Privacy Impact Assessment
for the

Federal Protective Service
Guard Contracting Reform Rulemaking

September 15, 2009

Contact Point
Ashley J. Lewis
Director
Office of Acquisition Management
U.S. Immigration and Customs Enforcement
(202) 732-2600

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

Abstract

The Federal Protective Service Guard Contracting Reform Act of 2008 requires U.S. Immigration and Customs Enforcement (ICE) to collect information regarding felony convictions from individuals who own, control, or operate a business concern seeking to provide contract security guard services to ICE's Federal Protective Service. Concurrent with this Privacy Impact Assessment (PIA), the Department of Homeland Security (DHS) has published a final rule implementing this requirement and providing guidelines under which the award of guard services contracts may be prohibited based on criminal history. Section 222 of the Homeland Security Act requires that DHS publish a PIA on rulemakings, including the type of personal information collected and the number of persons affected. This PIA is being conducted to comply with Section 222 and to publicly document the privacy impact of this new requirement.

Overview

The Federal Protective Service (FPS), an organization within ICE, procures contract guard services in support of its mission to mitigate risk to Federal facilities and their occupants, in a professional and cost effective manner. FPS procures contractor personnel to provide guard services at Federal facilities protected by FPS. The Federal Protective Service Guard Contracting Reform Act of 2008 (the Act) (Pub.L. 110-356) required DHS to promulgate a regulation prohibiting DHS from awarding FPS contracts for guard services to any business concern that is owned, controlled, or operated by an individual who has been convicted of a felony.[1] The Act further requires contractors to provide information to DHS regarding relevant felony convictions when submitting proposals. On March 18, 2009, DHS issued a notice of proposed rulemaking (74 FR 11512) to implement the requirements of the Act on behalf of ICE. Three public comments were received, which did not result in substantive changes to the final rule. The final rule summarizes the comments and provides brief responses outlining the Department's position on the various issues raised by the interested parties.

The final rule identifies which serious felonies may prohibit a contractor from being awarded a contract; requires contractors to provide information regarding any relevant felony convictions when submitting proposals; provides guidelines for the contracting officer to assess present responsibility, mitigating factors, and the risk associated with the previous conviction; and allows the contracting officer to award a contract notwithstanding a previous conviction under certain circumstances.

Under the final rule, only certain "serious" felony convictions will prohibit ICE from awarding a business concern a contract for FPS guard services, specifically those felonies that cast doubt on the integrity or business ethics of the business concern or are of a nature that are inconsistent with the mission of FPS. Serious felony convictions that would prohibit a contract award include but are not limited to:

[1] As defined in the final rule, *business concern* means a commercial enterprise and the people who constitute it. *Convicted of a felony* is defined as any conviction of a felony in violation of state or federal criminal statutes, including the Uniform Code of Military Justice, whether entered on a verdict or plea, including a plea of *nolo contendere*, for which a sentence has been imposed. *See* 74 FR 11512, 11514.

fraud arising out of a contract with the federal, state or local government; bribery, graft or a conflict of interest; threatened or actual harm to a government official, family member or government property; crimes of violence; threat to national security; commercial bribery, counterfeiting, forgery or trafficking in vehicles the identification numbers of which have been altered; obstruction of justice, perjury or subornation of perjury, or bribery of a witness; certain felony tax crimes; trafficking in illegal drugs, alcohol, firearms, explosives or other weapons; immigration violations and any other felony that involves dishonesty, fraud, deceit, misrepresentation, or deliberate violence; that reflects adversely on the individual's honesty, trustworthiness, or fitness to own, control, or operate a business concern; that casts doubt on the integrity or business ethics of the business concern; or is of a nature that is inconsistent with the mission of FPS.

ICE-issued solicitations and contracts for FPS guard services will contain an HSAR clause that will require offerors (*i.e.*, bidders) to disclose whether they are a business concern that is owned, controlled or operated by an individual convicted of a felony. If a business concern represents that they are owned, controlled or operated by an individual convicted of a felony they must also submit an additional document with their proposal called an "award request," which is a request that ICE award the contract despite the existence of a felony conviction because it is not a "serious felony" that would prohibit the contract award. The award request should provide additional information to support the offeror's claim that the individual's felony conviction is not a serious felony as defined by the regulation, or that such individual no longer owns, controls, or operates the business concern. The final rule requires that the award request will provide details regarding the felony conviction to include: name and date of birth of individual convicted of the felony, a full description of which roles or interests indicate that the individual owns, controls, or operates, or may own control or operate the business concern; date sentenced, statute/charge, docket/case number, court/jurisdiction, nature and circumstances surrounding the conviction, protective measures taken by the individual or business concern to reduce or eliminate the risk of further misconduct, whether the individual has made full restitution for the felony, and whether the individual has accepted responsibility for past misconduct resulting in the felony conviction.

