Privacy Impact Assessment
for the

Background Check Service

November 22, 2006

Contact Point
Elizabeth Gaffin
USCIS Privacy Officer
United States Citizenship and Immigration Services
202-272-1400

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The United States Citizenship and Immigration Services (USCIS) is developing the Background Check Service (BCS) to help streamline the established USCIS background check process. As part of the adjudication process, USCIS conducts three different background checks on applicants/petitioners applying for USCIS benefits. These include (1) a Federal Bureau of Investigation (FBI) Fingerprint Check, (2) a FBI Name Check and (3) a Customs and Border Protection (CBP) Treasury Enforcement Communication System/Interagency Border Inspection System (TECS/IBIS) Name Check. Prior to BCS, information relating to the FBI Fingerprint Checks and the FBI Name Checks was stored in two different systems. Information relating to the TECS/IBIS Name Checks was not stored in any system. BCS will be the central repository for all activity related to these background checks.

Introduction

The Office of Field Operations of the USCIS owns the Background Check Service (BCS).

As part of the adjudication process, when an applicant/petitioner applies for a USCIS benefit, a background check is conducted on that individual. To facilitate the process and improve efficiency, USCIS developed BCS as a centralized repository that contains the consolidated data on all background check requests and results. BCS allows authorized USCIS users to request background checks and access the data stored in BCS during the adjudication process in order to make an informed decision.

The FBI Fingerprint Check is a search of the FBI's Criminal Master File, Integrated Automated Fingerprint Identification System (IAFIS). This search will identify applicants/petitioners who have an arrest record. The FBI Name Check is a search of the FBI's Universal Index which consists of administrative, applicant, criminal, personnel, and other files compiled for law enforcement purposes. The TECS/IBIS Name Check is a search of a multi-agency database containing information from 26 different agencies. The information in TECS/IBIS includes records of known and suspected terrorist, sex offenders, people who are considered public safety risks and other people that may be of interest to the law enforcement community. TECS/IBIS will also be used to access National Crime Information Center (NCIC) records on wanted persons, criminal histories, and previous federal inspections.

BCS will not collect information directly from the applicant/petitioner. BCS will be the source of all background check activity related to USCIS operations.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

The information collected in BCS includes biographic data provided on the specific application/petition submitted by USCIS applicants/petitioners. This includes: Alien File Number (A-Number); First and Last Name; Date of Birth; Country of Birth; Gender; Nationality; Aliases; parental history; marital status and history; current and previous residences; employment history; and other biographic data associated with applicants/petitioners.

The information in BCS also includes the results of the FBI Fingerprint Check, FBI Name Check and TECS/IBIS Name Check. Specifically, the FBI Fingerprints Check result contains the criminal arrest record (RAP sheet) of the applicant/petitioner if one exists. If one does not exist, the FBI will provide us a response indicating that there was not a match on the 10 prints submitted. The FBI Name Check result contains the information relating to the file the FBI has on the applicant/petitioner if one exists. If there is no match, the FBI will provide us a response indicating that there was not a match on the name submitted. The TECS/IBIS Name Check result contains the information relating to the file in TECS/IBIS if one exists. If there is no TECS/IBIS match, a response will be provided indicating that there was not a match on the name submitted.

1.2 From whom is information collected?

The information in BCS relating to the FBI Fingerprint Check, the FBI Name Check and the TECS/IBIS Name Check is collected from the applicants/petitioners of UCSIS benefits. The information used for the FBI Name Check and the TECS/IBIS Name Check is taken from the application/petition submitted to USCIS by the applicant/petitioner or an authorized representative. The information from these applications/petitions is entered into one of USCIS' case management systems. These USCIS case management systems include the:

- Computer-Linked Application Information Management System (CLAIMS) 3, which is used to process applications including, but not limited to, an Adjustment of Status (Green Card) and Temporary Protective Status (TPS);
- CLAIMS 4, which is used to process applications for Naturalization;
- Refugee Asylum Parole System (RAPS), which is used to process Asylum applications; and
- Marriage Fraud Assurance System (MFAS), which is used for processing information relating to investigations of marriage fraud.

Note that BCS has no direct interaction with the benefit applicant/petitioner.

For the purposes of this document, these USCIS case management systems are hereby referred to as "Requesting Systems."

These Requesting Systems will send information to BCS, which will be used to generate a Name Check Request. The Name Check Results are collected from the FBI Name Check and TECS/IBIS Name Check. Both the requests and results will be stored in BCS.

