



Privacy Impact Assessment
for the

Bonds Online System (eBONDS) - Phase One

July 14, 2009

Contact Point

James T. Hayes, Jr.
Director, Office of Detention and Removal
U.S. Immigration and Customs Enforcement
(202) 732-3100

Reviewing Official

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



Abstract

The Bonds Online System (*eBONDS*) is a web-based application used primarily by surety agents and the Office of Detention and Removal Operations (DRO) at U.S. Immigration and Customs Enforcement (ICE) to facilitate the ICE immigration bond management process. The basic function of *eBONDS* Phase One is to allow surety companies to post immigration bonds online for aliens that DRO has determined are eligible for release on bond. The purpose of this Privacy Impact Assessment (PIA) is to document *eBONDS* use and collection of personally identifiable information (PII). Future phases of *eBONDS* will provide enhanced capabilities and PIAs will be conducted as necessary to address changes made by future deployments.

Overview

eBONDS is owned by ICE DRO and will be deployed in two phases. *eBONDS* Phase One enables surety agents to make online requests to verify that a particular alien in ICE custody is eligible for release pursuant to the posting of an immigration bond, and to initiate, complete, and submit to DRO a bond documentation package containing the ICE Immigration Bond Form (Form I-352, OMB Control No. 1653-0022), any riders (documents that amend the bond, such as updating personal information) to the bond, Power of Attorney forms, and digital signatures of the surety agent. *eBONDS* also tracks the status of all requests for verification of bond eligibility, the completion of the I-352, and the approval of bond documentation packages. *eBONDS* Phase Two will seek to further automate and facilitate the life cycle of the surety bond processing, and to automate the processing of cash bonds. The information collected and used in the *eBONDS* process is covered under the Bond Management Information System (BMIS) System of Records Notice (SORN)¹. This PIA covers only Phase One of the *eBONDS* system.

Background

An immigration bond is a formal written guaranty by an obligor (an individual, entity, or surety company) posted as security for the amount of the immigration 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.

In a typical surety bond scenario an alien has been arrested and detained by ICE officers. ICE then determines if the alien is eligible for release on bond and if so, ICE sets a bond amount. A bond requestor, generally a third party such as a family member of the alien, contacts a surety company to request that it post bond for the alien. A surety agent, acting on behalf of the surety company, posts bond to obtain the alien's release and promises that the alien will satisfy the terms of release, usually to return for a court

¹ The Bond Management Information System (BMIS) SORN (73 FR 52865, September 11, 2008) is available at www.dhs.gov/privacy.



appearance or voluntarily depart the U.S. at a future date. The surety bond amount serves as security to ensure performance and fulfillment of the bonded alien's obligations to the government. Should the alien not satisfy the terms of release, ICE declares the bond breached and the surety company must pay DHS the full amount of the bond plus interest and penalties.² If the conditions of a bond are satisfied, the bond is cancelled.

Prior to the deployment of *eBONDS*, a surety agent was required to visit a DRO field office in person. First, they would request that a DRO field officer verify an alien was eligible for bond, and then they would complete and submit the hard copy I-352 bond documentation package in order to post bond. Once the DRO officer reviewed and approved the package, the DRO officer would create a financial record of the bond in BMIS Web and ICE would release the alien. If the alien did not satisfy the terms of the bond (e.g., fails to appear in court), the bond was considered breached and the surety company was required to pay the bond amount to the U.S. Government.

With the deployment of *eBONDS*, the surety agent will be able to log on to *eBONDS*, verify the alien's bondable status online, complete and submit the I-352 package electronically, and obtain approval from DRO for the bond. No visits to DRO field offices are required. Surety agents will have *eBONDS* user accounts managed by a surety company.