The Act requires ICE to collect felony conviction information from all offerors at the time proposals are submitted; however, ICE will only review this information for the business concern determined to be the apparent successful offeror for a particular contract award. Otherwise, the felony conviction information will be stored in the contract file with other unsuccessful proposals until ICE may properly destroy the records under its records disposition plan.

The offeror will submit to ICE the felony conviction information with its proposal either electronically or in paper format as directed by the solicitation instructions. ICE will retain the successful offeror's proposal including any and all supporting information related to former felony convictions of its owners, controllers, and operators. After contract award, felony information submitted by the successful offeror will be stored separately from the official contract file in a secured location. If the felony information is provided in an electronic format, the information will be converted to hard copy format and stored in a secured location. Electronic information related to a specific individual and their felony conviction will not be stored on the ICE computer system. ICE government personnel and contractors or other agents will use this information for apparent successful offerors only to assess the felony conviction and determine if a contract award should be made to the business concern under the regulation.

Additionally, because the felony conviction information is a part of the contract file, ICE may share this information with the U.S. Justice Department and other Federal and State agencies for collection, enforcement, investigatory, or litigation purposes related to the contract award, enforcement, litigation, or other matters associated with the contract. For example, information may be shared with the General Accountability Office (GAO) or the DHS Inspector General's office in response to an audit or investigatory request.

Typical Transaction

When ICE issues a solicitation for FPS guard services, it will receive offers from various business concerns competing for the contract. If a given business concern is owned, controlled, or operated by an individual convicted of a felony as defined in the Homeland Security Acquisition Regulation (HSAR) clause contained in the solicitation, the prospective offeror will submit an award request with its proposal that petitions ICE to award the contract in spite of the felony conviction(s), and provide any information to support its claim that the conviction is not for a serious felony as defined in the regulation. The ICE contracting officer will maintain the award request with the solicitation in ICE's Office of Acquisition Management (OAQ) recordkeeping system. After evaluation of all offers, the ICE contracting officer will determine which business concern is the apparent successful offeror. If that business concern has submitted an award request, the contracting officer will review it, in consultation with other authorized agency officials, and assess the risk associated with the previous felony conviction. If the contracting officer determines that the conviction is not for a serious felony as defined by the regulation, or that the convicted individual no longer owns, controls or operates the business concern, the contracting officer will refer the award request to ICE's Head of the Contracting Activity (HCA) with a recommendation that the award request be approved. If the HCA approves the award request, the contracting officer may award the guard services contract to the offeror. If the HCA denies the award request, ICE will be prohibited under the Act and regulation from awarding the contract to that offeror as a result of the felony conviction.

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?

ICE will collect information on individuals convicted of a felony, when such individuals are represented by the offeror to own, control, or operate the business concern submitting an offer in response to a solicitation for FPS guard services. The information collected will include the individual's name and date of birth, a full description of which roles or interests indicate that the individual owns, controls, or operates, or may own control or operate the business concern; date sentenced, statute/charge (convicted offense), docket/case number, court/jurisdiction, nature and circumstances surrounding the conviction, protective measures taken by the individual or business concern to reduce or eliminate the risk of further

misconduct, whether the individual has made full restitution for the felony, and whether the individual has accepted responsibility for past misconduct resulting in the felony conviction.

ICE will also collect related information from official law enforcement sources to verify the information provided by the business concern, to the extent that it is available.

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

Information is received directly from a business concern that submits an offer in response to an ICE solicitation for FPS guard services. The business concern will be responsible for collecting the information from the individual convicted of the felony.

Information is also received from the Federal Bureau of Investigation's National Crime Information Center (NCIC) database to verify the information provided by the business concern, to the extent available.

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

This information is being collected to determine whether an individual that owns, controls, or operates the business concern submitting the offer, has been convicted of a felony that would disqualify the business concern from receiving a contract award. Collection of this information is mandated by the Federal Protective Service Guard Contracting Reform Act of 2008 (Pub.L. 110-356) and 48 CFR 3009.171.