The information relating to the FBI Fingerprint Check is collected from the applicant at the time the fingerprints are taken. Fingerprints are taken electronically at one of USCIS' Application Support Centers (ASC) or taken from hard copy fingerprint cards (FD-258) that are submitted for those applicants who are unable to go to an ASC. Again, this information will be collected as part of the application process associated with one of the requesting systems.

The responses to the FBI Fingerprint Check are collected electronically from the FBI and stored in BCS.

For the purposes of this document, FBI Fingerprint Check, FBI Name Check and TECS/IBIS Name Check are hereby referred to as "Background Information Source Systems."

1.3 Why is the information being collected?

The collection of information is required to verify the applicant/petitioner's eligibility for the benefit being sought. The eligibility requirements include conducting background checks. The applicant/petitioner could not seek the benefits provided by USCIS without the information collected from the applications/petitions.

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

The legal authority to collect this information comes from 8 U.S.C Section 1101 et seq.

In addition, the U.S. Office of Management and Budget (OMB) approves the format of every public form available from USCIS and authorizes USCIS to collect the requested information on the forms. Lastly, USCIS has signed Memoranda of Understanding (MOU) with CBP and the FBI that set forth the terms and conditions for the transfer and use of information pertaining to background checks and associated with the interaction with the Background Information Source Systems.

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

While the collection of information presents inherent privacy risks including the possible misuse

and inappropriate dissemination of data, USCIS implemented measures to mitigate these risks in the design of BCS by consolidating independent systems into one centralized system, which allows for more controlled security and more efficient system management.

USCIS developed and implemented BCS in accordance with DHS-approved security guidelines. Only users who need the information to effectively perform their job functions can gain access to BCS. These authorized users must go through an approval process and can only access BCS through DHS-approved equipment. Lastly, all USCIS adjudicators who will be using BCS during the adjudication process have received the Federal Law Enforcement Training Center (FLETC) Legal Division's Freedom of Information Act/Privacy Act (FOIA/PA) training.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

The biographical information will be used to create and submit Name Check Requests and to match the results of background checks to a particular applicant/petitioner.

The results of background checks will be used for adjudication purposes to determine an applicant's/petitioner's eligibility for a USCIS benefit. If the background check result from the FBI or TECS/IBIS yields an item of law enforcement or national security interest, USCIS may work with CBP, the FBI, or other law enforcement entities, such as Immigration and Customs Enforcement (ICE), to determine if law enforcement actions should be pursued. Additionally, the information in BCS may be used for future law enforcement action. If the applicant/petitioner becomes the subject of a national security or law enforcement investigation, the information in BCS could be provided in the interest of public safety.

In addition, the request and result data stored in BCS may be used by management to create reports that provide an accurate profile of the background check process from several different perspectives. With this uniformly presented information, USCIS will be able to actively and effectively manage these processes, identify issues before they become problems, and strategically plan and implement new measures to support USCIS' broader mission.

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

No. BCS will not be used for data mining.

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

The information from the Requesting Systems will be entered directly into BCS via an electronic interface. The data will be checked for accuracy and proper formatting during the electronic exchange. Background check requests will be sent to the Background Information Source Systems from BCS with a unique system generated Correlation Identifier that will be used to match results with the proper request and applicant/petitioner record. Furthermore, integrity checks will be conducted to ensure that the system is matching the correct data. These checks will match the A-Numbers, Receipt Numbers[1], First and Last Names, Dates of Birth, and other biographical information.

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.

Background check request and result records will be attributed to the correct applicant/petitioner file by matching fields such as A-Number, Receipt Number and Correlation ID. Integrity checks will be conducted at all points of data transfer and matching. Further, all information will reside on a secured network and server, with access limited to authorized personnel only. Lastly, audit logs will be kept in order to track and identify unauthorized uses of system information. Information, including the user's name, date and time of every transaction will be stored in a log. If misuse of data is suspected, these logs can be used to review and analyze all activity in BCS. The misuse of data could be suspected by reporting from employee and/or system monitoring, All BCS users will be notified that BCS stores these logs and USCIS management can use these to review any and all activity in BCS.

Section 3.0 Retention

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

USCIS has submitted a SF-115 form for the BCS system and is awaiting NARA approval. BCS will store data for 75 years from the date of the last action. At some point during the 75 years, the records may be archived.

[1] A Receipt Number is a unique number generated once a benefit application is accepted into a Requesting System.