Typical Transaction

In a typical *eBONDS* transaction, a surety agent logs into *eBONDS* for the purpose of posting a surety bond for an alien. The surety agent submits the relevant alien name and A-Number to *eBONDS* to determine whether an alien is eligible for bond. If *eBONDS* indicates the alien is bondable, *eBONDS* retrieves information about the alien for whom bond would be furnished and the bond amount from the ENFORCE Alien Removal Module (EARM)³, and the surety agent, surety company, and Power of Attorney from BMIS Web⁴ to create a record in *eBONDS*. The *eBONDS* record is created using the EARM and BMIS Web information pre-populated in the Form I-352 and the relevant Power of Attorney form. The surety agent accesses the alien's *eBONDS* record, completes the remaining fields regarding the alien residence address after release, and bond requestor information in the I-352, appends any riders to the bond, and digitally signs the I-352, creating a bond documentation package. A DRO officer reviews the bond documentation package through EARM for completeness and accuracy against information in EARM and BMIS Web. If the bond documentation package is complete and accurate, the DRO officer approves and digitally signs it. *eBONDS* notifies the surety agent via email that the bond has been approved. Forty-eight hours after the surety agent acknowledges receipt by logging into *eBONDS* and downloading a copy of the approved bond package, EARM converts the *eBONDS* record into the financial record of the bond in BMIS Web and the approved I-352 bond documentation is deleted automatically in *eBONDS*. ICE then releases the alien.

² 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.

³ EARM tracks the status of alien removal proceedings from initial arrest through the completion. For additional information on routine uses and categories of individuals in EARM please see the ICE Removable Alien Records (RARS) System of Record Notice (DHS/ICE-011, May 5, 2009, 74 FR 20719) at www.dhs.gov/privacy.

⁴ BMIS Web records and maintains for financial management purposes the immigration bonds that are posted for aliens involved in removal proceedings.



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?

eBONDS collects and uses information about aliens, bond requestors, and surety agents. Specifically, eBONDS maintains the following PII about the alien for whom the bond is requested:

- Alien name
- Alien Registration Number (A-Number)
- Alien residence address after release
- Alien's bondable status
- Detention location
- Date and country of birth
- Nationality
- Gender
- Date, port and means of entry.
- Name and address of the bond requestor (e.g., family member that requested the surety bond)

eBONDS also maintains the following surety agent information:

- Name of surety company
- Agent's name
- Address
- E-mail
- Phone number
- Digital signature
- Username and password
- Name of the surety administrator
- Surety company administrator username and password

In addition, eBONDS maintains information about the bond itself, such as the bond date and amount.



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

BMIS Web is the source of surety agent, surety company, and Power of Attorney information. EARM is the source for alien information and bond amount. Both BMIS Web and EARM collect PII directly from the surety agent and alien, respectively. To determine the bondable status of an alien, surety agents will submit name, A-Number and the following optional information: date of birth, nationality, gender and detention location. Once the alien is determined to be bondable, EARM pre-populates the Form I-352 with the name, A-Number, date of birth, nationality, gender and detention location, and BMIS Web pre-populates the Form I-352 with the amount of bond, and surety company information. BMIS Web also provides the relevant Power of Attorney form into eBONDS. Surety agents will also input into eBONDS the alien residence address after release, and bond requestor information.

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

eBONDS uses the information it collects from the surety agent, EARM, and BMIS Web to confirm the alien is eligible for bond and, if so, to facilitate the request and approval of the bond online. The information collected in eBONDS is also necessary for the enforcement of immigration bonds posted by surety companies, 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 surety bonds. Associated financial management activities include collection, reimbursement or forfeiture of the bond principal, and calculation and payment of interest. eBONDS directly supports the online administrative management activities of the immigration bond program, and indirectly supports the financial management of the immigration bond program by sending information about approved bonds to BMIS Web.

1.4 How is the information collected?

The surety agent logs on to eBONDS through the Internet and submits the alien name and A-Number, and the following operational information: date of birth, nationality, gender and detention location provided by the bond requestor. If the surety agent has submitted information for an alien who is eligible for bond, eBONDS then retrieves the alien information and bond amount from EARM and the surety agent information from BMIS Web, both through secure web services. eBONDS uses the information to electronically populate Form I-352.

