Diplomatic Security Federal Bureau of Investigations Connectivity (4516) – LiveScan Management System Software

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Name of system: Diplomatic Security Federal Bureau of Investigations Connectivity

(b) Bureau: DS/EX

(c) System acronym: DS FBIC

(d) iMatrix Asset ID Number: 4516

(e) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

DS FBIC is currently in the initial stages of the triennial re-authorization. Estimated completion is June 2018.

(c) Describe the purpose of the system:

The Crossmatch LSMS software applications, located within the DS FBIC boundary, capture fingerprints and other personal data electronically and formats this information into the FBI's electronic biometric transmission specification (EBTS) file. Once the user hits the submit button within the Crossmatch LSMS software application, the EBTS file is sent as an e-mail attachment to the FBI via the DS FBIC infrastructure/network. This EBTS file submission becomes an FBI request for background checks. This supports civil and criminal background investigation checks required by DS Field Offices (DS/DO/FLD), Personnel Security and Suitability (DS/SI/PSS), Badge Offices, and

High-Threat Posts (DS/HTP) to perform badging functions, and in support of Security Clearance and Suitability.

The Crossmatch LSMS software is installed on dedicated OpenNet workstations with a Crossmatch L Guardian device connected via USB port to capture fingerprints of the subject. The dedicated OpenNet workstations are located at Bureau of Diplomatic Security (DS) headquarters, DS Domestic field, resident offices, and specific high-threat posts, embassies, and consulates overseas.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
The DS FBIC uses the Crossmatch LSMS that collects biometrics data on potential employees, criminals, persons of interest, suspects to a crime or other individuals undergoing background and/or criminal investigations.

Information collected includes:

- Name
- Date of Birth
- Place of Birth
- Social Security Number
- Employment Information
- Address
- Fingerprints
- Physical description (height, weight, hair/eye color, tattoos and other markings, etc.)
- Arrest Record

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
The legal authorities are as documented in STATE-36 regarding Diplomatic Security records:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended);
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans).

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☐Yes, provide:
- SORN Name and Number:

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): Click here to enter a date.

☒No, explain how the information is retrieved without a personal identifier.

The Crossmatch LSMS software does not include a search function to query EFT files or the FBI's database. LSMS software is designed for submissions only.

Once FBI receives the EBTS file of the subject via the Crossmatch LSMS software, FBI assigns a universal control number (UCN) number for that transaction. The Crossmatch LSMS does not have this information because it is generated after Crossmatch has submitted the FBI request. The UCN number is included once the FBI response is received by the user. The user has the option to print out this response for including it in their case file.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)
If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)):
- Length of time the information is retained in the system:
- Type of information retained in the system:

Schedule Number	Length of Time	Type of Information
A-11-012-01 Criminal Investigative Case Files	Disposition: TEMPORARY. Cut off after case closes. Retire to RSC 10 years after closure for transfer to WNRC. Destroy 30 years after case closes.	Description: Headquarters, Field Offices and Overseas Files. Files contain information on investigations that range from passport and visa fraud, to smuggling, assault, and acts of terrorism, and they cover any investigations undertaken by DS, including, but not limited to, investigations internal to the Department of State. Files also consist of correspondence, reports, funds spent/received information, affidavits, subpoenas, search/arrest warrants, sworn statements, sentencing documents, evidence/property receipts, photos, copies of

		drivers licenses, birth and death certificates, passports, and other related documentation. Note that materials gathered during the execution of a search warrant may be in in these files.
A-11-025-01a Threat - Case Files - Contains correspondence, reports and other documentation on terrorist, criminal, and other specific threats or actions taken against individuals or property. Arranged by country.	Disposition: PERMANENT. Retire to the Records Service Center (RSC) when no longer needed for use in the office. Transfer to the Washington National Record Center 1 year after received by the RSC. Transfer to the National Archives when 25 years old in a format acceptable at that time.	Description: a. Cases concerning diplomats, American citizens, Department personnel or families, Department facilities or property, and cases of an unusual nature
A-11-025-01b Threat - Case Files - Contains correspondence, reports and other documentation on terrorist, criminal, and other specific threats or actions taken against individuals or property. Arranged by country	Disposition: Destroy/delete when 10 years old.	Description: b. All other cases.
A-11-027-01a DOS Clearance System	Disposition: N/A	The DOS Clearance System (DOSC) is the personnel security and suitability processing system and archive. The DOSC contains the security and suitability case files with their associated forms, reports, analysis, memoranda, worksheets, authorizations, etc. It tracks the various processing steps and activities involved with investigations and the determinations made regarding security clearances, public trust certifications and suitability. The system covers the entire