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

BCS has submitted a SF-115 form and is awaiting NARA approval.

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

The information is needed for the indicated time period because the relationship between an applicant/petitioner and USCIS may span the 75 years that the data is retained. USCIS will use the historical data in BCS in the adjudication of applications/petitions in the future. BCS adopted the retention schedule of 75 years from the official disposition guidelines for a USCIS "A" file. The A file is the physical paper file containing all correspondence and documentation, including all applications, petitions, reports, interview notes and other written communications for every applicant/petitioner.

The ability to forge identities is a growing concern and keeping this biographic data on record for lengthy periods of time can help protect against fraudulent benefit applications. USCIS has implemented several measures to combat identity fraud and storing all background check data in BCS for future use supports this initiative.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

BCS shares information internally with CBP through the TECS/IBIS interface for name check purposes. If a TECS/IBIS Name Check Result contains items of law enforcement interest, USCIS may provide the information to other law enforcement entities such as ICE/CBP to determine if further law enforcement activities should be pursued.

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

TECS/IBIS Name Check Requests and Results are shared between USCIS and CBP via the BCS TECS/IBIS interface. The information is shared in order to perform a TECS/IBIS Name Check. BCS will send TECS/IBIS a Name Check Request that includes the applicant/petitioner's biographical information including First and Last Name, Date of Birth, Gender and unique subject ID (for example, an A-Number or Correlation ID). CBP will use this information to conduct a background check against the TECS/IBIS system, and will send the results back to BCS.

The results will indicate if there was a match on any record in the database. USCIS may use this response data to determine if the information relates to Law Enforcement, National Security, Public Safety, Fraud or other areas of interest. USCIS may elect to share information with ICE by means of a "Referral for Investigation," an internal USCIS document that is used to initiate a fraud investigation. Along with this "Referral for Investigation" USCIS sends the Alien File, which contains all pertinent biographic information including A-Number, Name, Date of Birth, addresses and information relating to the background checks. USCIS may also elect to share the Alien File with other government or law enforcement agencies if the information relates to Law Enforcement, National Security, Public Safety, Fraud or other areas of interest. These agencies include but are not limited to local and federal law enforcement.

4.3 How is the information transmitted or disclosed?

TECS/IBIS Name Check requests and results are sent electronically between BCS and TECS/IBIS using the Extensible Markup Language[2] (XML) format through a secure and reliable electronic interface. The results are received and stored in BCS for access by adjudicators via the web-based BCS User Interface.

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

Internal sharing of data is conducted over secured networks controlled by DHS utilizing DHS approved computers, services, and software. The privacy risks associated with each step of internal sharing, including system and network security, data usage, data transmission and disclosure have been identified and mitigated through adherence to DHS policies and procedures such as System Design Life Cycle documentation and Certification and Accreditation documentation. In addition, only authorized users who need the information contained in BCS have access to the system.

Given the technical security aspects above, there will always be the possibility of misuse and inappropriate dissemination of information. To help mitigate these risks, security logs, audit logs of user activity, and strict access controls will be enforced. Users will be given access to the system only after an account request form has been authorized by the user's superior and the Password Issuance Control System (PICS) officer.

[2] XML is a widely used, industry standard language that facilitates the sharing of data across different systems.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

BCS shares information externally with the FBI for FBI Name Check and FBI Fingerprint Check purposes.

5.2 What information is shared and for what purpose?

FBI Name Check requests and results are shared between USCIS' BCS and the FBI National Name Check Program. BCS will send the FBI a Name Check Request that includes the applicant's/petitioner's biographical information. The FBI will use this information to conduct a background check against their system, and will send the results (FBI Name Check Response) back to BCS. The results will be separated into three categories: 1) No Record, 2) Pending, and 3) Error. A Pending response indicates that the FBI has to conduct further investigation to determine if they have information relating to the name submitted. Pending responses will be updated as the cases are closed. These updates come in the form of a weekly update file sent from the FBI to USCIS.

USCIS uses the FBI Name Check Response during the adjudication process to determine an applicant's/petitioner's eligibility for an immigration benefit. When a Pending case is closed, a hard copy of the FBI Name Check Report will be delivered to a USCIS Fraud official. These FBI Name Check Reports are sent to USCIS once a week, by a bonded delivery service. The FBI Name Check Report may be used for law enforcement activities.