1.5 How will the information be checked for accuracy?

Once the surety agent initiates a bond request in eBONDS for a particular alien, the information is checked for accuracy three times before the alien is approved for bond. First, a DRO officer verifies that the alien is eligible for a bond by reviewing the A-file⁵ and confirming in EARM the result of criminal checks,

⁵ The A-File is the record that contains copies of information regarding all transactions involving an individual as he/she passes through the U.S. immigration and inspection process. Previously, legacy Immigration and Naturalization Services (INS) handled all of these transactions. Since the formation of DHS, however, these



the address of the alien, the status of the surety agent, and any action taken by immigration courts. Until this information is confirmed, *eBONDS* will not create an alien bond record. Second, the surety agent confirms the information he or she submits to *eBONDS* (i.e., alien residence address after release, bond requestor name and address, amount of the bond) prior to digitally signing the I-352 and submitting the bond documentation package in *eBONDS* for DRO approval. Third, a DRO officer reviews and confirms that the bond package is complete and accurate compared to the information in EARM and BMIS Web before digitally signing the I-352 and approving the bond.

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.), § 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.

Privacy Risk: *eBONDS* could present a risk of the over-collection of PII.

Mitigation: *eBONDS* collects a limited amount of information about individuals that is narrowly tailored to effectively and efficiently carry out the purpose of the system, specifically to verify that an alien is eligible for bond and to facilitate the bond request and approval process for surety bonds. The limited scope of information ensures that any risks inherent to over-collection of PII are mitigated.

Privacy Risk: *eBONDS* could present a risk of data inaccuracy.

Mitigation: *eBONDS* records are initiated only by surety agents and personal information is collected directly from the surety agents, bond requestors, and other ICE systems that contain highly reliable information about the alien, usually collected from the alien directly. The alien and bond information provided by the surety agent is also manually cross-checked by ICE personnel against data in other ICE systems. The information in *eBONDS* that is imported from other ICE systems cannot be modified by the surety agent, thereby ensuring the accuracy and integrity of the information in the I-352.

responsibilities have been divided among USCIS, ICE, and CBP. While USCIS is the custodian of the A-File, all three components create and use A-Files. For additional information see the DHS-USCIS-001 Alien File (A-File) and Central Index System (CIS) System of Records (72 FR 1755) available at www.dhs.gov/privacy.



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.

ICE uses the information in *eBONDS* to verify if an alien can be processed for a surety bond, to approve or deny the surety agent's bond request, to track the status of requests for surety bonds, and to establish ICE's financial record of the bond in BMIS Web.

eBONDS uses the alien name and A-Number (with the following optional information: date of birth, nationality, gender and detention location) submitted by the surety agent to determine if an alien is eligible for a bond. A DRO officer uses this information to retrieve information about the alien from EARM and verify whether that alien is eligible for a bond. Further, *eBONDS* records each action taken by the surety agents and DRO officers for the purposes of requesting verification of an alien's eligibility for a surety bond, and processing a bond documentation package.

eBONDS uses the alien information and bond amount retrieved from EARM to pre-populate the I-352. *eBONDS* uses the surety agent and surety company information from BMIS Web to further pre-populate the I-352 and provide a copy of the Power of Attorney form. The surety agent then provides bond requestor information, alien location and phone number to complete the I-352. Once *eBONDS* has a completed I-352, with any bond riders and the Power of Attorney form attached, the surety agent signs the Form I-352 to create a bond documentation package. The surety agent submits the bond documentation package, which is either approved or denied by DRO. EARM converts the *eBONDS* record into the financial record of the bond in BMIS Web to support financial management activities related to the bond as described in the BMIS Web PIA.⁶

The addresses and phone number of the surety agents are collected to enable future contact and the delivery of any further notice regarding the bond.

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

Surety agents can search *eBONDS* records that they have initiated by date, and by status of the *eBONDS* records (e.g., requests for verification of alien bond eligibility submitted, bond documentation package approved). DRO field agents can generate simple reports of *eBONDS* data through an interface in EARM that show all bonds submitted by a surety agent or surety company, or for a particular date range.

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

eBONDS does not use commercial or publicly available data.

⁶ The Bond Management Information System Web Version (BMIS Web) PIA is available at www.dhs.gov/privacy.



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.**

Privacy Risk: Individuals with access to eBONDS information could misuse the data for reasons outside of the original scope of collection.

