Privacy Impact Assessment
for the

DHSAccessGate System

December 3, 2007

Contact Point
Herbin L. Gray
DHSAccessGate Program Office of Security/DHS-HQ
(202) 282-9787

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

Abstract

The Department of Homeland Security (DHS) is adding a new layer of security to its vendor employee access control procedures at certain facilities by offering a new and voluntary vendor program called the DHSAccessGate Program. Part of this program will involve the collection of personally identifiable information from individuals who are not DHS employees or contractors. The DHS Office of Security has conducted this privacy impact assessment because of the collection of new personally identifiable information.

Introduction

The DHS Office of Security is partnering with a service provider from the private sector to facilitate a new voluntary program at the DHS-HQ Nebraska Avenue Complex ("NAC") and other designated component facilities. The DHSAccessGate Program ("Program") will be offered on an optional basis to DHS-HQ-sponsored vendor companies and approved vendor employees who desire expedited, more convenient entrance at DHS-HQ facilities. For example, an electrician who will need regular access to the NAC for work on a building may consider utilizing the Program. Or, a vending machine supplier who regularly accesses NAC buildings to replenish vending machines may apply to the Program so that each visit to this facility is not slowed by the existing check-in process.

Participation in the Program will be strictly voluntary, and vendor employees will be under no obligation to join the Program. The Program will not replace existing visitor pass access control procedures.[1] Rather, the Program will be an optional alternative to those procedures.

To implement the Program, DHS-HQ will contract with a private service provider ("Service Provider") to provide registration, background screening, and related services.

The Program can be divided into four (4) distinct phases: Registration, Security Threat Assessment, Adjudication, and Badging. This introduction will outline the procedures for each phase. The numbered sections which follow will discuss the Program in detail.

Program Registration

DHS-HQ, in its sole discretion, will approve and sponsor the vendor companies whose employees will be eligible to register for the Program. DHS-HQ will provide the Service Provider with a list of DHS-HQ-approved vendor companies. Vendor companies not on the list that wish to participate in the Program may make a request to DHS-HQ.

The DHS-HQ-sponsored vendor companies each will designate a representative within their company to serve as the company's Program Administrator. The Program Administrator will serve as the vendor company's point of contact for the Program. The Service Provider will inform the Program Administrator when its company has been authorized by DHS-HQ to register for the Program. The Service Provider will

[1] Current access procedures involve a DHS employee submitting a Form 11000-13 to the Office of Security requesting access for specific individuals. The form must be submitted 48 hours prior to the arrival of the individual. Based on the reason for the person's visit and whether the Form 11000-13 has been submitted before the 48 hours the DHS employee may be required to escort the individual throughout the NAC premises.

issue a separate personal identification number (PIN) number to each vendor company for employee registration.

Vendor employees who wish to participate in the Program will register at the Service Provider's kiosk located at the DHS-HQ facility. The kiosk is a sit-down station with semi-enclosed sides for privacy. It contains a keyboard, camera and fingerprint reader. Vendor employees will begin the registration process by typing in their vendor company's PIN number. At the kiosk the employees then will input the following biographic and biometric information:

- Name
- Company
- Current residence address and billing address
- Date of birth
- Social security number (providing the social security number is voluntary, but failure to do so may prevent completion of the registration, performance of the background screening and activation of the Program badge)
- Digital photograph of face
- Digital fingerprint images

All PII collected by the Service Provider at the registration kiosk will be immediately encrypted. The PII then will be electronically transmitted over a secure Internet connection to the Service Provider's data center.

Security Threat Assessment (Background Screening)

The Service Provider will securely transmit to its Commercial Provider the biographic information it collects from vendor employees to perform background screenings of them. The background screenings will be conducted in strict accordance with DHS-HQ's specifications. The specifications are:

- Social security number validation and address verification
- Fraud database search
- Federal, state and county criminal history search
- Sex offender registry(ies) search
- Wants, outstanding warrants search
- Office of Foreign Assets Control (OFAC) Terrorist Watch List[2]

[2] The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers

Fingerprint-based criminal history records checks will not be performed.

The Commercial Provider will search various available data sources including a federal court database and a national criminal history database maintained by the Commercial Provider. The Commercial Provider's national criminal history database contains criminal history data from all 50 states and the District of Columbia that is reported and regularly updated by court systems, corrections departments, law enforcement, sex offender registries and other agencies at the state, county and municipal levels. A physical search of county records may be conducted to verify a disqualifying event that has been revealed during a database search.

A disqualifying event producing a "fail" result will exist based upon any one or more of the following: identity failure from social security number search; felony conviction within the DHS-HQ address history specifications; listing on a sexual offender registry; listing on the OFAC Terrorist Watch List; or any outstanding wants or warrants. Background screenings will be conducted immediately following Program registration and approximately every three (3) months thereafter including at annual renewal so long as the vendor employee remains in the Program. This ensures that the employee's threat risk suitability has not changed.

Neither DHS-HQ nor the Service Provider will receive from the Commercial Provider a copy of individual background screening reports. However, the Service Provider will authorize a limited number of its trained employees, who have a "need to know" in the performance of their official duties, to have password-protected access to the Commercial Provider's web portal to view the Commercial Provider's background screening data on individual Program participants. The Service Provider's authorized employees may need to view the data to check on the status of a background screening, confirm the results of a background screening, and/or to prepare aggregated statistical reports to DHS-HQ.

Because the PII is not being collected for employment purposes, the Service Provider will require vendor companies to agree that they will not use for employment purposes the "pass" or "fail" results of the Program background screenings conducted on their employees. Vendor companies thus will be barred from taking adverse employment action against their employees based upon the "pass" or "fail" results provided by the Service Provider.

Adjudication ("Adverse Action") Process

As part of the privacy protections afforded by the Program, users of background screening reports (referred to under the Fair Credit Reporting Act (FCRA) as "consumer reports") are required to follow certain adjudication procedures if they take adverse action against the subject of the screening that is based in whole or in part on any information contained in the consumer report. (FCRA 15 U.S.C. 1681m.) Accordingly, vendor employees who volunteer to undergo Program background screenings will have full FCRA rights of adjudication in the event of a background screening "fail." These protections are in accord with and in addition to any protections provided by the Privacy Act such as notice, access and redress. Details of these procedures are provided in Section 7.0: Redress.

---

designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them.

To summarize, the vendor employee will be mailed a written notification from the Commercial Provider if the employee has "failed" a Program background screening. The notification will be comprised of:

- An Adverse Action cover letter from the Commercial Provider notifying the vendor employee of the background screening "fail" result and the fact that adverse action is planned against the employee
- A copy of the background screening report
- A written summary of the employee's rights under the FCRA
- A Dispute Notification Form to be filled out if the employee wishes to dispute the "fail" result.

If the vendor employee notifies the Commercial Provider that he or she wishes to dispute the "fail" result, the Commercial Provider will conduct a dispute investigation in accordance with the FCRA. The Commercial Provider will provide the vendor employee with a written report of the results of the dispute investigation and a copy of the Amended Background Screening Report if the dispute investigation results in any change.

The Service Provider will inform vendor companies that a background screening "fail" may have occurred for any number of reasons, including possible identity theft, and that the vendor's employee has the right to dispute the result through the Adverse Action process. The vendor employee also will have the ability to appeal directly to DHS-HQ.

Program Badge Process

After a Participant Vendor employee passes the background screening, the Service Provider will manufacture and securely ship to DHS-HQ a Program badge for the employee. At the NAC, DHS-HQ will use the Program badge only once to verify identification of individuals who have passed the Program background screening. Based on the verification of the badge and the individual, DHS-HQ then will prepare and issue its own physical access badge to these individuals.

The Service Provider will notify the employer's Program Administrator when the Program badge is ready for pickup at DHS-HQ. The Program Administrator in turn will inform the employee. The employee then will phone a toll-free number of the Service Provider to request activation of the badge by providing his or her name and the last four digits of the employee's social security number. Upon receipt of this identity verification the Service Provider will remotely activate the badge. The employee will go the designated DHS-HQ facility to process the badge.

