



Privacy Impact Assessment
for the

Bond Management Information System Web Version (BMIS Web)

August 25, 2008

Contact Point

Lyn Rahilly

Privacy Officer

U.S. Immigration and Customs Enforcement

(202) 514-1900

Reviewing Official

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The Bond Management Information System/Web Version (BMIS Web) is an immigration bond management database used primarily by the Office of Financial Management (OFM) at U.S. Immigration and Customs Enforcement (ICE). The basic function of BMIS Web is to record and maintain for financial management purposes the immigration bonds that are posted for aliens involved in removal proceedings. ICE has conducted this PIA because the system collects personally identifiable information (PII).

Overview

BMIS Web is owned by the ICE Office of Financial Management (OFM). BMIS Web tracks the life cycle of immigration bonds from the time an individual posts a bond at an ICE Detention and Removal Operations (DRO) field office until the bond is considered closed. BMIS Web is scheduled to launch as a pilot in August 2008, with full deployment scheduled for September 2008. With the deployment of BMIS Web, ICE will retire the predecessor information technology system known as BMIS. ICE is also publishing in the *Federal Register* an updated system of records notice (SORN) for ICE's bond management process and information collections.

Background

In a typical transaction an alien is arrested by ICE officers and is detained. ICE determines the alien is eligible for release on bond and sets a bond amount. A third party posts the bond amount in cash to obtain the alien's release and promises that the alien will satisfy the terms of release, usually to return for a court appearance or voluntarily depart the U.S. at a future date. ICE holds the cash amount of the bond as security to guarantee the obligor will fulfill that promise. Should the alien not satisfy the terms of release, ICE declares the bond breached and the bond amount is forfeited to the U.S. Government.¹

An immigration bond is a formal written guaranty by the obligor (i.e., the person or entity that posts the bond) posted as security for the amount of the bond. The bond assures DHS that all of the conditions of the alien's release will be fulfilled by the obligor. Immigration bonds may be posted for the release from detention of aliens in removal proceedings and/or as voluntary departure bonds.

Immigration bonds may be posted by an individual's or entity's deposit of cash in the full amount of the bond (known as cash bonds) or by surety companies, which guarantee the bond on behalf of a third party (known as surety bonds). If the conditions of a bond are satisfied, the bond must be cancelled and, if a cash bond, the principal and accrued interest returned to the obligor. If a bond is declared breached, the cash deposited will be forfeited to the U.S. Government and accrued interest returned to the obligor. For breached surety bonds, surety companies must pay DHS the full amount of the bond plus interest and penalties.

To post a bond, the obligor completes Form I-352 (Immigration Bond) at the ICE field office, and ICE releases the alien. The information from Form I-352 is then entered into the BMIS Web system to track the life cycle of the bond, which includes payment of interest on the bond and default of the bond amount, among other steps of the cycle. If alien doesn't satisfy the terms of the bond (e.g., fails to appear in court),

¹ The bond principal is security guaranteeing performance by the alien released from detention much like a person's home functions as security for a mortgage loan to a lender. Should the home owner default on the terms of his loan, the lender may foreclose on the house; should the alien not satisfy the terms of release, the person (or the surety company) who posted the bond forfeits the bond money.



the bond is considered breached and the bond principal is forfeited to the U.S. Government. All of these bond activities are tracked in BMIS Web.

Not all of the data requested on the Form I-352 is entered into BMIS Web. Some of the information on the I-352 (such as indemnitor information) is retained on the paper form and used for enforcement of the immigration bond. This PIA will not discuss data elements not entered into BMIS Web because ICE is conducting this PIA on the BMIS Web system and not the Form I-352.

BMIS Web

BMIS Web interfaces with the ICE Federal Financial Management System (FFMS) with regard to all cash bond transactions, such as the posting of the cash bond and the disbursements paid to the individual who posted the bond, in order to record the cash received and disbursed on the general ledger of the financial records. BMIS Web also interfaces with the ICE Debt Collection System (DCOS) for any surety bonds on which amounts are owed to ICE and an invoice must be sent to the surety company or bonding agency. DCOS tracks the invoice from the time it is created to the time it is paid. ICE plans to retire DCOS in the near future, at which point this function will be performed by FFMS.