Mitigation: In order to allow their agents to use eBONDS, surety companies must register with ICE and acknowledge in writing that they will: only use eBONDS for the purpose of posting surety bonds; create, manage, and terminate user accounts in accordance with policy established by ICE; notify ICE in the event that they suspect or experience a security breach that impacts eBONDS; and follow guidance issued by ICE on the proper handling of personal information.

Only authorized users have access to eBONDS. Surety agents and surety company administrators must register for access by obtaining a digital certificate from the PKI administrator, providing a Power of Attorney agreement between the surety company and surety agent, and submitting a user access form to DRO. DRO then issues a username and password to the surety agents and surety company administrators. ICE personnel must provide system support for eBONDS and complete all mandatory annual privacy and security training, which stresses the importance of authorized use of personal data in government systems, in order access the eBONDS system. DRO field officers do not have access to eBONDS and can only run reports on eBONDS information through EARM. Further, eBONDS limits the type of access per user role. Surety company administrators can only review eBONDS records pertaining to their surety agents. Surety agents can only review eBONDS records that they have initiated. Both surety agents and surety company administrators must follow all instructions and rules of behavior when using eBONDS. Audit controls at the database level are reviewed for individuals who are found to have accessed or used the eBONDS data through eBONDS or EARM in an unauthorized manner and such individuals are disciplined in accordance with ICE policy. These controls 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?**

The eBONDS system retains surety agent and surety company administrator user information and system activity history. It retains a copy of the approved I-352 bond documentation package. It also retains I-352 forms that are not approved by a DRO officer, including bond requests that are rejected, withdrawn or not submitted for approval.

eBONDS will delete the approved I-352 bond documentation package 48 hours after acknowledgement of receipt by the surety agent, at which time the PDF is transferred to BMIS Web for permanent retention. eBONDS will delete any eBONDS records not approved by a DRO field officer, including records that are rejected, withdrawn or not submitted, one week from the date when the record was initially created. Please refer to the BMIS Web PIA for records retention information.



3.2 How long is information retained?

Approved I-352s are retained until the surety agent acknowledges receipt of the approved I-352 in eBONDS. Forty-eight hours after the surety acknowledges receipt, the approved I-352 is transferred to BMIS Web and deleted from eBONDS. eBONDS deletes any I-352 forms that are not approved by a DRO officer, including bond requests that are rejected, withdrawn or not submitted for approval, one week from the date when the record was initially created. eBONDS I-352 data in BMIS Web is retained for six years and three months after the bond is closed or cancelled. The retention is the same for bonds that are breached. Copies of the I-352 are also placed into the alien's A-file and maintained for the life of that file (75 years). United States Citizenship and Immigration Services (USCIS) is responsible for the maintenance of an alien's A-File.

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

No. ICE is currently operating under a retention schedule governing bond records that was previously approved by NARA when the bond program was part of the legacy Immigration and Naturalization Service (INS). Because INS was abolished in 2003 and the bond program was transferred to ICE, and because new records related to the bond program will be created with the deployment of eBONDS, ICE has drafted a new retention schedule that, once approved, will specifically govern retention of ICE's bond records including eBONDS information. This proposed retention schedule is currently under review by NARA..

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

Privacy Risk: Retaining eBONDS data longer than necessary would violate the Fair Information Principle of minimization which requires systems and programs to retain only the information necessary and relevant to complete the task associated with its initial collection.

Mitigation: eBONDS only retains the alien bond information for limited periods appropriate to the purpose of the system. For example, the approved I-352 is retained in the system for only 48 hours once the surety agent retrieves a copy of the bond record from the system. I-352s that are not approved are only maintained in the system for a week. The week timeframe provides surety agents some time to return to, review, and complete the bond documentations packages for submission to DRO without creating a persistent repository of incomplete records. Accordingly, the information is retained for a time that is limited and appropriate.

The approved I-352s sent to BMIS Web are 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. See BMIS Web PIA for additional information.



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?

eBONDS does not directly share information outside of ICE; however, the PII collected through eBONDS is provided to ICE's BMIS Web, and may be further disclosed within DHS as described in the BMIS Web PIA.

4.2 How is the information transmitted or disclosed?

No eBONDS information is directly transmitted or disclosed outside of ICE.