A DHS-HQ access control representative will read the barcode on the badge by using a handheld device attached to a computer station housed at the DHS-HQ facility; the computer station is owned and controlled by the Service Provider. The computer station will contain a local database of DHS-HQ facility. Program participants whose data was securely transmitted in encrypted form through a dedicated telephone line from the Service Provider's Data Center and which is updated regularly. The barcode contains no personally identifiable information (PII) and is encoded only with a unique identifier. The computer station will query for the unique identifier in its own internal database. If the identifier is valid, the name, photograph, company name, and access privilege status associated with the individual assigned to the badge will appear on the computer station screen. (The computer station is a "stand-alone" system not connected to or accessible by any Government networks.)

DHS-HQ will be able to perform secondary identity verification by having the individual place a finger on a module on the computer station to read the individual's fingerprint and compare it with the fingerprint template associated with the badge as stored in the local database. (No fingerprint image is stored on or retrievable from the local database.) The computer station will display whether or not there is a fingerprint match; the fingerprint template itself will not be displayed.

To further verify the vendor employee's identity, the employee will present to DHS-HQ for its review a copy of the employee's I-9 documentation.[3]

Once DHS-HQ has completed processing the Program badge, the identity and Program eligibility verification process is complete.

The remainder PIA will discuss the specific details of the Program.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The Service Provider will collect the following biographic information from Program registrants in order to conduct its background screenings:

- Full legal name
- Company
- Date of birth
- Current residence address and billing address
- Social security number

Participation in the Program, and therefore provision of the requested information including Social Security Number, is voluntary. However, failure of the registrant to provide all of the requested biographic information will prevent completion of the registration and background screening process. Vendor employees are not eligible to participate in the Program if they do not pass the Program background screening.

The Service Provider also will collect the following biometric information from Program registrants in order to allow DHS-HQ to verify vendor employee identity and eligibility to participate in the Program:

- Digital photograph
- Digital fingerprints

In addition, at the Program badge issuance process, DHS-HQ will require vendor employees to produce acceptable I-9 documentation to verify identity. DHS-HQ will review but not retain these identification documents. The Service Provider will neither review nor collect these documents.

[3] The lists of acceptable identification documents are described in *Form I-9, OMB No. 1615-0047, Employment Eligibility Verification*, subject to any updates as referenced by the U.S. Citizenship and Immigration Services at www.uscis.gov

1.2 From whom is information collected?

Biographic and biometric information will be collected directly from the vendor employees when they register at the Program registration kiosk which is owned, managed, and controlled by the Service Provider. The kiosk will be placed at a convenient location at the DHS-HQ visitor's center.

Vendor employees who have passed the Program background screening also may be required to present their fingerprint at Program badge issuance, to determine whether the fingerprint at badge issuance matches the template of the fingerprint collected by the Service Provider at registration (the template is stored in the Service Provider's computer station local database), as secondary verification of the employee's identity. DHS-HQ will conduct this fingerprint match one time only, at badge issuance. DHS-HQ will not view, and will not collect or retain, Program participants' fingerprint image or template.

1.3 Why is the information being collected?

Biographic information will be collected from vendor employee Program registrants to conduct an initial security threat assessment and ongoing additional security threat assessments of Program participants throughout their membership in the Program. The Service Provider, through its Commercial Provider, will use the social security number and address information to verify identity. Address history also will be used as a basis for the criminal background history portion of the screening. The Service Provider will compare the applicants' information against terrorist-related, criminal history and law enforcement databases to ensure that the applicant meets the risk suitability requirements of DHS-HQ for purposes of Program participation. The social security number will be used to conduct the SSN validation process, to provide a means of conducting the criminal history search, and to verify identification to activate the Program badge.

The biometric information will be used to verify vendor employees' identity and Program eligibility at the time they appear at the designated DHS-HQ facility for the Program badge process.

1.4 How is the information collected?

a. *Biographic information*

The Service Provider will collect vendor employees' biographic information (name, company, current residence and billing address, date of birth and social security number) as well as their biometric information (digital photograph and digital fingerprints) at a registration kiosk.

The kiosk will be owned, maintained, and controlled by the Service Provider. The kiosk will be placed at a convenient location at the DHS-HQ visitor's center. The kiosk will have privacy sides (lateral vision enclosures) and a chair, and will be installed with a keyboard, monitor screen, a digital camera and fingerprint reader. The vendor employee applicant will be seated before the keyboard. The applicant will type in the requested biographic information on a series of screens displayed on the monitor.

To proceed with registration, the applicant first will be required to read and "accept" a written notice on the kiosk screen that will explain what information is being collected, the purposes of collection, the uses of information, and the terms and conditions of participating in the Program. The notice also will explain that participation in the Program does not guarantee entry at any DHS-HQ facility, and that DHS-HQ always maintains the right to decide who can and cannot enter its facilities. If the applicant does not wish to

accept the terms of the notice, the applicant can click "I do not accept" and automatically will be "quit" from the registration process.

If the applicant accepts the notice, the applicant will type in his or her biographic information. To identify and allow for correction of errors in the typing of the social security number, the applicant will be required to type in the number on two separate screens. Both social security number entries must match in order for the registration to proceed. The social security numbers will not be displayed on the screen; only "x's" will be displayed.

The final page of the kiosk screen will display the biographic information keyed in by the applicant (for privacy reasons, the social security number will not be displayed) for the applicant's final review. The applicant will be able to correct any erroneous information at that time. Once the applicant is satisfied that the information is correct, the applicant will complete the registration by transmitting the designated button.

b. *Biometric information*

Biometric information (digital photo image, fingerprint images) also will be collected at the registration station. To collect the digital photo image, one of the registration screens will ask the vendor employee to look at the camera immediately above the screen, center his or her image with the roller ball mouse, and click the camera to record the image. The digital photo image then will be displayed on the screen. If the applicant is not satisfied with the photo image, the applicant will be able to re-take the photo. The applicant will click his or her acceptance of the photo image.

To collect the fingerprint images, the applicant will receive on-screen instructions on placement of the individual index finger and thumb for both the right and left hand. Placement will be made on a glass screen adjacent to the keyboard. Duplicate images will be recorded (and must match) for each of these digits. The fingerprint reader is calibrated to reject images unless they are clear and readable, and to reject the duplicate image if it does not match with the first image.

Vendor employees who have passed the Program background screening also may be asked to provide biometrics at the time they appear at the designated DHS-HQ to process the Program badge. The employee may be required to present his or her fingerprint image to match against the fingerprint template stored in the computer station local database, as secondary verification of the employee's identity.

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

The Secretary of Homeland Security has broad powers to protect the buildings, grounds, and property that are owned, occupied or secured by the Federal government and the persons on the property, and may prescribe regulations necessary for the protection and administration of property owned or occupied by the Federal government and persons on the property. (40 U.S.C. 1315(a) and (c).) Collection of this information is authorized by the Homeland Security Act of 2002; National Security Act of 1947; 44 U.S.C. chapters 21, 29, 31, and 35; 5 U.S.C. Sections 301, 3301, and 7902; 40 U.S.C. 1315; Executive Orders 10450, 10865, 12333, 12356, 12958, as amended, 12968, 13142, 13284; the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, Section 3001 (50 U.S.C. 435b).

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

The information collected will be used to conduct background screenings (security threat assessments) on vendor employees who volunteer to participate in the Program, and to verify their identity. Vendor employees who pass the background screening will be eligible to receive a physical access card from DHS-HQ to present to enter the designated facility.

An important element of the Program is the fact that participation will be strictly voluntary. Vendor employees who are concerned about the privacy implications of providing the PII requested of the Program will be able to choose not to participate in the Program and instead continue to use the DHS-HQ facility's standard access procedures.