BCS electronically receives and stores FBI Fingerprint Check requests and responses. If the FBI Fingerprint Check yields a match, the FBI will return a copy of the FBI Identification Record (commonly referred to as a Rap Sheet. The Rap Sheet information will be stored in BCS. USCIS uses the Rap Sheet during the adjudication process to determine an applicant/petitioner's eligibility for an immigration benefit. In addition, the information in the Rap Sheet could be used to trigger further investigation or law enforcement actions because new information about the location of an individual is available based on the application/petition.

5.3 How is the information transmitted or disclosed?

FBI Name Check requests, results, and weekly updates are transmitted via an encrypted e-mail communication channel between USCIS and the FBI. The FBI Name Check request, result, and weekly update files will be encrypted in accordance with NIST's Advanced Encryption Standard. This method of transfer was developed in accordance with OMB Memos M-06-15 "Safeguarding Personally Identifiable Information" and M-06-16 "Protection of Sensitive Agency Information," as well as DHS Management Directive Number 11042.1 "Safeguarding Sensitive But Unclassified (For Official Use Only) Information." If the FBI Name Check search yields a match, a hard copy

of the FBI Name Check Report will be delivered to a USCIS Fraud official by an FBI employee with a Top Secret clearance. These reports are sent from the FBI to USCIS weekly.

FBI Fingerprint Check requests and results are electronically transmitted through the Benefit Biometric Support System (BBSS), USCIS' electronic interface to the FBI's fingerprint system known as the Integrated Automated Fingerprint Identification System (IAFIS). The fingerprint data is encrypted during this transmission and is transmitted over a secure network.

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?

Yes. USCIS has existing MOUs with the FBI. The terms and conditions for the exchange of data for Name and Fingerprint Check purposes are provided for in the MOUs between USCIS and the FBI and limit the use and re-dissemination of the information. The FBI does not share any information provided by USCIS in order to conduct either a Name Check or Fingerprint Check.

5.5 How is the shared information secured by the recipient?

The recipient of the shared information is the FBI. The information provided to the FBI by USCIS is restricted to FBI employees with Top Secret Clearances who work in secure buildings.

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

The only external agency receiving BCS information is the FBI. This information is used solely to enable the FBI to perform Name and Fingerprint Checks. The transfer of the data is pursuant to the MOUs entered into between USCIS and the FBI. FBI employees who perform Name and Fingerprint Checks have received the required training to perform the checks.

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

For the purpose of conducting an FBI Fingerprint Check, data is shared over DHS and FBI secured networks. FBI employees are trained and authorized to deal with biographic and biometric data. In addition, the FBI has policies and procedures in place to ensure that information is not inappropriately disseminated.

Given the technical security considerations, there is a possibility of misuse and inappropriate dissemination, but these risks are mitigated by taking advantage of the DHS Security

specifications that require audit logs of user activity, security logs and strict access controls.

Sharing data for the purpose of conducting FBI Name Checks presents a privacy risk. The use of e-mail to deliver the FBI Name Check request, result and weekly update files does present a privacy risk. The privacy risks include misuse of data, theft of data, and/or compromise of data integrity. The identified risks have been mitigated by designing the transmission system in accordance with DHS, OMB, and NIST guidelines for securing Sensitive But Unclassified (SBU) For Official Use Only (FOUO) data. These guidelines provide a baseline to data security and integrity, which have been followed and surpassed with the addition of NIST approved data encryption.

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?

A Systems of Records Notice (SORN) and Privacy Impact Assessment (PIA) will be published for BCS. Applicants/petitioners will be notified by a Privacy Act Notice and a signature release authorization on the benefit form. One of the most widely used forms is the N-400 Application for Naturalization. A copy of the form's Privacy Act Notice and signature release authorization has been attached as an appendix.

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

Applicants/petitioners who apply for USCIS benefits are presented with a Privacy Act Notice and a signature release authorization on the benefit application/petition. The Privacy Act Notice details the authority and uses of information the applicant/petitioner will provide on the USCIS benefit application/petition. The form also contains a signature certification and authorization to release any information from an applicant/petitioner record that USCIS needs to determine eligibility. It is within the rights of the applicant/petitioner to decline to provide the required information; however, it will result in the denial of the applicant's/petitioner's benefit request.

USCIS benefit applications/petitions require certain biographic information be provided and may also require submission of fingerprints and photographs. This information is critical in making an informed adjudication decision in granting or denying a USCIS benefit. The failure to submit such information would prohibit USCIS from processing and properly adjudicating the application/petition and thus preclude the applicant/petitioner from receiving the benefit.