BMIS Web maintains personal information about the individual who posted the bond (also known as the obligor), the bonded alien, the surety company and/or bonding agency,² and other general information about the bond itself, such as amount, number, date, etc. BMIS Web information is shared with the Internal Revenue Service (IRS) to report any interest paid to obligors. Information about surety bonds may be shared with Department of Justice legal counsel; the U.S. Treasury Department; State insurance regulators; debt collection agencies; insurance investigators for surety companies or bonding agencies; and legal representatives for surety companies and bonding agencies. This information is shared when ICE is pursuing further collection efforts on monies owed on a bond or if a surety bonding agent or agency is being investigated for its financial stability, licensing or business practices.

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?

For cash bonds, the personally identifiable information that is maintained in BMIS Web consists of the following:

- Obligor information - name, address, phone number, and Social Security Number (SSN)
- Alien information - alien number (A-Number), name, current location, and date of birth

² When a surety bond is issued, the obligor is the surety company. The surety company takes the financial risk of non-performance of the immigration bond. The bonding agency is the entity that is licensed to represent the surety company and engage in bond transactions on behalf of the company.



For surety bonds, the obligor is a surety company and not an individual. The same alien and obligor information listed above will be collected, except ICE will collect a Taxpayer Identification Number (TIN) instead of an SSN. ICE will also collect the bonding agency and agent's name and contact information.

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

All information above is provided by the obligor on the immigration bond form (Form I-352), also known as the bond contract. The information is then entered into the BMIS Web system to track the life cycle of the bond.

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

This information is necessary for the enforcement of immigration bonds, including the administration of the bonds and associated financial management activities. Immigration bond administration includes acceptance and approval, declarations of breach, cancellation and referral for collection of breached bonds. Associated financial management activities include collection, reimbursement or forfeiture of the bond principal, and calculation and payment of interest. BMIS Web supports only the financial management activities of the immigration bond program. The bond administration activities are supported by other ICE systems.

1.4 How is the information collected?

The information is collected from the obligor on Form I-352, "Immigration Bond," which is an OMB-approved form under the Paperwork Reduction Act. (OMB Control No. 1653-0022.)

1.5 How will the information be checked for accuracy?

ICE verifies the information provided by the obligor about him or herself by verifying it against identification documents presented by the obligor. Information provided about the bonded alien (e.g., Alien Number, etc.) is verified by ICE personnel using data from other ICE systems.

Internal quality control procedures exist to minimize data entry errors when information is entered into BMIS Web from Form I-352, and later when disbursements are made to the obligor.

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

ICE operates the immigration bond program pursuant to the authority granted to the Secretary of Homeland Security in Title 8, United States Code (U.S.C.), § 1103, and 8 U.S.C. § 1226. DHS regulations are found at Title 8, Code of Federal Regulation (C.F.R.), Section 103.6.



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

ICE collects only a limited amount of information about obligors and bonded aliens that is narrowly tailored to effectively and efficiently carry out the purposes of the program. All PII collected is necessary to perform bond administration and financial management functions. For example, the obligor's Social Security Number is used by ICE to issue an IRS Form 1099 to the obligor reporting interest payments, as required by federal income tax law.

Further, information is collected directly from obligors who complete the bond form. This ensures that information provided is as accurate as possible. Bonded alien information provided by the obligor is verified by ICE personnel using other ICE systems that contain highly reliable information about the alien, usually collected from the alien directly.

The limited scope of information ensures that any risks inherent to over-collection and accuracy of PII are mitigated.

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.