In addition, to allay concerns of private citizens who may not wish to share their PII with the government, the Program has been designed to minimize the amount of PII that the Service Provider shares with DHS-HQ. For purposes of the Service Provider's collection, use and storage of PII, Program participants will have broad privacy protections accorded to them under the FCRA and any other applicable laws. Program participants also will have a contractual relationship with the Service Provider through an Individual User Agreement, which imposes obligations upon the Service Provider to maintain privacy safeguards. DHS-HQ is mandated by federal law (i.e., the Privacy Act) to maintain privacy protections of Program participant PII.

The Service Provider will employ the principle of least-privilege access and will use strong encryption on PII, and will encrypt its entire database backups to protect the data. Individual dates of birth, social security numbers and biometrics will be encrypted prior to being placed in the Service Provider's database. PII collected during registration will be temporarily stored in encrypted form on the registration station and then will be transmitted in encrypted form to the Service Provider's Data Center, at which time the information will be deleted from the registration station.

The Service Provider's database will be a stand-alone system that will not be connected to any DHS-HQ or other Government network or server. The Service Provider will securely transmit PII data using FIPS 140-2-compliant encryption algorithms to communicate over telephone lines to send Program participant information to and from the Service Provider's Data Center. Neither DHS-HQ nor any other government agency will have physical or logical access (i.e., connection of computer systems or networks) to the Service Provider's database.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The biographic and biometric information that is gathered from vendor employees who voluntarily register for the Program will be used for the following purposes:

- To conduct background screenings (security threat assessments) on individuals who wish to participate in the Program;
- To use biometric technologies to verify the identity of Program participants;

- To manufacture a Program badge that is used to verify the identity of Program participants and verify their eligibility to participate in the Program;
- To prepare aggregated statistical reports to DHS-HQ on the total number of enrolled Participant vendor companies and their registered employees and the total number of background screening fails, passes and successful adjudications (the reports will contain no PII); and
- To assist in the management of Program participant records and background screenings.
- To conduct a check of state, local, and municipal felony convictions the Commercial Provider uses biographic information

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

No. Note, however, that the Service Provider will use collected information to prepare aggregated statistical reports to DHS-HQ containing no PII. The Service Provider will be allowed to collect PII only for the purposes of the Program.

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

The Service Provider will collect biographic and biometric information directly from the vendor employees who choose to participate in the Program. Vendor employee applicants will type their social security number twice (requiring a match) to minimize the risk of a typing error, and they will have an opportunity to review and approve all other PII they type into the registration kiosk before clicking the submission button.

The Service Provider through its Commercial Provider will check the accuracy of individual biographic information through the background screening process by conducting a social security number search and address verification search. Part of the background screening process involves a Quality Assurance review to resolve any inconsistencies among identifying information provided by the Vendor employee. The Service Provider's Commercial Provider will assign trained professionals to conduct a Quality Assurance review of completed background reports and to maintain an audit process for background screening reports to ensure their accuracy, completeness and quality. The Commercial Provider will provide, to Vendor employees who "fail" the Program background screening, written notice of the screening results, a copy of the background screening report, notification of the employee's right to adjudicate the results by requesting a re-screening, and a dispute form. If the reason for the "fail" is that the employee provided inaccurate data, the employee will have an opportunity to correct the inaccuracy through this Adverse Action process.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Collected individual information will be used only for the purposes stated in this PIA. The Service Provider will authorize only a limited number of Service Provider personnel to perform Program services that involve handling of PII. The Service Provider will not disclose to DHS-HQ or participant Vendor companies any vendor employee's background screening report or the contents of such report, but will inform them of the employee's "pass/fail" status. The Service Provider will require participant Vendor companies to agree they will not use this "pass/fail" information for employment purposes.

Because the Program will be using the services of the Commercial Provider, ensuring the accuracy of the use of such data is an important privacy mitigation step. Should the Commercial Provider disqualify someone based on state, local, or other municipal record the Commercial Provider may physically locate the record and verify its accuracy. This ensures that individuals disqualified on the basis of Commercial Provider information, albeit information taken from state, local, and other municipal court systems, will be disqualified for verifiable reasons, i.e., the individual is a convicted felon.

Section 3.0 Retention

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

DHS-HQ retains limited individual information that it collects under this Program in accordance with the record schedules set by the National Archives and Records Administration (NARA) and in accordance with DHS Management Directive (MD) 11042.1 Safeguarding Sensitive and Unclassified Information (FOUO), and as described in the retention and disposal provisions of the Office of Security File System" (71 Fed.Reg 53700). If DHS elects to retain information identifying a person as being on an OFAC Terrorist Watch List, subject to an outstanding warrant or a fugitive, the information will be retained for at least 20 years.

The Service Provider will retain the individual information it collects under the Program for three years from the date of the individual's date of separation from the Program.

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

No, but DHS Records Management will officially submit and coordinate with NARA agency approval of its retention schedule. DHS-HQ will not destroy any Program records until after it has obtained NARA approval.

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

Program information will be maintained in accordance with the NARA-approved record retention schedules in furtherance of the purposes of this Program. DHS-HQ will destroy the record upon

notification of death or not later than 5 years after separation or transfer of the employee or later than 5 years after contract relationship expires, which ever is applicable. The service provider may retain the information for five years thereafter, to enable the Service Provider to make timely updates to its database to reflect changes in Program participants' status such as employment status changes and updated background screening results; to fulfill requests by individuals for information retained on them; to permit judicial review in the event of litigation; and to reduce the incidence of fraudulent applications.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

DHS-HQ will not share this information outside of the Office of Security or Internal Security.

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

Because DHS is not collecting the data elements minimal information sharing internal to DHS occurs. The Service Provider will transmit to DHS-HQ only the (1) name, (2) company and (3) background screening "pass" or "fail" result for each vendor employee who volunteers to participate in the Program

4.3 How is the information transmitted or disclosed?

The Service Provider will transmit the "pass" or "fail" via encrypted or password-protected electronic submission.

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

Internal sharing is left to the absolute minimum amount necessary. This mitigates a significant amount of information sharing risk. Any PII which may be disclosed internally will be transmitted or disclosed accordance with DHS Management Directive (MD) 11042.1 Safeguarding Sensitive and Unclassified Information (FOUO).

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Access to Information

To mitigate potential privacy concerns on the part of vendor employees, most PII collected through the Program will not be shared with DHS or other government agencies. The Service Provider will transmit to DHS-HQ only the (1) name, (2) company and (3) background screening "pass" or "fail" result for each vendor employee who volunteers to participate in the Program. The Service Provider also will inform DHS-

HQ if a background screening reveals that the subject is listed on the OFAC Terrorist Watch List, or is a fugitive or the subject of an open warrant. Additionally, the Service Provider will provide DHS-HQ with aggregated statistical reports that do not contain any PII.

As part of the background screening process, Service Provider will provide to Commercial Provider biographic information used to check felony convictions at the state, local, and municipal levels. This information may be manually verified should a match occur that might disqualify and individual from the Program.

Appendix A details which entities have access to PII during the course of an individual's Program membership.

Information about individuals that is received by DHS-HQ pertaining to a background screening failure may lead the government to conduct a National Crime Information Center ("NCIC") background check that may be shared without the individual's consent as permitted by the Privacy Act of 1974 (5 U.S.C. section 552a(b)), including to an appropriate government law enforcement entity, if records show a violation or potential violation of law; the Department of Justice, a court, or other adjudicative body when the records are relevant and necessary to a lawsuit; a federal, state, local, tribal, or foreign agency whose records could facilitate a decision whether to retain an employee, continue a security clearance, or agree to use a contract. The full System of Records Notice (SORN) with a complete description of routine uses was published in the Federal Register and can be viewed at: System of Records Notice, 71 Fed. Reg. 53697 (Sept. 12, 2006); Notice of Proposed Rule-Making, 71 Fed. Reg. 53609 (Sept. 12, 2006).