Therefore, through the application process, individuals have consented to the use of the information for adjudication purposes, including background investigations.

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?

A Privacy Act Notice detailing authority and uses of information is presented to the applicant/petitioner. The form also contains a signature certification and authorization to release any information from an applicant/petitioner record that USCIS needs to determine eligibility, which includes biometric and biographic information.

All USCIS application and petition forms include a Privacy Act Notice and a signature release authorizing "…the release of any information from my records that USCIS needs to determine eligibility for the benefit…"

Consent is given for any use to determine eligibility, when the applicant/petitioner signs the application/petition.

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

The collection of personally identifiable information is a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. The privacy risk associated with this particular collection of information is that the individual may not be fully aware that their information will be used to conduct a background investigation. In order to mitigate this risk, USCIS has provided a Privacy Act Notice on benefit application/petition forms. The form also contains a signature certification and authorization to release any information provided by an applicant/petitioner. To further mitigate this risk, USCIS is issuing this PIA and the associated SORN.

Section 7.0
Individual Access, Redress and Correction

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

The biographic and personally identifiable information contained in BCS is received from the Requesting and Background Information Source Systems as discussed in Section 1.2. BCS does not directly collect information from applicants/petitioners. Therefore, the proper way to gain access to individual information is through these Requesting and Background Information

Source Systems. BCS has no means of direct communication with an applicant/petitioner; all data in BCS is obtained from previously entered data that comprises an individual's USCIS record. For an individual to gain access to their USCIS record they can file a Freedom of Information Act (FOIA) request. USCIS has the final discretion on withholding or releasing information. BCS may contain law enforcement sensitive information, which could possibly compromise ongoing criminal investigations if released to the individual.

If an individual would like to file a FOIA request to view their USCIS record the request can be mailed to the following address:

Freedom of Information Act/Privacy Act Program
U.S. Citizenship and Immigration Services
111 Massachusetts Avenue, N.W., 2nd Floor
ULLICO Building
Washington, D.C. 20529

Further information for FOIA requests for USCIS records can also be found at http://www.uscis.gov.

7.2 What are the procedures for correcting erroneous information?

All data in BCS is obtained from previously entered data in the Requesting Systems and Background Information Source Systems. If an individual would like to correct known erroneous information in their USCIS record, the individual can file a USCIS form directed at changing the specific erroneous information. For example, an applicant/petitioner can change their address by filing a Change of Address form (AR-11). After this form is processed the changes will reach BCS through one of the Requesting Systems (see Section 1.2) and all relevant fields will be updated in BCS. If an applicant/petitioner believes their file is incorrect but does not know which information is erroneous, the applicant/petitioner may file a FOIA request as detailed in Section 7.1.

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

Individuals are notified of the procedures for correcting their information on USCIS forms, the USCIS website and by USCIS personnel who interact with benefit applicants/petitioners.

7.4 If no redress is provided, are alternatives are available?

Normal USCIS procedure for redress is provided to applicants/petitioners as outlined in Sections 7.1 and 7.2.

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.

The data contained within BCS is obtained from both the Requesting and Background Information Source Systems (see Section 1.2), and as such, individuals must address all information access rights to these systems. Previously established procedures for changing biographical information may be followed to correct known erroneous information, for example filing an AR-11 form to change an applicant/petitioner's address. If the applicant/petitioner suspects erroneous information but does not know which part of the information is incorrect, the applicant/petitioner can file a FOIA request as detailed in section 7.1.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Access will be limited to authorized USCIS employees and contractors. Within that user group, BCS will offer four levels of access: System Administrator, Billing, Adjudicator, and 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.

Yes. Contractors are used to maintain systems and to provide technical support. All access to the BCS system follows the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

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

Yes. There will be four classes of users for BCS:

- Class 1 – Adjudicator – Users requiring Name Check submission and Query capabilities;
- Class 2 – Billing – Users requiring only Billing Reconciliation Function;
- Class 3 – Management – Users requiring all standard functions and ability to run Reports; and

- Class 4 – System Administrator – Users requiring system administrative privileges.

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

A standard request form (G-872B) must be completed by each user and authorized by a supervisor in that department and by the system owner's representative.

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

BCS will maintain activity logs including transactions by users. Reports can be run to verify that a user's activity is consistent with their permissions.