1.4 How is the information collected?

ICE solicitations for FPS guard services will include a provision that requires any prospective offeror to submit the information in the form of an award request as part of their offer. The offer and award request, if any, are submitted electronically or in paper form depending on the particular instructions provided in each specific ICE solicitation. The final rule requires the business concern to collect the required information from the individual convicted of the felony, and to provide the individual with a written Privacy Notice detailing the authority and purpose of the collection, how the information will be shared, and whether providing the information is mandatory or voluntary.

1.5 How will the information be checked for accuracy?

The business concern will be responsible for collecting the required information from the individual convicted of the felony. The regulation requires the offeror to make a representation that the information is accurate. Any offeror who knowingly falsifies a material fact or makes a false statement is subject to criminal sanctions in accordance with 18 U.S.C. § 1001. In certain circumstances, ICE may also seek to verify or analyze the information through other sources. For example, if a business concern representing that it is owned, controlled or operated by an individual convicted of a felony is the apparent successful offeror, the contracting officer may request the assistance of the FPS Suitability and

Adjudication officials and/or ICE's legal counsel in conducting an assessment of the conviction to determine if it is a serious felony under the regulation. As part of the assessment process, FPS may utilize the NCIC to retrieve records concerning the felony conviction. If the records obtained from NCIC show that the information submitted by the business concern is incomplete or inaccurate, the award request may be denied and the business concern will be ineligible for contract award.

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

The collection of this information is required by the Federal Protective Service Guard Contracting Reform Act of 2008 (Pub.L. 110-356) and 48 CFR 3009.171.

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

The privacy risk associated with collecting this information is that more personal information will be collected than is strictly necessary. While any offeror subject to this requirement must provide this information with their offer, the ICE contracting officer will only review the felony conviction information of the business concern that is considered to be the apparent successful offeror. Because the Act specifically requires felony conviction information be submitted to ICE with all proposals for FPS contract guard services, ICE does not have the discretion to limit its collection of conviction information to only those business concerns that are the apparent successful offeror. This privacy risk is somewhat mitigated by the fact that the conviction information requested is limited to the minimum amount of information necessary for the contracting officer to determine whether the conviction is serious under the regulation, and should prohibit the vendor from receiving a contract award.

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 will use this information to determine whether an individual that owns, controls, or operates a business concern has been convicted of a serious felony that would disqualify the business concern from receiving a contract award for FPS guard services. This information will be used by ICE government personnel and contractors or other authorized agents to assess the individual's felony conviction (for apparent successful offerors only) and determine whether an award request should be approved or denied under the regulation. ICE may share this personal information with the U.S. Justice Department and other Federal and State agencies for collection, enforcement, investigatory, or litigation purposes related to the contract award, enforcement, litigation, or other matters associated with the contract. For example,

information may be shared with the General Accountability Office (GAO) or the DHS Inspector General's office in response to an audit or investigatory request.

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

No automated data processing systems or tools are used to analyze the felony conviction information.

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

ICE does not use commercial or publicly available datasets in the course of this regulatory process.

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.

All ICE employees and contractors are required to comply with the Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS, which details security and privacy controls for the appropriate handling of sensitive personal data.

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 offeror will submit to ICE the felony conviction information with its proposal either electronically or in paper format as directed by the solicitation instructions. ICE will retain the successful offeror's proposal including any and all supporting information related to former felony convictions of its owners, controllers, and operators. After contract award, felony information submitted by the successful offeror will be stored separately from the official contract file in a secured location. If the felony information is provided in an electronic format, the information will be converted to hard copy format and stored in a secured location. Electronic information related to a specific individual and their felony conviction will not be stored on the ICE computer system. ICE also retains felony information for unsuccessful offerors.

3.2 How long is information retained?

Pursuant to Federal Acquisition Regulation (FAR) 4.804 and the General Records Schedule (GRS) 3, contract files and any unsuccessful proposals that are stored with that contract file must be retained for six years and three months following completion of the contract (generally based on final payment, but see 48 CFR 4.805). Under GRS 3, unsuccessful proposals that are stored separately from the contract file need only be retained until the contract is completed. Due to the storage limitations, unsuccessful proposals are typically stored separately from the related contract file.

In order to further mitigate the risk associated with unauthorized disclosure, ICE proposes to retain the felony conviction information for a shorter period than is currently specified by the National Archives and Records Administration's General Records Schedule (GRS) 3. ICE intends to request NARA approval to retain felony information for any successful offeror only until the related contract is physically completed. The average period of performance for guard service contracts is five years. Once the related contract is considered to be physically complete, the felony information will be destroyed. It will further be proposed that felony information submitted by unsuccessful offerors be retained only until the contract award decision is announced and the protest period has lapsed. Generally, the contract award process for FPS Guard Contracts can take up to nine months, sometimes longer, from the date initial offers are received in response to a solicitation. Once the contract award decision has been announced and the protest period has lapsed, the felony information submitted by the unsuccessful offeror will be destroyed. For procurements that result in litigation, the files related to that litigation will be retained for three years after final court adjudication, consistent with GRS 3.