DHS-HQ may share an individual's biographic information with the Terrorist Screening Center ("TSC") and other national security organizations to the extent necessary to resolve potential matches, facilitate an operational response, or to advance intelligence, counterintelligence, law enforcement or other official purposes related to DHS or national security in accordance with the provisions of the Privacy Act and the applicable SORN.

5.2 What information is shared and for what purpose?

The Service Provider will share biographic information with its Commercial Provider to perform background screenings. The Commercial Provider will notify DHS-HQ, and the Service Provider or its Commercial Provider also may contact law enforcement, if a background screening reveals that a Program registrant is listed on the OFAC Terrorist Watch List or is a fugitive or the subject of an open warrant, in order to assist active law enforcement and national security. Individual information also is submitted against a national law enforcement submission to determine whether the subject is reported as missing, wanted, a fugitive or an escaped inmate, to assist active law enforcement and national security. The Service Provider also will inform the vendor employee's employer (through the Program Administrator) whether the employee passed or failed the background screening, for the purpose of informing the employer of the employee's eligibility (or non-eligibility) to participate in the Program.

As detailed in 5.1, DHS may share information with the appropriate law enforcement entity should the results of a background check warrant further investigation.

5.3 How is the information transmitted or disclosed?

All data to be externally shared by DHS-HQ will be transmitted electronically and will be encrypted in compliance with departmental policies. The Service Provider will programmatically and securely transmit to its Commercial Provider, through secure sockets layer (SSL) or encryption, individual biographic information to perform background screenings. Information submitted against the national law enforcement submission will be transmitted electronically, through encryption and password protection. The Service Provider will transmit "pass" and "fail" information to the employer's Program Administrator electronically or by phone. Biometric image data collected at registration stations will be handled as sensitive personal information throughout the process. Biometric images will be stored as compressed and encrypted data. In addition, biometric images and the biometric templates created from this data will be suitably controlled to prevent any interception, alteration, release, or other data compromise that could result in unauthorized use.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

DHS expects to contract with a service provider that is a principal provider of background investigations at eight major DOD facilities. As part of the background investigation, each subject will be required to submit designated PII. Participation in the Program is voluntary, and therefore providing this data will be voluntary; however, submitting the information will be required in order to proceed with the necessary background investigation that underpins an individual's ability to participate in the Program. In addition, information may be shared in accordance with the applicable SORN, the "Office of Security File System" DHS-OS-001 (see 71 F.R 53700). The Service Provider will contractually require its Commercial Provider to comply fully with the requirements of the FCRA and the Privacy Act, including the proper safeguarding of all PII on individuals who are the subject of background screenings. The Service Provider will be contractually required to treat PII as confidential and to adhere to adequate privacy safeguards.

5.5 How is the shared information secured by the recipient?

Any Federal agency receiving Program PII is expected to handle the information in accordance with the Privacy Act, that agency's SORN(s) and FISMA. In addition, information received from the Service Provider and its Commercial Provider must be protected against compromise through encryption technologies and physical security.

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

No specific training is required for this Program; however, any Federal agency receiving this information is expected to handle it in accordance with the Privacy Act and that agency's SORN(s). The Service Provider and its Commercial Provider provide privacy training to their personnel to ensure meeting DHS-HQ's Program standards.

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

DHS-HQ will share this information under the applicable SORN and the Privacy Act. The Service Provider will share biographic information with its Commercial Provider to perform background screenings, and a subset of biographic information to DHS-HQ. Names also may be submitted to federal law enforcement to check for fugitives or who are wanted, and may be submitted to law enforcement and/or the intelligence community, as appropriate, if an individual is found to be listed on the OFAC Terrorist Watch List.

Any privacy risks are mitigated by limiting sharing of this information, ensuring that recipients properly handle the information, and using secure transmission methods.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. The information collected by DHS-HQ will be associated with the "Office of Security File System" (71 Fed.Reg 53700). This SORN describes the information being collected, purposes of collection, routine uses, and policies and practices.

In addition, pursuant to the FCRA and consistent with the Privacy Act, the Service Provider will provide a comprehensive notice to vendor employees, in the form of a User Agreement, both at the registration kiosk and on the Service Provider's website. At the Service Provider's registration kiosk, each vendor employee will be required to read the User Agreement, which will provide detailed information about the types of information to be collected, the use of the information, the vendor employee's rights and obligations with respect to collected information, and the vendor employee's right to decline to provide the requested information and thereby withdraw from Program registration. The User Agreement also will describe the individual's right to request a copy of the background screening report(s) conducted on the individual as well as the right to dispute the results of the screening in the event of a background screening "fail" result. A copy of a User Agreement template is attached to this document as Appendix B. The registration kiosk is designed such that a Program registrant cannot continue with the registration process without assenting to the User Agreement. If an individual does not wish to assent to the User Agreement, the individual can exit the registration process and thereby opt out of participating in the Program. Such individuals will continue to use the DHS-HQ facility's standard access procedures.

The User Agreement also will be available for viewing and printing from the Contractor's website, where it will be available in both English and Spanish.

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

Yes. Participation in the Program is strictly voluntary, and vendor employees are under no obligation to join the Program. Vendor employees who choose not to participate in the Program will not be asked to provide the information for the Program. Such individuals may continue to use the DHS-HQ facility's standard access procedures.

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

The Service Provider's User Agreement provides individuals with an opportunity to consent to the specified uses described in the User Agreement. Individuals do not have the right to selectively consent to the specified uses.

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

The Service Provider will provide vendor employees with a comprehensive and meaningful notice form that details the types of information being collected, purposes of collection, uses of collected information and retention of collected information, thereby enabling the individuals to exercise informed consent prior to disclosing any information to the Service Provider. In addition, the System of Records Notices published by DHS provides robust notice about the nature of this collection, the uses of the information, and the overall purpose for which the information is collected.

In addition, individual privacy concerns are mitigated by the voluntary nature of the Program and by the fact that limited PII will be shared with the government.

Section 7.0 Individual Access, Redress and Correction

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

Vendor employees will have the right to review the PII on them that is retained by DHS-HQ, pursuant to the requirements of the Privacy Act. The procedures for requesting their information from DHS-HQ are described in the applicable SORN. Vendor employees also may have a right to obtain a copy of the DHS-HQ Program information on them through the Freedom of Information Act ("FOIA").

Vendor employees will also have the right to review the PII that is retained by the Service Provider and its Commercial Provider, pursuant to the requirements of the FCRA. The FCRA promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. The FCRA entitles individuals who are the subject of a consumer report, such as a background screening, to request the information in their file from a consumer reporting agency. (15 U.S.C. 2681g.) The User Agreement that must be reviewed and accepted by each Program registrant will describe the individual's right to request a

copy of the background screenings conducted on the individual as well as the right to dispute the information in the background screening report in the event of a background screening "fail" result. In addition, the Commercial Provider will provide a copy of the background screening report, and a summary of rights under the FCRA, to vendor employees who "fail" a Program background screening.

7.2 What are the procedures for correcting erroneous information?

The procedures for correcting erroneous information retained by DHS-HQ are governed by the Privacy Act and are described in the applicable SORN. Individuals may write to the System Manager, the Director of Departmental Disclosure, and state clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought.

As part of the privacy protections afforded by the Program, users of background screening reports (referred to under the Fair Credit Reporting Act (FCRA) as "consumer reports") are required to follow certain adjudication procedures if they take adverse action against the subject of the screening that is based in whole or in part on any information contained in the consumer report. (FCRA 15 U.S.C. 1681m.) Accordingly, vendor employees who volunteer to undergo Program background screenings will have full FCRA rights of adjudication in the event of a background screening "fail."

The vendor employee will be mailed a written notification from the Commercial Provider if the employee has "failed" a Program background screening. The notification will be comprised of:

- An Adverse Action cover letter from the Commercial Provider notifying the vendor employee of the background screening "fail" result and the fact that adverse action is planned against the employee (i.e., a badge will not be issued, where the vendor employee is a Program applicant; the Program badge will be disabled, where the vendor employee is a Program participant)
- A copy of the background screening report
- A written summary of the employee's rights under the FCRA
- A Dispute Notification Form to be filled out if the employee wishes to dispute the "fail" result.