		process and interfaces with other external databases for information.
B-08-002-01a(2) Local Personnel Investigative Files	Disposition: Destroy three years after termination of employment.	Description: This covers both Department of State Non-American employees and other U.S. Government agency Non-American employees - when post security office conducts investigation. a. Locals who were certified for employment. (2) Regional Security Office copy.
B-08-002-01b(2) Local Personnel Investigative Files	Disposition: Note card and destroy.	Description: b. Locals who were refused certification for employment on the basis of information of record. (2) Regional Security Office copy.
B-08-002-01c(2)(a) Local Personnel Investigative Files	Disposition: Destroy when 5 years old.	Description: c. Locals who were investigated, but who abandoned their application. (2) Regional Security Office copy. (a) File containing derogatory information.
B-08-002-01c(2)(b) Local Personnel Investigative Files	Disposition: Destroy when 1 year old.	Description: c. Locals who were investigated, but who abandoned their application. (2) Regional Security Office copy.
B-08-002-01d(2) Local Personnel Investigative Files	Disposition: Destroy 5 years after termination, except for certain reporting required by security regulations	Description: d. Locals and local applicants who were terminated for cause. (2) Regional Security Office copy.
B-08-002-03a Security Case Files	Disposition: Card and destroy 1 year after case is closed.	Description: Security investigative files involving attempted penetration, fraud, loss of diplomatic pouches, and other cases not pertaining to investigations of individuals who are or may be employed by the Department or other Federal agencies. The record copies of these cases are retained by the Office of Security.

B-08-002-03b Security Case Files	Disposition: Permanent. Retire to RSC one year after case has been closed or designated inactive. Transfer to WRNC when 5 years old. Transfer to NARA when 30 years old.	Description: Case files involving terrorist groups, unsolved or significant murders, or special events. Contains information from newspaper clippings, reports, correspondence with local authorities, cables, etc.
B-08-002-04 Security Investigation Case Files - Foreign Nationals, escapees, exchanges, refugees, and visa applicants	Disposition: Cut off when case is closed and reported to the Department, requesting post, or other agency. Destroy case 1 year after cut-off date.	Description: Security investigation case files conducted for the Department, other posts, and other agencies. Correspondence, reports, and other documentation on security investigations conducted at the request of the Department, other posts, or other agencies in order to determine eligibility of escapees, refugees, and other foreign nationals for assistance, employment, exchange programs, or visas covering: criminal investigations, law enforcement agencies, offenses, visa fraud, and other related subjects.
B-08-002-05b Security Investigation Card Files	Disposition: Destroy 20 years after transfer to the inactive file	Description: Regional Security Office - Card files on security investigations conducted at post. Cards record basic data on cases of: Foreign Service Nationals certified for employment, including initial and subsequent investigations; Foreign Nationals refused employment; Foreign Nationals who abandoned an employment application after the security investigation was conducted; U.S. Government employees for whom overseas investigation is required; Non-American citizens being investigated for employment elsewhere, for a visa or other assistance, or for participation in an exchange program; Individuals involved in incidents such as attempted penetration, fraud, or loss of diplomatic pouches.
A-03-005-22 Personnel Security and Access Clearance Records	Temporary. Destroy 1 year after consideration of the candidate ends, but	Description: Records of people not issued clearances. Includes case files of applicants not hired.

	longer retention is authorized if required for business use.	Records about security clearances and other clearances for access to Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program. Includes: • questionnaires • summaries of reports prepared by the investigating agency • documentation of agency adjudication process and final determination Note: GRS 3.2, Information Systems Security Records, items 030 and 031, covers Information system access records. Exclusion: Copies of investigative reports covered in items 170 and 171. Disposition: Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use. DispAuthNo: DAA-GRS-2017-0006-0024 (GRS 5.6, item 180)
A-03-005-23 Personnel Security and Access Clearance Records	Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.	Description: Records of people issued clearances. Records about security clearances and other clearances for access to Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program. Includes: • questionnaires • summaries of reports prepared by the investigating agency • documentation of agency adjudication process and final determination

		Note: GRS 3.2, Information Systems Security Records, items 030 and 031, covers Information system access records. Exclusion: Copies of investigative reports covered in items 170 and 171. Disposition: Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use. (Supersedes GRS 18, item 22a) DispAuthNo: DAA-GRS-2017-0006-0025 (GRS 5.6, item 181)

---

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐No

The collection of the SSN is not required but highly recommended. When available it is used to perform a thorough criminal background check within national criminal database such as National Crime Information Center (NCIC).

