Privacy Impact Assessment (PIA): BioCheck

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: July 12, 2010

(b) Name of system: Biometric Check

(c) System acronym: BioCheck

(d) IT Asset Baseline (ITAB) number: 5044

(e) System description:

The BioCheck application is a client/server application used to capture biographic information such as the name and date of birth of visa petitioners. BioCheck also utilizes a Ten Print Live Scan (TPLS) component which captures fingerprint information from visa petitioners.

The information captured by BioCheck is replicated to the Consular Consolidated Database (CCD) from where it is sent via a web service to the United States Citizenship and Immigration Services (USCIS) for a background check. USCIS will forward the fingerprints to the FBI's Integrated Automated Fingerprint Information System (IAFIS). The FBI returns results to USCIS, which then converts the FBI response into one of three responses: (1) derogatory information exists (red light) response; (2) no derogatory information exists (green light) response; or (3) error response. USCIS sends the response back to the CCD via a web service and the response is replicated back to the BioCheck application.

A consular officer at post reviews the response returned for each visa petitioner. If the petitioner receives a green indicator, then the processing of the immigrant visa petition may continue. Petitioners receiving a red indicator must follow up with USCIS before the petition processing may proceed. If an error response is returned, the biometrics of the petitioner need to be collected again and resubmitted.

Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security re-certification
- ☐ PIA Information Review

(f) Explanation of modification (if applicable): N/A

(g) Date of previous PIA (if applicable): N/A

3. Characterization of the Information

The system:

☐ Does NOT contain PII. If this is the case, you must only complete Section 13.

☒ Does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

BioCheck collects the following PII from visa petitioners:

- First name, middle name and last name
- Fingerprints
- Facial Photograph
- Social Security Number
- Country of birth
- Date of birth

BioCheck also collects and maintains the IAFIS response retrieved from the CCD as described above.

b. How is the information collected?

Consular officers, locally employed staff, and eligible family members (consular users) use the BioCheck system to capture the fingerprints and a photograph depicting the face and head of the applicant . This is done using an electronic fingerprint scanner and a digital camera respectively. The personal information is collected directly from the American citizen visa petitioner using Form CIS I-130.

c. Why is the information collected and maintained?

The information is collected so a required background check can be performed on the individual as required by the Adam Walsh Child Protection and Safety Act. The passage of Section 402 of the Adam Walsh Child Protection and Safety Act amends section 204 of the Immigration and Naturalization Act (INA) to prohibit U.S. citizens and lawful permanent resident aliens who have been convicted of any “specified offense against a minor” from filing a family-based petition for immigrant status (Form I-130) on behalf of a beneficiary. As a result, the post cannot approve the petition until U.S. Citizenship and Immigration Services (USCIS) has conducted the required background check and confirmed that the petitioner is eligible to file the Form I-130.

d. How will the information be checked for accuracy?

American citizen visa petitioners must first provide proof of citizenship (usually in the form of a passport). The petitioner must then complete a petition for a family member, most likely a Form IR-1 or IH-3 or 4. Once this process is completed fingerprints are taken, and Biocheck processes these prints to provide a red light/green light response.

Accuracy of the information on an immigrant visa application is the responsibility of the applicant and BioCheck users including the Department of State employees/contractors/customer service reps/consular officers overseas.

In addition, quality checks are conducted against the submitted documentation at every stage and administrative policies minimize instances of inaccurate data. Consular users will review the initial documentation and identification forms in the hard file sent by National Visa Center (NVC) against the BioCheck data. Any new documentation or identification forms submitted by the applicant are also reviewed and verified against data in BioCheck. Any changes to biographical data thereafter will alert the users that new checks need to be performed. The final stage of review is the interview and final adjudication conducted by the Foreign Service Officer (FSO). The FSO will verify that all information is correct and factual before issuing the visa.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 22 U.S.C 2651(a) (Organization of Department of State)
- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Adam Walsh Child Protection and Safety Act, 18 U.S.C. 3509(m)
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)
- Child Status Protection Act (HR 1209) 2002

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

The personal data collected by BioCheck is the minimum necessary to carry out the function of BioCheck as identified in Section 3(c) above.

Once the information is sent to USCIS, none of the data can be accessed. Therefore, it cannot be viewed or modified. The only data that is displayed in BioCheck is the individual's name. This limits the privacy risks to:

- **Insider threat** – Employee misuse of data.
- **Theft during transmission** – the data may be compromised during electronic transmission.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation

In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the information assurance standards published by the National Institute of Standards and Technology (NIST), there are management, operational, and technical security controls implemented to protect the data. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), training, and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The individual's personal and biometric information is sent to USCIS for a background check to determine eligibility to petition for an immigrant visa by checking petitioner biometrics against USCIS and FBI databases. The FBI returns results to USCIS, which then converts the FBI response into one of three responses: (1) derogatory information exists (red light) response; (2) no derogatory information exists (green light) response; or (3) error response.

AMCIT BIOCHECK information is stored in separate tables in the CCD and is excluded from being viewed by our partners at other agencies because of Privacy Act considerations.

All the officers see is the red light/green light for Adam Walsh purposes.

Data can be retrieved in BioCheck by keyword searches such as applicant name, alien registration number, case number, and/or by barcode scanning.