If the vendor employee notifies the Commercial Provider that he or she wishes to dispute the "fail" result, the Commercial Provider will conduct a dispute investigation in accordance with the FCRA. The Commercial Provider will provide the vendor employee with a written report of the results of the dispute investigation and a copy of the Amended Background Screening Report if the dispute investigation results in any change.

The Service Provider will inform the vendor company of an employee's background screening "fail." The Service Provider will inform the vendor company that the "fail" may have occurred for any number of reasons, including possible identity theft, and that the vendor's employee has the right to dispute the result through the Adverse Action process. The Service Provider also will provide DHS-HQ with the names of individuals who "fail" the Program background screening. The Service Provider will inform the vendor company and DHS-HQ if an individual has successfully adjudicated a "fail" result.

The procedures for correcting erroneous information retained by the Service Provider and its Commercial Provider are governed by the FCRA. Where an individual disputes any information in a consumer report

and notifies the agency of such dispute, the agency is required to conduct a reasonable reinvestigation to determine whether the disputed information is inaccurate. (15 U.S.C. 1681i.) In the case of vendor employees who "fail" a Program background screening, the Commercial Provider will follow a comprehensive Adverse Action process, as follows:

- The Commercial Provider will promptly notify Participant Vendor employees by mail of a "fail" result. The Commercial Provider will send the employee (a) a cover letter explaining that the individual has "failed" a Program background screening, faces adverse action and has a right to review and dispute the accuracy of the background screening information; (b) a copy of the background screening report, (c) a summary of rights under the FCRA; and (4) a Dispute Resolution Form.
- The employee will be given an opportunity to provide a statement on the Dispute Resolution Form for return to the Commercial Provider.
- If the Commercial Provider does not receive a dispute from the individual after five days, the Commercial Provider will mail another Adverse Action letter to the subject employee.
- If the employee submits a dispute, the Commercial Provider will conduct a reinvestigation and notify the individual in writing of the disposition.
- If the individual still disputes the results, he or she can place a permanent statement to that effect and an explanation in the file of the Commercial Provider. However, if a "fail" result has not been changed to a "pass" following the Adverse Action process, the individual will not qualify to participate in the Program. This Adverse Action process takes at least 30 days.
- While the Adverse Action process is pending, the employee may continue to access the DHS-HQ facility in accordance with DHS-HQ standard access procedures. Likewise, in the event the "fail" result does not change, the vendor employee may continue to access the DHS-HQ facility in accordance with DHS-HQ standard access procedures.
- If the Commercial Provider's reinvestigation results in a change in the background screening result ("pass" instead of "fail"), the subject vendor employee will be so notified in writing. Thus having passed the background screening, the employee will qualify to participate in the Program.

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

The procedures for correcting erroneous information retained by DHS-HQ are described in the applicable SORN. The procedures for correcting erroneous information retained by the Service Provider and its Commercial Provider are referenced in the User Agreement that is located on the kiosk as well as the Service Provider's website. Correction procedures also are described in detail in the set of Adverse Action documents that is mailed to vendor employees who "fail" a Program background screening.

7.4 If no redress is provided, are alternatives available?

Redress procedures are provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Individuals may request access to or correction of their PII pursuant to redress processes including through a request pursuant to the Privacy Act or FOIA (DHS-HQ), in accordance with the FCRA, or pursuant to the Adverse Action process (Service Provider and Commercial Provider), consistent with exemptions contained in the SORN and pursuant to applicable law.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

In order for DHS-HQ to manage, upgrade and utilize the system, system administrators, security administrators, IT specialists, analysts and other persons may have a need to access the system or the information in the system in the performance of their duties. Role-based access controls will be employed to limit the access of information by different users based on the need to know. DHS-HQ also will employ processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users will be permitted access to system resources. Strict adherence to access control policies will be automatically enforced by the System in coordination with and through oversight by DHS-HQ security officers.

Likewise, in order for the Service Provider and its Commercial Provider to manage, upgrade and utilize their own separate private databases, their database administrators, security administrators, IT specialists, analysts and other persons may have a need to access the databases or the information in the databases in the performance of their duties. Role-based access controls will be employed to limit the access of information by different users based on the need to know. For example, only a limited number of Service Provider personnel who have a need to know will be authorized to receive password-protected access to the Commercial Provider's background screening report information on vendor employees who have registered for the Program. The Service Provider and its Commercial Provider also will employ processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users will be permitted access to database resources. Strict adherence to access control policies will be enforced by the Service Provider's and the Commercial Provider's management.

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

Neither the Service Provider nor its Commercial Provider will have physical or logical access to the System. DHS-HQ may use contractors to perform IT maintenance and security monitoring tasks; such contractors will have access to the System in order to perform their official duties. All contractors performing this work will be subject to Homeland Security Acquisition Regulation (HSAR) requirements for suitability and a background investigation.

No DHS-HQ or other Government user groups will have physical or logical access to the Service Provider's or its Commercial Provider's separate private databases.

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

Role-based access controls are used for controlling access to the System using the policy of Least Privilege, which states that the System will enforce the most restrictive set of rights/privileges or access need by users based on their roles.

The Service Provider and its Commercial Provider also will adhere to the policy of least privilege, for controlling access to their respective private databases. They will create roles for each level of access required for their employees to perform their job functions and will follow procedures including security and privacy training, and need-based job responsibility.

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

The system maintained by DHS-HQ, and the separate private databases maintained by the Service Provider and its Commercial Provider, all will be secured against unauthorized access through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards.

Personnel for DHS-HQ, the Service Provider and its Commercial Provider all will receive mandatory privacy training on the use and disclosure of Program-related PII. They also will receive any appropriate security training and have any necessary background investigations for access to sensitive information based on their respective security policies and procedures.

All government and contractor personnel will be vetted and approved for access to the facility where DHS-HQ's system is housed, issued photo badges with integrated proximity devices imbedded, and given specific access to areas necessary to perform their job function. A Rules of Behavior document will provide an overall guidance of how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees will be required to read and sign a copy of the Rules of Behavior prior to receiving access to the System. Similar vetting, badging and rules of behavior will be in place for the personnel of the Service Provider and its Commercial Provider who will have access to the separate private databases containing Program-related PII.

All personnel working in or accessing the DHS-HQ facility are required to wear a security office issued control badge with photo and name. The badges will provide the electronic access control cards used to gain entrance to the secure area for the computer operations room. Badges must be worn and displayed at all times while on the premises. Badging and access control rules also will be in place for the personnel of the Service Provider and its Commercial Provider who will have access to the separate private databases containing Program-related PII.

DHS-HQ will handle its system data in accordance with the Privacy Act and the System will comply with FISMA requirements. The Service Provider and its Commercial Provider will maintain their separate private databases that contain Program-related PII in conformance with the FCRA and consistent with the Privacy Act and FISMA. The Service Provider and its Commercial Provider will be required to document how their separate private databases meet with these standards.

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

Employees or contractors are assigned roles for accessing DHS-HQ's System based upon job function. The Facility Security Officer and the Information System Security Officer coordinate to ensure compliance to policy, and manage the activation or deactivation of both physical and computer accounts and privileges as required or when expired. DHS-HQ ensures that personnel access the System have security training commensurate with their duties and responsibilities. All personnel are trained through DHS-HQ's security and awareness training program when they join the organization and periodically thereafter. The status of personnel who have completed the training is reported to DHS-HQ on a regular basis.

The Service Provider and its Commercial Provider both follow similar processes and procedures with respect to role assignment and verification according to established security and auditing procedures. Typically their supervisors assign access roles and review such roles on at least an annual basis to ensure that users have the appropriate access. Personnel who no longer require access are removed from access privileges. In the event an employee is separated from employment, Service Provider and its Commercial Provider will remove such employee from access privileges in advance of the employment separation where practicable.