For criminal investigations, the collection of the social security number will depend on the willingness of the subject when asked by the interviewer/user (e.g. DS Agent). In some cases, there are subjects that are aware of their criminal offenses, and they give false information or no information at all. Any information given by the subject is entered by the interviewer/user in the Crossmatch LSMS software accompanied by their electronic fingerprints to generate an FBI request. Once the FBI request is received by FBI, FBI checks the fingerprint for a match on their database and, if there is a match, confirms the legitimacy of the other personal information gathered during the interview of the subject.

For civil employment background investigations, the SSN is a key unique identifier to perform investigations on a subject as part of the process to determine employment eligibility.

- If yes, under what authorization?

(c) How is the information collected?
The interviewer's (e.g. DS Agent, DS PSS personnel) objective when using the system, is to gather the electronic fingerprint and personal information of the subject to generate the EBTS file required for an FBI criminal or background check. This is gathered by retrieving it from the individual directly during the interview; by retrieving other artifacts about the subject that contain the information (e.g. social security card, birth certificate, and passport). These types of information, including the electronic fingerprints, are entered within the Crossmatch LSMS software to generate the EBTS file and then submitted to FBI.

(d) Where is the information housed?
☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?
During the initial gathering of the information, there are no processes to determine if the information is accurate. However, the main purpose of the LSMS software is to submit a FBI request based on information gathered from the subject and verify if this information is available in the FBI's database. If the subject is in the FBI database, the agent can then compare the FBI's information about the subject against the information gathered from the subject.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
The agent enters the information provided by the subject in the Crossmatch LSMS software (e.g. name, fingerprints). The information is current during the time it was entered in the system and submitted to FBI. Because the purpose of the LSMS software is to submit an FBI background request based on information gathered from the subject, there is no need for the information to remain current in LSMS once the information is submitted to FBI.

(g) Does the system use information from commercial sources? Is the information publicly available?
The Crossmatch LSMS software does not use commercial information, publicly available information, or information from other Federal agency databases.

(h) Is notice provided to the individual prior to the collection of his or her information?
For criminal background investigations, subjects are verbally informed why they are being interviewed or why the DS Agents are gathering information, which is to perform background check and criminal records.

For civilian investigations, subjects are informed via documentation (e.g. official forms) that the gathering of their information (via official forms and interviews) is for the purpose of a background check (e.g. part of the employment process, to determine the

validity of their information). Notice of this type of collection of information is described in the System of Records Notice (SORN) titled Security Records, STATE-36.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
  Individuals do have this right. However, declining to provide information can have an adverse impact on background checks, which, in many cases, are a requirement to obtain employment with the Department.
- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?
All of the information collected in the Crossmatch LSMS is necessary for identification and investigation purposes; therefore privacy concerns did not influence which information is, or will be, collected and entered in the Crossmatch LSMS software.

5. Use of information

(a) What is/are the intended use(s) for the information?
The Crossmatch LSMS software and scanner are used to capture fingerprints electronically, and collect information about the individual, which is needed for subject identification in investigations. All scanned fingerprints and collected information are the minimum amount of PII needed to identify a given individual. Prints are captured using OpenNet connected terminals and emailed to DS headquarters where they are printed and stored in file cabinets for purposes of auditing. Storage of records is consistent with Department retention schedules.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes, all of the information collected in Crossmatch is necessary for identification and investigation purposes.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The Crossmatch Software is only shared to make a FBI request for background check. The information is sent to and shared with the FBI to determine if there is a match in their database. The results from the FBI background check are sent to the appropriate DS personnel requesting the background investigation for purposes of analysis and storage. It is for DS consumption only.

(b) What information will be shared?