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.

There is no internal sharing of eBONDS data with other non-ICE systems or users so there is no internal sharing risk.

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?

eBONDS directly shares alien information from EARM with the surety agents that have requested bond for that alien. The alien information disclosed includes the verification of the alien's eligibility for a bond, alien name, A-Number, detention location, date and country of birth, nationality, and date, port and means of entry. eBONDS provides this information to notify surety agents that an alien is eligible for a bond and to facilitate the creation of the bond documentation package by the surety agent.

eBONDS indirectly shares data outside DHS through BMIS Web, which may make that information available to other Federal agencies in support of ICE collection efforts. Further information on external sharing through BMIS Web may be found in the BMIS Web PIA.



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 of information through eBONDS (i.e. providing bondable status of an alien and returning the surety and alien information comprising the bond documentation package) with the surety agent is compatible with the original purpose for collection, namely to facilitate the issuance of surety bonds for eligible aliens. Any indirect external sharing of eBONDS data that may occur through BMIS Web is also compatible with the original collection and falls within the scope of published routine uses in the Bond Management Information System (BMIS) System of Records Notice, DHS/ICE-004 (73 FR 52865, Sept.11, 2008).

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

eBONDS data is shared with the surety agent electronically through the system itself. Access to the information requires the surety agent to log in to the eBONDS system through a Secure Sockets Layer (SSL) (i.e., encrypted) connection.

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

Privacy Risk: eBONDS could present a risk of the insecure transmission of information.

Mitigation: Appropriate security measures have been taken during electronic transmission so that the risk of compromise is minimal, including the use of SSL connections, PKI and usernames/passwords that ensure only authorized surety agents and surety company administrators have access to eBONDS.

Privacy Risk: There is a potential risk of the over-disclosure of alien data from ICE enforcement systems to surety agents via the I-352.

Mitigation: To mitigate the risk of over-disclosure, ICE requires all surety companies using eBONDS to register and acknowledge in writing that they will: only use eBONDS for the purpose of posting surety bonds; create, manage, and terminate user accounts in accordance with policy established by ICE; notify ICE in the event that they suspect or experience a security breach that impacts eBONDS, and follow guidance issued by ICE on the proper handling of personal information.

Further, eBONDS provides surety agents and surety company administrators with limited data from EARM and BMIS Web, prohibits modification of data pre-populated by EARM and BMIS Web, and limits their access to only those records in eBONDS for which they have a need-to-know. Surety company administrators can only review eBONDS records pertaining to their surety agents. Surety agents can only



review eBONDS records that they have initiated. In addition, this PIA and the SORN provides public notice of this external sharing as well as an opportunity to 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?

At each eBONDS logon, surety agents view a notice informing them of the terms for accessing eBONDS and the possible ways that their PII and information regarding their activity in eBONDS could be used and shared. By logging on, the surety agent acknowledges agreement with the notice.

Aliens whose information is submitted in eBONDS do not receive notice regarding the use of their information in I-352s because their information is not collected at the time of the bonding process.

General public notice is also provided by this PIA, the BMIS SORN (73 FR 52865, Sept. 11, 2008) and the BMIS Web PIA, which collectively describe information collected and maintained by ICE as part of the bond management process.

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

No. Surety agents must provide information about themselves to create an eBONDS account. Aliens for whom bond requests are made do not provide information because they are in custody and are not able to request bond for themselves.

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. Surety agents may not consent to limited uses of their information. Because the aliens are in custody, they are not in a position to consent to the use of their information nor to request their own bond.

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.

Privacy Risk: There is a risk of a lack of notice of the collection and uses of the information.

Mitigation: Surety agents whose information is collected by eBONDS receive three forms of notice: this PIA, the BMIS Web SORN, and the Privacy Act Statement included on the system log-in and the immigration bond form. The alien receives notice through this PIA, the BMIS Web SORN, and the Privacy



Act Statements on the forms for alien removal proceedings. The 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?

Individuals may request access to records about them in eBONDS by following the procedures outlined in the BMIS SORN. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in eBONDS could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

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

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

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

The surety agents can access their own information by logging in to the eBONDS system.