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

DHS-HQ must comply with the Privacy Act and FISMA to ensure the privacy and security of the information collected and submitted to DHS-HQ. The Service Provider and its Commercial Provider must perform their duties in compliance with the FCRA and consistent with the Privacy Act and FISMA.

The Program is will limit dissemination of vendor employee PII only to those with a need to know, to minimize the risk of data misuse. The Service Provider will collect only PII needed to perform Program background screenings and to prepare the Program badge. The Service Provider will provide only biographic, and not biometric, information to its Commercial Provider to perform the background screenings. The Service Provider will authorize only a limited number of its personnel to receive password-protected access to the Commercial Provider's web portal to review the details of individual background screening reports. Neither the Service Provider nor its Commercial Provider will share with DHS-HQ or any vendor company the substance of any individual background screening report, or associate the reason for a "fail" to any identifiable individual. The only PII that the Service Provider will provide to DHS-HQ is the vendor employee's name, company and "pass" or "fail" background screening result and, if applicable, any search results reflecting the individual is the subject of an outstanding warrant or on the Terrorist Watch List . DHS-HQ will not have physical or logical access to the separate private databases of either the Service Provider or its Commercial Provider; these private entities will not have physical or logical access to DHS-HQ's System. In addition, the Service Provider will require vendor companies to agree that they will not use background screening results for employment purposes.

The System will be audited annually by the DHS IT Security Office and will include a real-time audit trail to:

1. Track access to electronic information and changes to data;

2. Monitor implementation and use of intrusion detection software and hardware;
3. Verify installation of data integrity monitoring software;
4. Provide real time monitoring of System audit logs; and
5. Ensure separation of data access based upon user roles and responsibilities.

The Service Provider will use published National Institute of Standards and Technology ("NIST") best practices regarding access logging for auditing consistent with these measures. Data that the Services Provider exports to its Commercial Provider is tracked in the Service Provider's database.

The Service Provider will employ the principle of least-privilege access and uses strong encryption on PII in its database as well as encrypting entire database backups so that data at rest also is protected. The dates of birth and social security numbers of individuals will be encrypted prior to being placed into the Service Provider's database and never will leave the business logic machine's memory. PII collected during registration will be encrypted for the Service Provider's data center's restricted access, before being placed on the hard drive or transmitted to the Data Center. PII will be programmatically and securely (via SSL or encryption) exported to the Service Provider's Commercial Provider.

The Service Provider will send its personnel to the physical premises of its Commercial Provider on a regular basis to conduct a comprehensive on-site audit, to ensure that the Commercial Provider is adhering to stringent privacy and security practices and procedures.

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

Privacy and data security training will be required of all personnel of DHS-HQ, the Service Provider and the Commercial Provider who are involved in collection, maintenance, use or storage of PII collected through the Program. Personnel will be updated on privacy and data security on at least an annual basis.

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

Information in DHS-HQ's System will be safeguarded in accordance with FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. The Department will follow DHS Management Directive (MD) 11042.1 Safeguarding Sensitive and Unclassified Information (FOUO), and DHS Policy for FOIA Compliance MD 0460.1. The Department will obtain any necessary Certification and Accreditation for this System.

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

Information on DHS-HQ'S System, and on the Service Provider's and its Commercial Provider's separate private databases, will be secured consistent with applicable Federal standards. Security controls will be in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need-to-know policy. Physical access to the System and private databases will be controlled with the use of identity badges. The System and the databases will be housed in controlled computer or Data Centers within secure facilities. In addition, administrative controls, such as periodic monitoring of logs and accounts, will help to prevent and/or discover unauthorized access. Audit logs will be maintained and monitored to track user access and unauthorized access attempts. In addition, DHS-HQ oversight may include unannounced and/or unscheduled inspections. In addition, DHS-HQ will require the Service Provider to meet stringent criteria for maintaining the privacy and security of all Program-related data in its and its Commercial Provider's databases, which are based on the NIST standards 800-53 Federal Information Processing Standards (FIPS) 199. By requiring the Service Provider to meet these criteria, DHS-HQ minimizes any attendant privacy risks associated with the handling of Program-related PII by the non-Federal entities that are not subject to Federal IT security and privacy laws, regulations and policies.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The System primarily will be built from Commercial Off the Shelf (COTS) products. System components will include COTS hardware and operating systems.

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

The Program is designed to allow for collection of only those data elements necessary to allow DHS-HQ, and the Service Provider and its Commercial Provider, to perform their tasks. The Service Provider will collect only individual information needed to perform Program background screenings and to prepare the Program badge. The Service Provider will provide only biographic, and not biometric, information to perform the background screenings. The Service Provider will authorize only a limited number of its personnel to receive password-protected access to the Commercial Provider's website to review the details of individual background screening reports. Neither the Service Provider nor its Commercial Provider will share with DHS-HQ or any vendor company the substance of any individual background screening report, or associate the reason for a "fail" to any identifiable individual. The only PII that the Service Provider will provide to DHS-HQ is the vendor employee's name, company and "pass" or "fail" background screening result. DHS-HQ will not have physical or logical access to the separate private databases of either the Service Provider or its Commercial Provider; these private entities will not have physical or logical access to DHS-HQ's System.

In addition, the Program is designed to provide for secure transmission of Program participant PII through encryption, SSL and other technology to minimize the risk of data loss or interception.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, DHS-HQ has designed an information technology infrastructure that will protect against inadvertent use of PII collected from vendor employees who choose to participate in the Program. Access to PII will be strictly controlled; only personnel who have a need to know and who have undergone privacy and data security training will have access to the PII. DHS-HQ will not transmit or otherwise share this information with entities outside of DHS that are not described in the routine uses in the applicable SORN, or with other agencies as may be required pursuant to the Privacy Act. Additionally, the System will include a real time audit function to track access to electronic information, and any infraction of security rules will be dealt with quickly and appropriately. Procedures and policies will be in place to ensure that no unauthorized access to System information occurs and that operational safeguards are firmly in place to prevent system abuses. The Service Provider and its Commercial Provider will follow similar measures to enhance privacy and data security.

The Program badge manufactured by the Service Provider is designed to contain minimal PII, and only enough to verify an employee's identity at the time of the badge process. The badge will display only the vendor employee's name, company and photograph, along with a barcode that is based upon a unique identifier which, when scanned using the Service Provider's equipment, can securely communicate to the Service Provider's Data Center and verify a biometric match.

Responsible Officials

Herbin L. Gray

DHSAccessGate Program Office of Security/DHS-HQ

Department of Homeland Security

(202) 282-9787

Approval Signature Page

Original signed and on file with the DHS Privacy Office

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

Appendix A

"Retained," as used in Table 1, is defined as storing and maintaining the specified data in the normal course of duty following an individual's registration in the Program.

Table 1

	PRIVATE SECTOR SYSTEMS BOUNDARY		**GOVERNMENT SYSTEMS BOUNDARY**	
	Program Badge (Individual)	***Service Provider***	***DHSAccessGate System***	***DHS-HQ***
Unique Identifier	Stored and retained.	Created, stored and retained.	Not collected, stored or retained.	Not retained. One-time scan for identity verification at badge issuance.
Biographic information	Name and company of individual displayed, and accessed through barcode scan.	Collect, store and retain name, employer, date of birth, social security number, and residence and billing address of individual.	Collect, store and retain only name and company of individual.	Collect, store and retain only name and company of individual.
Biometric images – photo	Displayed, and accessed through barcode scan.	Collected, stored and retained.	Not collected, stored or retained.	Not collected, stored or retained. One-time viewing for identity verification at badge issuance.
Biometric images - fingerprints	Not accessed, stored or retained.	Collected, stored and retained.	Not collected, stored or retained.	Not collected, stored or retained.
Biometric template – fingerprints	Access for "match" purposes available for secondary identity verification at badge issuance, through barcode scan.	Created, stored and retained.	Not collected, stored or retained.	Not collected, stored or retained. One-time scan for "match" for secondary identity verification at badge issuance.
Copy of ID documents	Not collected, stored or retained.	Not collected, stored or retained.	Scanned and verified.	Scanned and verified.
Security Threat Assessment Result ("Pass"	Access available at badge issuance, through barcode	Collected, stored and retained.	Collected, stored and retained.	Collected, stored and retained.

or "Fail")	scan.			
Security Threat Assessment History	Not accessed, stored or retained.	Collected, stored and retained through commercial provider. Password access by Service Provider.	Not collected, stored or retained.	Not collected, stored or retained. However, private sector service provider will notify DHS-HQ if background screening shows individual is on the OFAC terrorist watch list, is the subject of an open warrant, or is a fugitive.
Billing Information	Not accessed, stored or retained.	Collected, stored and retained.	Not collected, stored or retained.	Not collected, stored or retained.

