses, or organizations are engaging in potentially illegal activities. Consequently, this information will be protected by a full array of technical, physical, and operational controls as required by DHS Security Directive 4300A. These security controls include transmission and at-rest encryption, access controls, auditing, retention limits, logging of users' activities, as well as logging and management



of electronic extracts per OMB Memorandum 06-16, and security certification and accreditation of CTMS. Users will be held personally responsible for handling this information appropriately.

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 What type of project is the program or system?

This will be an operational system and program that will support various monitoring and compliance activities in the Verification Division.

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

The Monitoring and Compliance Branch is currently in the operational phase, and this is the first iteration of the CTMS solution. CTMS will be in the operational phase of the information technology lifecycle upon the publication of this PIA and accompanying SORN.

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

The current iteration of CTMS will be built on a platform of COTS database, business workflow, and information storage and management located products in secure storage facilities of VIS developed under the privacy guidelines and in compliance with DHS Security Policy 4300A and Federal Information Security Management Act (FISMA) requirements. CTMS users, who are USCIS employees, may access CTMS remotely over accredited secure laptops at E-Verify and SAVE user (employer or government client, respectively) locations during site investigations. Because of the potential for data breaches when using portable media, CTMS laptops will comply with all applicable security controls including OMB Memorandum 06-16, as well as appropriate DHS and FISMA requirements.



The basic capabilities that this system provides include compliance management, basic data storage, incident tracking and searching, and reporting. Search capabilities are defined for the various prohibited behaviors in order to minimize the opportunity to do random and unauthorized searching. Furthermore, auditing capabilities ensure personal accountability.

Responsible Official

Claire Stapleton

Privacy Branch Chief, Verification Division

Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security