As described above, the information is generally used to ensure that the alien fulfills the conditions of the bond and for the administration of immigration bond and associated financial management activities. Immigration bond administration includes issuance, maintenance, cancellation, and revocation of bonds. Financial management activities include collection, reimbursement or forfeiture of the bond principal, and calculation and payment of interest, including issuance of IRS Form 1099 to the obligor reflecting interest paid on the bond.

Obligor and bonded alien contact information is needed to communicate on an as-needed basis about the bond or the bonded alien. The obligor's SSN/TIN is specifically used to satisfy IRS requirements to issue IRS Form 1099 to the obligor for interest paid on the bond. The SSN/TIN is also required by the Treasury Department for it to issue payments to the obligor on behalf of ICE through the Treasury Secure Payment System. The alien information is used to properly and accurately identify which aliens are released on bond, the amount of the bond, and its status.

When a surety bond is issued, the information is needed to allow ICE to communicate with the surety company and/or bonding agency on an as-needed basis about the bond or the bonded alien. If the surety bond is breached then the information about the surety company, agent and bonding agency is needed to allow ICE to issue an invoice of the amount owed on the bond and to issue further collection documents to the appropriate responsible parties.



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

BMIS Web can run simple reports based on bond status or date ranges for issuance of bonds.

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

The system does not use commercial or publicly available data.

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

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

In the standard operating procedures for the system and in the training provided to staff members, system users are instructed how to protect information in the system from disclosure to inappropriate third parties. For example, when third parties contact ICE to obtain bond-related information, users are instructed to provide information from the system only to the obligor. Users are instructed to seek information from a requestor, such as the obligor's address, SSN, the name of the bonded alien, etc., to verify his or her identity as the obligor before information will be disclosed from the system.

These procedures ensure privacy risks associated with misuse of data remain mitigated.

Section 3.0 Retention

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

3.1 What information is retained?

All information entered into BMIS Web is retained in the system. This includes the information described in Section 1.1 above as well as information about the bonding agency and/or surety company (if any) and the bond itself. The system will also retain any historical activities related to the bonds, such as a cancellation, breach, or disbursements.

3.2 How long is information retained?

Under the existing retention schedule, information maintained in BMIS Web is retained for six (6) years and three (3) months after the bond is closed or cancelled and the collateral is returned to the obligor. The retention period is the same for bonds that are breached. Copies of the Form I-352 (Immigration Bond)



are placed into the alien's A-File and maintained for the life of that file (75 years).³ United States Citizenship and Immigration Services (USCIS) is responsible for the maintenance of an alien's A-File.

ICE is in the process of reviewing and updating all of its retention schedules, including the schedule that applies to the bond information described above. In the event that these retention periods are modified, ICE will update this PIA.

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

Yes. A retention schedule was approved by NARA for the bond information described above when the bond program was part of the legacy Immigration and Naturalization Service. ICE is in the process of reviewing and updating all of its legacy records retention schedules, including the one for bond information.

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

The information in BMIS Web is retained for as long as the bond is considered open and then for six years and three months thereafter to ensure bond information is available to ICE during the lifetime of the bond and for any related litigation that may be filed. This retention period is consistent with the existing retention schedule and appropriate in length given the agency's mission and the purpose of the bond program.

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?

On a weekly basis, ICE shares BMIS Web information through an electronic interface with USCIS's Central Index System (CIS) in order to obtain the current location of the bonded alien's A-File from CIS, which DHS uses to track A-File locations nationwide. BMIS Web is then updated with the current A-File location data. The information exchanged between the two systems is limited to the alien's A-Number and the

³ The Alien File (A-File) is a federal record that contains information regarding all transactions involving an individual as he/she passes through the U.S. immigration and inspection processes. DHS's Citizenship and Immigration Services (USCIS) is the agency that is the custodian of the A-File. Additional information about the A-File is available in the A-File and Central Index System system of records notice (SORN) on the DHS Privacy Office website at www.dhs.gov/privacy. See 72 Fed. Reg. 1755 (Jan. 16, 2007).



location of the A-File. In addition, USCIS does not retain any BMIS Web information once the update has completed.