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

GRS 3 and the FAR 4.804 currently provide retention periods for contract solicitation materials. Agency procedures dictate that we follow the GRS unless a deviation is obtained. ICE is in the process of requesting a deviation from some retention periods in GRS 3 to allow ICE to destroy felony conviction information at the point it is no longer needed. Due to the fact that the FAR allows agencies to prescribe their own record retention procedures, a FAR deviation is not required.

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

There is a risk that information about individuals' felony convictions will be retained for a longer period than necessary to accomplish the purposes of this regulatory program. ICE proposes to retain the information concerning felony convictions for the minimum period of time needed to accomplish the purposes of this regulatory program. The proposed retention periods are appropriately limited to the purposes for which the information is collected, namely the award of contracts and the contract administration process.

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?

This information may be shared with or disclosed to DHS personnel and contractors for purposes related to agency oversight. For example, the DHS Inspector General may request access to this information as a part of an audit or investigation.

4.2 How is the information transmitted or disclosed?

ICE may share information by electronic or paper means. If information is transmitted electronically, proper security measures are taken in accordance with the Handbook on Safeguarding Sensitive PII at DHS, including encryption when appropriate.

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.

Inappropriate sharing is a risk inherent to any collection of personally identifiable information (PII). DHS employees and contractors are trained on the appropriate use and sharing of PII. Further, any sharing of information must align with the purpose of the initial collection as well as the Privacy Notice provided at the time of collection.

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?

ICE may share this information with the U.S. Justice Department and other Federal and State agencies for collection, enforcement, investigatory, or litigation purposes related to the contract award, enforcement, litigation, or other matters associated with the contract. For example, information may be shared with the General Accountability Office (GAO) as a part of an audit or investigation.

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 primary purpose of the information collection is for the Department's internal use to determine whether an individual that owns, controls, or operates the business concern submitting the offer has been convicted of a felony that would disqualify the offeror from receiving a contract award. Sharing this information with other Federal and State agencies for purposes related to the contract award or the contract, such as litigation or oversight activities, is consistent with the original purposes for which the data was collected.

Because the information collected on individuals' felony convictions under this final rule is be stored in the ICE Office of Acquisition Management recordkeeping system by the contract name and number, this information is not a part of a Privacy Act system of records and a system of records notice (SORN) is not required.

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

Any information shared with organizations outside the Department is required to be appropriately secured per Office of Management and Budget Memoranda 06-15, *Safeguarding Personally Identifiable Information*, and 06-16, Protection of Sensitive Agency Information and the *DHS Handbook for Safeguarding Personally Identifiable Information*. These policies require that electronic files containing PII be transported and stored in an encrypted format, stored only on Government furnished equipment and physically secured when in transit. Hard copy PII must be stored in locked compartments.

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

A privacy risk exists that data will be improperly disclosed for purposes that are unrelated to the initial collection. With respect to the information collected under this rule, ICE will only share information outside DHS when it is consistent with the purposes for which it was collected, namely the award of contracts and the contract administration process.

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?

Yes. The final rule requires that any affected business concern provide the individual with a written privacy notice regarding the voluntary nature of the collection, its intended purpose, routine uses, and ICE's authority to collect the information. It is anticipated that the award request form will also contain a privacy notice.

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

Yes. Submission of this information by the individual is voluntary, however, failure to provide it may result in denial of a contract award to the business concern itself.

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. Individuals do not have the option to provide for particular uses of their information. ICE will use their information for the purposes described in this PIA and the privacy notice provided to the individual.

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.

A privacy risk associated with the collection of felony information is that the individual is not aware of the purpose for which the information he or she submits may be used. The final rule requires that the business concern provide a privacy notice to the individual from whom the information is collected. This risk is also mitigated by limiting the use of information to what is necessary for the purposes of determining whether the felony conviction should preclude a vendor from being awarded a contract for guard services. Furthermore, this regulation was promulgated through a notice and comment process, and public comments were received and considered in the development of the final rule. This public posting also provided advance notice to individuals about this collection of information. Prior to submission, the individuals will know the PII related to felony convictions is required as part of the FPS solicitation process, there fore the individual will know the information will be collected and may be used.