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

BCS contains audit trail records to resubmit, review, and examine the originally submitted Name Check request transactions. Since Name Check request data can be resubmitted based on an expired timeframe, audit trails will be needed to ensure that the Name Check request data is not duplicated. BCS will also maintain audit logs on all FBI Fingerprint transactions. All BCS transactions are subject to monitoring and review to ensure that the original requests or results data are not lost, manipulated, or compromised in any manner. Audit trails will also be kept for BCS user activity. Lastly, NIST approved data encryption will be used for data transportation between USCIS and the FBI to ensure that data has not been tampered with en route and to prevent unauthorized personnel from viewing the data.

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

Training on the BCS system will be provided to BCS users. This training will address appropriate privacy concerns. In addition, USCIS employees and contractors who have filled out a G-872B form (see Section 8.4) and have been granted appropriate access levels (see Section 8.3) by a superior, will be assigned a login and password from PICS used to access the system. These users will have previously undergone federally approved clearance investigations and signed appropriate documentation in order to obtain the appropriate access levels. In addition, every Federal employee and contractor is required to take annual computer security awareness training.

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

The BCS Team is currently engaged in the Certification and Accreditation process with the appropriate USCIS OCIO security staff. The system will have at least a temporary Authority to Operate[3] before it is made operational.

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

Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users will be broken into specific classes with specific access rights. Audit trails will be kept in order to track and identify unauthorized uses of system information. Data encryption will be employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, BCS complies with the DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack and unauthorized information dissemination.

Section 9.0 Technology

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

The system was designed with both commercial off-the-shelf products and custom designed software, databases, and user interfaces.

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

BCS developers followed the System Development Life Cycle 6.0 security guidelines in the design and development of BCS. All documentation has been reviewed and approved by USCIS Information Technology (IT) Security. Background check request and result records will be attributed to the correct applicant/petitioner file by matching on multiple data points including A-Number, Receipt Number, Last Name and Date of Birth. BCS data integrity checks were designed based on a detailed analysis of data sources (see Section 1.2) and specific data elements coming into BCS. In addition to these integrity controls the system was designed to acknowledge successful and failed data deliveries to ensure that data was never lost in transit. Further, for interaction with Background Information Source Systems, all requests will contain a

[3] A temporary Authority to Operate can last from 3 months to 6 months.

system generated Correlation ID that will be used to match the results with the proper request. The current method for sending FBI Name Check requests and receiving the results does present a security and privacy risk. BCS has been developed with industry standard interfaces that will allow for interface expansion. In the future, when the FBI develops an electronic system for submitting and receiving Name Check results, BCS will be able to easily interface with this secure system.

9.3 What design choices were made to enhance privacy?

BCS is only available to USCIS employees and contractors with appropriate security and access controls. The general public will not have access to the system. Protection and integrity of data, security and privacy are of paramount concern. The system follows all DHS Security guidelines for enhanced security, including the Certification and Accreditation security documents, Federal Information Processing Standards (FIPS) 199, Federal Information Security Management Act (FISMA), Trusted Agent-Federal Information Security Management Act (TA-FISMA), Office of Management and Budget (OMB) memoranda, and National Institute of Standards and Technology (NIST) security guidelines.

The system will provide more efficient management of the USCIS background check process by consolidating all of the actions to a single system. The ability to track data and user activities though audit logs on a consolidated system is far easier and provides better accountability than multiple systems can provide.

Conclusion

BCS was designed to facilitate the USCIS background check process. USCIS conducts background checks on applicants/petitioners during benefit adjudication. BCS provides centralized electronic routing, storage and processing of Name Check requests and results, as well as receiving request and result data for FBI Fingerprint Checks. The applicant/petitioner data used in creating Name Check requests is derived from Requesting Systems (See Section 1.2). BCS will store the basic biographic information needed to uniquely identify the applicants/petitioners, all Name Check request data, Name Check results data and FBI Fingerprint Check request and result data associated with that applicant/petitioner. During the transaction process, BCS does not alter or modify the biographic request or result data.
The ways in which BCS addresses privacy concerns include, but are not limited to:

- Granting access to pre-approved USCIS employees and contractors;
- Auditing transaction records to ensure that requested information and result data are not manipulated or compromised;
- Providing BCS users with training that addresses privacy concerns; and
- Drafting a PIA and SORN that states USCIS' intentions for the use of the private information data collected from USCIS applicants/petitioners. This will be shared with the public upon publication in the *Federal Register*.

BCS is a multi-phased project and is currently in its first phase. As future phases are developed, this PIA and associated SORN will be revised to address those updates.

Responsible Officials

Greg Collett, USCIS, Office of Field Operations

Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security