Information collected through Form I-352 may be made available to Customs and Border Protection (CBP) or other DHS components should those components establish a need to know the information. However, no ICE or other DHS systems receive direct data feeds from BMIS Web.

4.2 How is the information transmitted or disclosed?

The electronic comparison occurs within the DHS network behind the DHS firewall.

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

The privacy risks posed by BMIS Web's electronic interface with another DHS application are mitigated by several factors. First, this interface is performed through a batch process. A batch process is more secure than a real-time connection because it is an executable routine that is not accessible to BMIS Web users. Second, the interface occurs within the DHS network behind the DHS firewall, and is therefore highly secure. Third, the information being exchanged between the two systems is limited to the alien's A-Number and the location of the A-File.

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?

Information is shared with the U.S. Treasury Department and the U.S. Department of Justice. The obligor's name, address, and SSN/TIN are shared with the Treasury Department at the time disbursements are made to the obligor. The Treasury Department issues the checks for ICE. The information is also shared with the IRS when interest payments are issued to obligors by issuing IRS Form 1099-INT. The bond information for surety companies and their agents is shared with the Department of Justice when ICE has been unsuccessful in collecting the amounts due on the surety bond invoices. Both the Department of Justice and the Treasury Department may assist ICE with collection efforts.

When money is owed to ICE on a surety bond, BMIS Web sends the surety bond information to another ICE system, DCOS, to be invoiced. DCOS is currently the receivable system that tracks the invoice from the time it is created to the time it is paid. From DCOS, information may be disclosed to other agencies, such as the Treasury and Justice Departments, for debt collection purposes if the surety bond is not paid in a timely manner. The information is disclosed from DCOS, however, and not from BMIS Web.



Information about surety bonds may be shared with Department of Justice legal counsel; the U.S. Treasury Department; State insurance regulators; insurance investigators for surety companies or bonding agencies; credit bureaus; debt collection agencies; and legal representatives for surety companies and bonding agencies. This information is shared when ICE is pursuing further collection efforts on bond receivables or if an agent or bonding agency that posts surety bonds is being investigated for its financial stability, licensing or business practices.

Disclosures may be made from this system to consumer reporting agencies in accordance with 31 U.S.C. 3711(e) for the purpose of collecting money owed to the U.S. Government from an obligor as a result of overpayment of interest or default of the bond.

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.

The sharing described above is compatible with the original purpose for collection, namely to perform financial management activities for the immigration bond program. All external sharing falls within the scope of published routine uses in the Bond Management Information System of Records Notice. The information that is provided to IRS for interest payment reporting is required under federal income tax laws and regulations. In addition, agencies are required to share unpaid debt information for collection purposes under several federal laws, including the Debt Collection Improvement Act.

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

BMIS Web shares information electronically with the Treasury Department for payment of disbursements through Treasury's Secure Payment System (SPS). Transmission of SPS data is protected using public key infrastructure (PKI) encryption. Information shared with IRS is sent electronically through an encrypted IRS system for tax-related forms that requires an agency identification number, a user ID, and a password to access. Information is sent electronically to the Department of Justice via encrypted e-mails.

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

The sharing of information described above is in accordance with federal mandates to report to the IRS interest income paid, and to collect debts owed to the federal government. The privacy risks associated with this sharing relates to the secure transmission of data to these agencies. In each case, appropriate security measures have been taken during electronic transmission so that the risk of compromise is minimal. The risks associated with sharing this information are also mitigated by the existence of a published SORN describing the BMIS Web data. This PIA and the SORN provides public notice of and an



opportunity for the public to comment on this external sharing as well as request their information if they choose to do so.

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?

The obligors provide the information at the time they are posting the immigration bond. The immigration bond form (Form I-352) provides a Privacy Act Statement that informs the individual of the authority for and purpose of the collection, the possible ways in which the information will be shared, and whether providing the information is mandatory or voluntary (see Appendix A).