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 seeking notification of and access to any record described in this PIA, or seeking to contest its content, may contact the contracting officer of record or submit a request in writing to ICE's Freedom of Information Act (FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one DHS component maintains 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.

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

Should individuals seek to correct inaccurate information or remove their information from an offer that has been submitted in response to a solicitation for FPS guard services prior to contract award, an authorized representative of the business concern submitting the offer must contact the contracting officer of record and request that the firm's offer be formally withdrawn or submit a revision or modification to the offer. After contract award, it is recommended that an authorized representative of the business concern that submitted the inaccurate or erroneous information contact the contracting officer of record. The contracting officer will handle such requests on a case by case basis.

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

The procedure for submitting a request to correct information is outlined in this PIA in Questions 7.1 and 7.2.

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

As stated above, individuals may submit requests for access and correction.

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

As described above, individuals will be able to access and seek correction of the felony conviction information that was provided to ICE during the contract solicitation process. These procedures are appropriate to address the transparency and data accuracy concerns related to the maintenance of this type of information about individuals.

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?

ICE Office of Acquisitions intends to issue an internal policy directive which will delineate how the acquisition office is to handle, store and safeguard felony information. Felony information for successful offerors will be stored in hard copy in a secured location that can only be accessed by a limited number of authorized DHS personnel who have a need to know in the course of their official duties. The internal policy will dictate which authorized personnel will maintain and have access to the hard copy felony information. ICE does not intend to store electronic copies of felony information on the ICE network. If internal or external sharing of the information is done electronically, the information will be secured per Office of Management and Budget Memoranda 06-15, *Safeguarding Personally Identifiable Information*, and 06-16, *Protection of Sensitive Agency Information*, and the *DHS Handbook for Safeguarding Personally Identifiable Information*.

8.2 Will Department contractors have access to the system?

Department contractors may be required to have access to information concerning individuals' felony convictions. ICE Office of Acquisition uses contractors to support various acquisition-related functions to include contract closeout and other tasks that may involve access to the felony conviction information. The FPS Suitability Branch also may use contractor support to run reports and provide a risk assessment. The Department conducts thorough background checks on every employee and contractor. All contractors are required to sign non-disclosure agreements which prohibit the use and release of this information without proper authorization. Furthermore, all Department employees and contractors are trained on security procedures, specifically as they relate to PII.

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

All ICE personnel and contractors complete annual mandatory privacy and security training and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information.

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

This PIA describes an ICE regulatory program and not an IT system; therefore, a Certification & Accreditation is not required.

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

All Department information systems are audited regularly to ensure appropriate use and access to information. Specifically related to an individual's felony information, such information residing on a local area network's shared drive are restricted by access controls to only those personnel in the Office of Acquisition Management who require it for completion of their official duties.

Electronic copies of the documents are stored on government-furnished equipment that complies with DHS and ICE security standards. Electronic copies may also be stored on a shared drive on the ICE network that is accessible only to individuals working in the ICE contracts office. Hard copies of proposals are stored in ICE facilities that can only be accessed by authorized DHS personnel.

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 risk of unauthorized access exists with any information technology system or document. The Department conducts thorough background checks on every employee and contractor. Access to the systems and networks which store the information are protected pursuant to established Departmental procedures.

All Department employees and contractors are trained on security procedures, specifically as they relate to PII.

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 is a regulatory program related to the appropriate administration and award of FPS contracts.

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

This regulatory program is not an IT system and was therefore not developed using a lifecycle.

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

Appendix: Privacy Statement

Privacy Notice. The collection of this information is authorized by the Federal Protective Service Guard Contracting Reform Act of 2008 (Pub. L. 110–356) and Department of Homeland Security (DHS) implementing regulations at Homeland Security Acquisition Regulation (HSAR) 48 CFR 3009.171. This information is being collected to determine whether an individual that owns, controls, or operates the business concern submitting this offer has been convicted of a felony that would disqualify the offeror from receiving an award. This information will be used by and disclosed to DHS personnel and contractors or other agents who require this information to determine whether an award request should be approved or denied. Additionally, DHS may share this personal information with the U.S. Justice Department and other Federal and State agencies for collection, enforcement, investigatory, or litigation purposes, or as otherwise authorized. Submission of this information by the individual is voluntary, however, failure to provide it may result in denial of an award to the offeror. Individuals who wish to correct inaccurate information in or to remove their information from an offer that has been submitted should contact the business concern submitting the offer and request correction.