Appendix B – Individual User Agreement

USER AGREEMENT: INDIVIDUALS

Terms and Conditions for Registering, and Renewing

Registration, with the [CONTRACTOR] Program

Please carefully read the following terms and conditions of this Agreement. It affects your legal rights. We encourage you to download and retain for your records a hard copy of this Agreement at [CONTRACTOR WEBSITE ADDRESS].

[CONTRACTOR] enters into this Agreement with you on behalf of itself and on behalf of its related companies, subsidiaries and affiliates.

By selecting the program acceptance button below, you accept the following terms and conditions and you agree to be bound by them.

IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, SELECT "I do not accept the terms" BELOW AND "QUIT" THE [CONTRACTOR] REGISTRATION PROCESS.

1. [CONTRACTOR PROGRAM] overview

Welcome to [CONTRACTOR PROGRAM NAME]! [CONTRACT PROGRAM NAME] has been developed to enhance access security at participating military, DHS and other government facilities. It also is designed to improve on-site access for vendor companies and their employees, like you, who conduct official business on military, DHS, or other government facilities.

The registration process is simple. First, vendors request approval from a participating military, DHS or other government facility to join [CONTRACTOR PROGRAM NAME]. If approved, the vendor then registers with [CONTRACTOR PROGRAM NAME]. Next, the vendor provides [CONTRACTOR PROGRAM NAME] with a list of approved employees. The employees then stop by the [CONTRACTOR PROGRAM NAME] Registration Station at the facility, and register with [CONTRACTOR PROGRAM NAME].

[CONTRACTOR PROGRAM NAME] carefully screens all [CONTRACTOR PROGRAM NAME] participants. As part of the registration process, each [CONTRACTOR PROGRAM NAME] employee registrant must pass a confidential [CONTRACTOR PROGRAM NAME] background screening. That badge is used as part of an integrated solution that lets the participating facility know that the employee meets the [CONTRACTOR PROGRAM NAME] criteria to participate in the [CONTRACTOR PROGRAM NAME.]

The employee's [CONTRACTOR PROGRAM NAME] registration is valid for one year. At all times during that year the employee must continue to meet [CONTRACTOR PROGRAM NAME] background screening standards and in all other respects must remain eligible to participate in [CONTRACTOR PROGRAM NAME]. Periodic background screenings are conducted on a regular basis, to verify continued eligibility.

2. Confidential Background Screenings

[CONTRACTOR PROGRAM NAME] takes seriously its commitment to security. That is why [CONTRACTOR PROGRAM NAME] restricts its program to companies and their employees who, at all times, meet [CONTRACTOR PROGRAM NAME]'s background screening standards.

As a [CONTRACTOR PROGRAM NAME] participant, you will undergo, and must pass, background screenings on an ongoing basis to verify your eligibility to participate in [CONTRACTOR PROGRAM NAME]. Background screenings will be conducted on you under circumstances that include but are not limited to the following:

- When you first register with [CONTRACTOR PROGRAM NAME]

- Periodically throughout the term of your [CONTRACTOR PROGRAM NAME] registration, as often as every 30 days

- When your employer, or you, renew your registration with [CONTRACTOR PROGRAM NAME]

- At any time upon request by the military, DHS or other government facility at which you are a [CONTRACTOR PROGRAM NAME] participant

- At any time, in [CONTRACTOR PROGRAM NAME]'s sole discretion, to verify that you meet the standards of [CONTRACTOR PROGRAM NAME]'s background screening standards

[CONTRACTOR PROGRAM NAME] contracts with one or more background screening providers to conduct [CONTRACTOR PROGRAM NAME] background screenings. In compliance with the Fair Credit and Reporting Act (the "FCRA") and other applicable laws, this is to inform you that, by giving your approval below and by entering your personally identifiable data, you hereby consent and authorize [CONTRACTOR PROGRAM NAME] and/or its third-party background screening provider(s) to perform background screenings of you in order to verify your eligibility to participate in [CONTRACTOR PROGRAM NAME]. The data obtained through the background screenings may include any or all of the following:

Individual Information:

- Name
- Social Security Number (providing the social security number is voluntary, but failure to do so may prevent completion of the registration, performance of the background screening and activation of the Program badge)
- Company-issued Employee Identification Number
- Individual photo
- Date of birth
- Fingerprints
- Address
- Phone number
- Social Security Number verification
- Felony and misdemeanor convictions
- Outstanding warrants
- Sexual offender convictions
- Terrorist or OFAC watch lists

Public records may be used in the background screening reports, such as civil and/or criminal records. You have the right to dispute the information on the report and request additional disclosures provided under section 606(b) of the FCRA, and a written summary of your rights pursuant to section 609(c) of the FCRA.

If any of your background screenings produces a "fail" result, [CONTRACTOR PROGRAM NAME] and/or its third-party background screening providers will so notify you. [CONTRACTOR PROGRAM NAME] also may notify your employer and possibly also the participating facility of your "fail" result. In the event of a "fail" result, you, and only you, will be provided with a copy of your background screening report and will be afforded an opportunity to dispute the information in it. If you do not timely dispute the background screening results or, if you do so but are

unsuccessful in changing the results, you will not qualify to participate in [CONTRACTOR PROGRAM NAME]. Your employer, and also the participating facility, will be so notified.

[CONTRACTOR PROGRAM NAME] and/or its third-party background screening providers will NOT provide your employer with a copy of the background screening reports or disclose to your employer the contents of the background screening reports. However, [CONTRACTOR PROGRAM NAME] and/or its third-party background screening providers WILL notify your employer as to whether you "pass" or "fail" the background screenings. Upon request, [CONTRACTOR PROGRAM NAME] also may provide the United States military, DHS and/or other United States government agency with your name and/or other identifying information, if they have a need for such information in the performance of their official duties.

You further hereby authorize [CONTRACTOR PROGRAM NAME] and its third-party background screening provider(s) to retain your data, and any updates to that data, for a commercially reasonable period of time. [CONTRACTOR PROGRAM NAME] and its third-party background screening providers are committed to maintaining this data in the strictest of confidence, and follow stringent fair information practices in accordance with the FCRA and other applicable laws and regulations.

3. Registering with [CONTRACTOR PROGRAM NAME]

To complete your registration with [CONTRACTOR PROGRAM NAME], you first must pass a confidential [CONTRACTOR PROGRAM NAME] background screening. See Section 2, above.

If you pass the [CONTRACTOR PROGRAM NAME] background screening, [CONTRACTOR PROGRAM NAME] will issue you a badge that displays your name, company and photo. Your [CONTRACTOR PROGRAM NAME] registration will be valid for one year, provided that you pass all [CONTRACTOR PROGRAM NAME] background screenings conducted during the term of your [CONTRACTOR PROGRAM NAME] registration, and provided that you remain in all other respects eligible to participate in [CONTRACTOR PROGRAM NAME].