Existing notice is provided by the SORN, INS Bond Management Information System (67 FR 64136), October 17, 2002. Parallel to this PIA, ICE is updating the existing notice with a new notice under the DHS, specifically the U.S. Immigration and Customs Enforcement Bond Management Information System of Records. This SORN for BMIS Web provides coverage for the information maintained in BMIS Web and for other information collected and maintained as part of the bond management process.

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

Yes, but if an obligor elects not to provide this information, he or she will not be able to post an immigration bond.

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

No. If the obligor elects to provide the information on the immigration bond form, there is no opportunity for the obligor to consent to some uses but not others. Each use of information, however, will comport with the SORN for the system (see question 6.1).

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

Individuals who seek to post immigration bonds for aliens are provided three forms notice: this PIA, the SORN, and the Privacy Act Statement included on the immigration bond form. Both notices are accurate and reflect the current stated uses and sharing of the information. This notice is sufficient to mitigate any risks associated with a lack of notice of the collection of the information or the uses of the information.



Section 7.0 Access, Redress and Correction

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?

Obligors are provided with a copy of their bond contract at the time of posting the bond. If they need the same or additional information at a later date, the ICE Detention and Removal Operations (DRO) field office where the bond was posted will provide it if the requestor can verify their identity by providing identification or verifying specific information on the bond contract.

Typically when a disbursement is owed to obligors, they will contact ICE OFM directly rather than the DRO field office. To verify the obligor's identity, OFM compares the obligor's signatures from the bond contract to the signature on the obligor's written request for information. If there is a discrepancy, additional signature samples are requested.

In addition to the procedures above, individuals may request access to records about them in BMIS Web by following the procedures outlined in the BMIS SORN, as well as through the ICE FOIA process (FOIA, 425 I Street, NW, Washington DC, 20536).

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

The procedures for editing or reviewing a bond form that is already on file are the same as those noted in question 7.1.

In the event ICE declares a cash bond breached, which means the cash or securities pledged in support of the bond are deemed forfeited, the individual obligor has the right to request that ICE reconsider its decision pursuant to 8 C.F.R. Part 103. Thereafter, obligors can administratively appeal adverse decisions to the Administrative Appeals Office at U.S. Citizenship and Immigration Services.

If the obligors need to correct the information regarding the bond, they would request that change in writing, sign the request, and submit it to ICE OFM. Obligors are asked to send a copy of an identity document, such as a driver's license, to verify their identity. The signature on the request would be compared to signature on the bond contract to verify the obligor's identity. Additionally, certain forms and activities related to the bond management process, such as the Form I-395, Affidavit in Lieu of Lost Receipt, and the Form I-312, Designation of Attorney in Fact, require a notarized signature.

In addition to the procedures above, individuals may request correction of records about them in BMIS Web by following the procedures outlined in the BMIS SORN.



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

At the time the bond is posted, obligors are provided with phone numbers and addresses for the local DRO field office. If they need to correct their address, there is a form that is issued by the ICE DRO office for that purpose. The obligors are also made aware of the contact information for ICE OFM on Form I-391, which is issued when the bond is cancelled.

The procedure for submitting a request to correct information through the ICE Freedom of Information Act (FOIA) office is also outlined in the BMIS SORN.

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

Formal redress procedures are provided.

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

The obligor has three potential means to access and correct information about them in BMIS Web. The first is by contacting the DRO field office or the ICE OFM office to obtain or correct information. The second is through the ICE FOIA office and a formal request to access or correct their records under the Privacy Act, where appropriate. The third means to correct information is through the administrative appeals process described in Question 7.2. These procedures are adequate to address the individual's right to access and correct their records.

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?