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

If individuals obtain access to the information in eBONDS pursuant to the procedures outlined in the BMIS SORN, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the BMIS SORN. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.



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

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

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

Surety agents seeking to correct their own inaccurate or erroneous information must notify their surety company administrator. The surety company administrator will then logon and update the requested information. Corrections to information on approved I-352s may be made by the DRO field office.

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

The Help Function of *eBONDS* provides surety agents with instructions on how to facilitate corrections of their information in the system. Surety agents are notified of the procedures for correcting their information at the time the bond is posted, which includes the phone numbers and addresses for the local DRO field office. At the time of the request, the DRO field officer will ask that the individual digitally sign any change requests. Their digital signature will be compared to the public key maintained within the *eBONDS* system. If they need to correct their address, there is a form that is issued by the ICE DRO office for that purpose.

The procedure for submitting a request to correct information through the ICE FOIA office is also outlined in Question 7.2 above and the BMIS SORN.

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

Formal redress is provided through the access and correction procedures discussed above.

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

Privacy Risk: The privacy risks are of a lack of access to information and inability to seek redress and correction.



Mitigation: Surety agents entering their personal information, and the alien whose personal information is entered by the surety agents, have means to access and correct information about themselves. The surety agent may access their information by logging into the system and may have their information corrected by filing a request with their account administrator. Aliens may access and correct information about themselves by contacting the DRO field office or through the FOIA process. 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?

All surety companies must register with ICE in order to allow their agents to access and use eBONDS. As part of the registration process, surety companies must acknowledge in writing that they will: only use eBONDS for the purpose of posting surety bonds; create, manage, and terminate user accounts in accordance with policy established by ICE; notify ICE in the event that they suspect or experience a security breach that impacts eBONDS, and follow guidance issued by ICE on the proper handling of PII. They must also submit user access forms, PKI certificates, and Power of Attorney agreements between the surety company and surety agents. DRO issues the surety agents usernames and passwords via email to allow secure access to eBONDS.

ICE eBONDS system administrators that support the system have direct access. Other ICE personnel do not have direct access to eBONDS but access information during the bonding process through a user interface in EARM. Read/write permission through the EARM application is strictly based upon functional role assignments for eBONDS.

8.2 Will Department contractors have access to the system?

Yes. The eBONDS contract software developers have read-only access to eBONDS. This access is required when providing support for problems or questions identified by users. Other ICE contractors may have access to information from eBONDS through EARM, for the purposes of updating eBONDS user information, viewing and approving bond requests, viewing bond submissions and approving bond submissions.

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

The surety agents using eBONDS are non-government employees who work for surety companies. DHS does not provide any privacy training to surety company employees / users, however, DHS provides surety companies with guidance on proper handling of PII and requires surety agents to agree with terms of system use.



All ICE personnel and contractors having access to eBONDS or to eBONDS information through EARM complete annual mandatory privacy and security training. In addition, in the standard operating procedures for bonds and in user training, users are instructed to verify the identity of surety agents 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 complete by August 1, 2009.

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

eBONDS 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, i.e. any action taken by the surety agent or system administrator directly accessing eBONDS. The eBONDS 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. DRO will review audit trails when there is indication of system misuse and at random to ensure users are accessing and updating eBONDS records according to their assigned roles.

All failed logon attempts are recorded in an audit log and periodically reviewed. The eBONDS Information System Security Officer will review audit trails at least once per week, or in accordance with the System Security Plan. The eBONDS 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 system administrators in their monitoring, analysis, and reporting. The process is consistently followed.

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

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

Mitigation: Both risks have been mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above and elsewhere in this PIA, those controls include: encrypted transmission of data, use of PKI certificates to authenticate users, a registration process for all surety companies, written agreements for the appropriate



use of the system, filters that limit the information accessible to surety agents and surety company administrators to their eBONDS records, role-based access for ICE personnel, auditing, 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 process modernization effort to streamline completion and electronic submission of the I-352.

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

eBONDS Phase I will be deployed operationally in July 2009. The ICE System Lifecycle Management methodology, Waterfall, was used for development.

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

No.

Responsible Officials

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

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security