Issuance and refusal information is shared with the Department of Homeland Security (DHS) including name, DOB, gender, and visa information such as issuance or refusal date and visa foil number.

b. What types of methods are used to analyze the data? What new information may be produced?

BioCheck generates a status report for management purposes. This report includes statistics only that are not traceable to any individuals. These reports are used solely for management purposes.

No new information is produced in BioCheck. Data mining is not used to analyze data.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

N/A

d. Is the system a contractor used and owned system?

BioCheck is a government-owned system. Government personnel are the primary users of BioCheck. Contractors are involved with the design and development of the system. All users are required to pass an annual cyber security awareness course/privacy training, and to sign non-disclosure and rules of behavior agreements.

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

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted.

Information system security officers (ISSOs) determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for BioCheck. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

All users, including external agencies' users, are screened prior to their employment with the Department or their respective agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before they are given access to the OpenNet and any CA/CST system, including IVO, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

Consular officers/users, system administrators, and database administrators are trained through security awareness training to safeguard PII from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided at post, domestic sites and external agencies for the proper disposal of paper containing PII.

5. Retention

a. How long is information retained?

Once a response is returned from USCIS, the individual's personal information and biometric data is deleted. The only information the system retains is the individual's name and the response from USCIS.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging.

Access to BioCheck is password-protected and under the direct supervision of the system manager. Once the information is sent to USCIS, none of the data can be accessed. Therefore, it cannot be viewed or modified. The only data that is displayed in the system is the individual's name. The use of BioCheck does not result in the creation of hard copy records.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The individual's personal and biometric information is shared with the Consular Consolidated Database (CCD). The CCD sends the data to USCIS and the FBI so a background check may be performed.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Information system security officers (ISSOs) determine the access level an application user (including managers) may require depending on the user's particular job function and level of clearance. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted.

An Interface Control Document (ICD) is used to define and disclose transmission formats via OpenNet. The Department of State systems that interface with BioCheck are strictly controlled by Firewall and NIDS rules sets that limit ingress and egress to BioCheck. All changes are requested from the Firewall Advisor Board (FAB) using a Universal Trouble Ticket (UTT). Each UTT is vetted by technical personnel and management prior to the change being implemented.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risk to privacy of sharing information contained in BioCheck with third parties is that the information provided will be used for unauthorized purposes, lost, stolen or misappropriated.

Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly

adhered to in order to ensure appropriate data transfers and storage methods are applied.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

BioCheck data is shared via data sharing arrangements. The individual's fingerprints, photo and personal data are sent to USCIS and FBI so a background check can be performed.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

BioCheck data is replicated from the database at each post to the CCD. The CCD forwards the information to the Department's datashare applications.

Each data sharing arrangement with Federal agency partners is covered by a written agreement in the form of a memorandum of understanding (MOU) or exchange of letters as well as technical documentation including an interface control document and interagency security agreement. Data is sent through encrypted lines.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risk to privacy of sharing information contained in BioCheck with third parties is that the information provided will be used for unauthorized purposes, lost, stolen or misappropriated.

BioCheck information is shared with U.S. government agencies with a statutory requirement and in accordance with confidentiality requirements under INA section 222(f). Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure any risk is addressed through the user-authorization process.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Visa Records: State-39.

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

The BioCheck information is collected as part of the process for filing the Form I-130 visa petition. Form I-130 contains the following Privacy Act notice:

We ask for the information on this form, and associated evidence, to determine if you have established eligibility for the immigration benefit for which you are filing. Our legal right to ask for this information is in 8 U.S.C. 1255. We may provide this information to other government agencies. Failure to provide this information, and any requested evidence, may delay a final decision or result in denial of your request.

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

Information is given voluntarily by the individual and with his or her consent. For example, individuals who petition for a beneficiary must supply all the requested information and may not decline to provide part or all the information required, if they wish visa services.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Individuals may decline to provide information, but they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

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

The Privacy Act notice is provided in writing in the instructions on the Form I-130 visa petition. In addition, the relevant SORN, State-39, provides notice to the individual of the use of his or her information.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals have no direct access to information in BioCheck. If any information was entered in error, the BioCheck user must submit a new background check with the new information. Once a background check is submitted, it cannot be modified.

BioCheck information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correction of their personally identifiable information (PII) pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act System of Records Notice (SORN), and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out

protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

To the extent information in BioCheck may be Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements.

Therefore this category of privacy risk is appropriately mitigated in BioCheck.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to BioCheck is limited to authorized Department of State users, including contractors, who have a justified need for the information in order to perform their official duties. To access the system, authorized users must be an authorized user of the Department of State' unclassified network. Access to BioCheck requires a unique user account assigned by a supervisor. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning a logon. Activity by authorized users is monitored, logged, and audited.

The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for the BioCheck application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

b. What privacy orientation or training for the system is provided authorized users?

All users must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

BioCheck does not employ any technology known to elevate privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since BioCheck does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum satisfactory in this application.

12. Security

a. What is the security certification and accreditation (C&A) status of the system?

Department of State operates BioCheck in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. Department of State is in the process of conducting a risk assessment as part of the full certification and accreditation (C&A) process for the BioCheck system to identify appropriate security controls to protect against risk and implemented controls. The Department will perform routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to function as intended in accordance with the Federal Information Security Management Act (FISMA) provision for the system's triennial recertification.