User requests for access to BMIS Web must be approved by the user's supervisor to ensure that access is appropriate and related to the individual's duties. A user request form is completed and signed by the supervisor. The roles and privileges assigned to a particular user are predetermined depending on that user's function. The ICE DRO offices have read-only access to BMIS Web because they do not have a need to enter or edit data in the system. The ICE OFM bonds branch supervisor, accounting technicians and accountants have read-write privileges in BMIS Web. These rights allow them to enter new bonds and to update the bond status (e.g., fact that a bond has been cancelled or breached) when that information is received from ICE field offices. It also allows them to reimburse the obligor for the principal and/or interest on the bond.



8.2 Will Department contractors have access to the system?

Yes. The BMIS Web contract software developers have read-only access to BMIS Web. In addition, contractors that are supporting ICE DRO have read-only access to the system. These contractors are helping to reduce the backlog of open bonds. No other Department contractors have access to BMIS Web.

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

BMIS Web application training is provided by ICE OFM. All ICE personnel and contractors also complete annual mandatory privacy and security training. In addition, the standard operating procedures for bonds and in user training, users are instructed to verify the identity of obligors seeking information from the system to ensure that information is not disclosed to unauthorized third parties.

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

The Certification and Accreditation process is in progress but is expected to be completed on August 15, 2008.

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

BMIS Web will use database-level auditing to capture information associated with any viewing, insert, update, or delete of records in the dataset, and the user that performed the activity. The BMIS Web application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value. OFM reviews audit trails when there is indication of system misuse and at random to ensure users are accessing and updating bond records according to their job function and responsibilities.

All failed logon attempts are recorded in an audit log and periodically reviewed. The BMIS Web Information System Security Officer will review audit trails at least once per week, or in accordance with the System Security Plan. The BMIS Web system and supporting infrastructure audit logs will be maintained as part of and in accordance with the existing ICE system maintenance policies and procedures for ICE.

ICE also has a process in place for investigating and responding to suspicious activities on the system. That process includes automated tools to assist the administrators in their monitoring, analysis, and reporting. The process is consistently followed. Additionally, BMIS Web runs within the DHS network and is protected by DHS network firewalls. There are no real-time interfaces between BMIS Web and other systems.



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 privacy risks to this system are primarily the risks of unauthorized system access or use and inadequate system security. Both risks have been mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above and elsewhere in this PIA, those controls include user access controls, auditing, intrusion detection software, and user training.

Section 9.0 Technology

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 project is a system modernization project, converting the BMIS mainframe-based application to one that is web-based. It has minimal enhanced functionality, but it captures the same data as the mainframe-based version and transmits the information to the same customers within the ICE organization and at other agencies. BMIS Web is scheduled to deploy initially as a pilot in August 2008, and then fully deploy in September 2008.

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

BMIS Web is currently being developed with testing completed in June 2008 and a target date of August 2008 to be operational as a pilot. Full deployment is scheduled for September 2008.



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

No.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security



Appendix A

PRIVACY ACT STATEMENT

Authority and Purpose: The Immigration and Nationality Act, as amended, (8 U.S.C. 1103, 1183, 1226, 1229c, and 1363) authorizes the collection of this information to provide for the posting, maintenance, cancellation, and breach of an immigration surety bond, and for associated financial management activities, including collection of unpaid monies, reimbursement of the bond principal, and the calculation, payment, and reporting of interest. The Internal Revenue Code (26 U.S.C. 6109) authorizes the collection of the Social Security number (SSN).

Disclosure: Furnishing this information is voluntary; however, failure to provide it will result in the non-issuance of the immigration bond. For cash bonds, your SSN is necessary to pay interest through the U.S. Treasury Department and to comply with Internal Revenue Service requirements to report interest payments.

Routine Uses: This information will be used by and disclosed to DHS personnel and contractors or other agents who need the information to support the enforcement of immigration laws and the provision of immigration benefits. DHS may share this information with the U.S. Treasury Department to report interest paid to an obligor, and to facilitate payments to or collection of monies owed by an obligor. DHS may also share this information with the U.S. Justice Department and other Federal and State agencies for collection, enforcement, investigatory, or litigation purposes, or as otherwise authorized pursuant to its published Privacy Act system of records notice.