4. Rights and obligations while registered with [CONTRACTOR PROGRAM NAME]

As a [CONTRACTOR PROGRAM NAME] participant, you are issued a [CONTRACTOR PROGRAM NAME] badge. The [CONTRACTOR PROGRAM NAME] badge is for your use only, for the term of your [CONTRACTOR PROGRAM NAME] registration. At all times you must take care of it. You may not share, lend or transfer your badge to anyone else. Please be careful to avoid scratching the badge or getting it wet. If your badge is lost or damaged, you must immediately notify your employer (or, if you are a sole proprietorship, you must immediately notify [CONTRACTOR PROGRAM NAME] at (XXX) XXX-XXXX). In addition, if you stop working for your current employer, or if you stop participating in [CONTRACTOR PROGRAM NAME], you must immediately return the [CONTRACTOR PROGRAM NAME] badge to your employer.

During the term of your [CONTRACTOR PROGRAM NAME] registration you will be subject to periodic background screenings, as often as deemed required by [CONTRACTOR PROGRAM NAME] and at its sole discretion. This is done to verify that at all times you continue to meet the background screening standards of [CONTRACTOR PROGRAM NAME]. See section 2, above.

5. Renewing your [CONTRACTOR PROGRAM NAME] registration

At the end of the first year with [CONTRACTOR PROGRAM NAME], your employer, if approved by the facility to continue participation in the [CONTRACTOR PROGRAM NAME] Program, may renew the company registration for another year by paying the annual renewal fee. If your employer completes the company renewal, your employer may renew your [CONTRACTOR PROGRAM NAME] registration. Your renewal is contingent upon your passing a confidential [CONTRACTOR PROGRAM NAME] background screening and in all other respects meeting the [CONTRACTOR PROGRAM NAME] eligibility criteria. See Section 2, above.

[CONTRACTOR PROGRAM NAME] processes employee renewals at the request of the vendor companies. If you do not want your company to renew your [CONTRACTOR PROGRAM NAME] registration for another year,

please notify your company's [CONTRACTOR PROGRAM NAME] vendor Administrator at least 45 days before the one-year anniversary of your current registration.

6. Grounds for revoking your [CONTRACTOR PROGRAM NAME] registration

Your [CONTRACTOR PROGRAM NAME] registration is valid for one year, provided that you remain [CONTRACTOR PROGRAM NAME]-eligible for that entire year. If, during the year, you become ineligible to remain a participant in [CONTRACTOR PROGRAM NAME], your [CONTRACTOR PROGRAM NAME] registration will be revoked and you must return your [CONTRACTOR PROGRAM NAME] badge to your employer. Grounds for becoming ineligible, and having your [CONTRACTOR PROGRAM NAME] registration revoked, include but are not limited to:

- You no longer work for the company through which you registered with [CONTRACTOR PROGRAM NAME]

- You do not pass a [CONTRACTOR PROGRAM NAME] background screening

- Your work functions no longer include visiting the participating facility

- Your employer requests to remove you from the [CONTRACTOR PROGRAM NAME] program

- Your company no longer is eligible, or ends its participation in, [CONTRACTOR PROGRAM NAME]

- The facility for which you have a [CONTRACTOR PROGRAM NAME] badge no longer participates in [CONTRACTOR PROGRAM NAME]

- The facility removes you from [CONTRACTOR PROGRAM NAME]

- The facility removes your company from [CONTRACTOR PROGRAM NAME]

- You violate any term or condition of this Agreement

7. General restrictions, limitations and resolution of disputes

- This registration does not by itself confer eligibility on you to participate in [CONTRACTOR PROGRAM NAME]. Your participation is subject to the terms and conditions set forth in this Agreement as well as to the approval of the participating facility and your employer.

- This registration does not guarantee you access to any military, DHS or other government facility. The facility maintains the right to deny you entrance and to take any security precautions it deems necessary, including but not limited to randomly inspecting your vehicle and its contents.

- A participating facility may revoke your company's, and/or your, access privileges under [CONTRACTOR PROGRAM NAME] at any time for any reason. You agree that, in such event, you have no financial, legal or other remedies against [CONTRACTOR PROGRAM NAME] or any agency of the United States Government.

- [CONTRACTOR PROGRAM NAME] prohibits employers from using [CONTRACTOR PROGRAM NAME] as a pre-employment screening service or as a basis for adverse employment action. You agree that you have no remedy, in equity or law, and will initiate no legal action, against [CONTRACTOR PROGRAM NAME] or any of its related companies, officers, directors, employees, agents, subsidiaries or affiliates, or against any agency of the United States government, for any adverse pre-employment or employment action taken against you arising in any way from your registration with, or participation in, [CONTRACTOR PROGRAM NAME].

- [CONTRACTOR PROGRAM NAME] takes pride in its background screening service but cannot guarantee the accuracy of the data obtained. As explained in Section 2, above, you have the right to dispute a "fail" result of a [CONTRACTOR PROGRAM NAME] background screening. You agree that you have no remedy, in equity or law, and will initiate no legal action, against [CONTRACTOR PROGRAM NAME] or any of its related companies, officers, directors, employees, agents, subsidiaries or affiliates, or against any agency of the United States government, arising

from any dispute over the accuracy or completeness of data derived from a [CONTRACTOR PROGRAM NAME] background screening, or arising from your not passing a [CONTRACTOR PROGRAM NAME] background screening.

- [CONTRACTOR PROGRAM NAME] contracts with one or more third parties to conduct [CONTRACTOR PROGRAM NAME] background screenings. Such third party(ies) conform to the highest standards of care with respect to protection of personally identifiable data. [CONTRACTOR PROGRAM NAME] stores on its own servers only limited personally identifiable information on [CONTRACTOR PROGRAM NAME] participants. [CONTRACTOR PROGRAM NAME] does not store on its servers, and maintains no database containing, the contents of background screenings conducted on [CONTRACTOR PROGRAM NAME] participants. Such data is stored with [CONTRACTOR PROGRAM NAME]'s third-party background screening provider(s). You agree that any rights you may have against [CONTRACTOR PROGRAM NAME] arising from storage of your personally identifiable data, is limited to data stored by [CONTRACTOR PROGRAM NAME] on its own servers or contained in [CONTRACTOR PROGRAM NAME]'s own database. You agree that you have no remedy, in equity or law, and will initiate no legal action, against [CONTRACTOR PROGRAM NAME] or any of its related companies, officers, directors, employees, agents, subsidiaries or affiliates, arising from the storage of any personally identifiable data on you that is not maintained on [CONTRACTOR PROGRAM NAME]'s own servers or contained in [CONTRACTOR PROGRAM NAME]'s own database.

- You agree that, if you have a dispute with [CONTRACTOR PROGRAM NAME], you will so notify [CONTRACTOR PROGRAM NAME] in writing within six months of the event or the action giving rise to the dispute. You agree to make every effort to resolve the dispute informally. You further agree that, in the event of a breach of this Agreement by [CONTRACTOR PROGRAM NAME], your sole and exclusive remedy will be an amount equal to your registration fee for the year in which the breach occurred.

- This Agreement is governed by the laws of the State of Oregon, notwithstanding conflicts of laws principles. You agree that any legal action brought under this Agreement must be brought in Washington County, Oregon. The prevailing party shall be entitled to recover its/his/her legal costs and attorney's fees.

- If any provision of this Agreement is found by a proper legal authority to be unenforceable, that provision shall be severed and the remainder of this Agreement shall continue in full force and effect.

This Agreement constitutes the entire agreement between you and [CONTRACTOR PROGRAM NAME] with respect to the [CONTRACTOR PROGRAM NAME] program. This Agreement supersedes any proposal or any prior or contemporaneous writings or other agreements, oral or written, and any other communications or representations relating to the [CONTRACTOR PROGRAM NAME] program.

If you have any questions regarding your company's participation in [CONTRACTOR PROGRAM NAME], please refer your questions to your company's [CONTRACTOR PROGRAM NAME] vendor Administrator.