The Crossmatch LSMS software is only for the outgoing process; FBI receives the following information DS gathered from the subject:

- Name
- Date of Birth
- Place of Birth
- Social Security Number
- Employment Information
- Address
- Fingerprints
- Physical description (height, weight, hair/eye color, tattoos and other markings, etc.)
- Arrest Record

(c) What is the purpose for sharing the information?

The information sent to the FBI is to search their database for a match with their records. The information received from FBI and sent to the DS personnel requesting the background investigation is for the purpose of performing criminal and/or background investigations.

(d) The information to be shared is transmitted or disclosed by what methods?

The FBI can only communicate with the Crossmatch LSMS software via SMTP e-mail services. FBI requests are sent via e-mail as an attached .eft file. FBI responses are sent back to DS via e-mail as an attached .eft or .rsp file. These transactions are through a private WAN encrypted link between DoS and FBI.

(e) What safeguards are in place for each internal or external sharing arrangement?

When it comes to policy, a Memo of Agreement is in place to state the intent of the communication between DoS and FBI passing through this private WAN link. In terms of physical safeguards, firewalls are in place that only allow particular systems to interact. Also, the private WAN link is encrypted. In terms of process safeguards, FBI can only process FBI requests with the appropriate ORI number that is only associated with the appropriate e-mail that will receive the FBI responses.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
The primary privacy risk is the inadvertent spillage of individual PII outside the confines of the OpenNet network. This risk is mitigated through the Department's annual cyber security briefing requirement and by the standard procedures and instruction provided to investigators as part of their work. Risks associated with sharing privacy information are generally related to personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure of PII. These include, but are not limited to, annual security training, separation of duties, least privilege and personnel screening.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Procedures for notification and redress are published in the system of records notice identified – Security Records, State-36 – and in rules published in 22 CFR 171.31. The procedures instruct the individual on how to inquire into the existence of such records, how to request access to their records, and how to request amendment of their record.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
In terms of using the Crossmatch LSMS software, the objective is to gather accurate information and capture clear fingerprints directly from the subject to provide the FBI with accurate information used for finding a match in the FBI database. Inaccuracy or erroneous information will depend on the subject's provided information. In terms of the FBI results derived from the Crossmatch LSMS FBI background check request, the subject's gathered information can then be compared with the FBI records, if there was a match. Any discrepancy can be discussed with the subject to determine why there is a discrepancy with the information, or analyzed, if the subject was not honest during the interview.
If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
Procedures for notification and redress are published in the system of records notice identified – Security Records, State-36 – and in rules published at 22 CFR 171.31. The

procedures instruct the individual on how to inquire into the existence of such records, how to request access to their records, and how to request amendment of their record.

In terms of FBI request submissions, the FBI notifies DS personnel via e-mail if certain information is inadequate, incomplete or erroneous based on the field type (e.g. fingerprints are not clear).

8. Security Controls

(a) How is the information in the system secured?

Users are required to use specific OpenNet workstations and are required to log into the workstation using their OpenNet PIV card. The Crossmatch LSMS software checks if the authenticated user is allowed to use the application. The private WAN link between DoS and the FBI is encrypted to secure transmission between the two organizations. Responses from the FBI are only allowed for a specific e-mail address based on the Originating Agency Identifier (ORI) during the FBI request submission.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Access to DS FBIC is limited to a small number of DS personnel. In order to gain access to utilize the equipment, an individual must be verified as a DS investigator having a legitimate need to use the device. The DS investigator requests acquisition of the equipment and will request that it be installed to their OpenNet workstation. Once installed, the DS investigator is required to email any data captured to their designated division (e.g. Office of Personnel Security and Suitability (DS/SI/PSS), DS/FLD, Badge Office). Once emailed, the EBTS file may be deleted from the local PC. Since this is desktop connected hardware and locally installed software, the standard audit log review process for any OpenNet PC are in place. The following sections of the FAM apply:

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Users are logged when they log into the designated OpenNet workstation. The log-in process is recorded under the OpenNet domain system logs. The Crossmatch LSMS software also has historical logging, when an FBI request is created, submitted and if the transmission is successful.

(d) Explain the privacy training provided to authorized users of the system.
All DS users of the Crossmatch product are trained in the proper use of this information. They are also required to undergo computer security and privacy awareness training prior to use and must complete refresher training annually in order to retain access.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
As stated in Section 8 (a), users are required to use specific OpenNet workstations and are required to log into the workstation using their OpenNet PIV card. The Crossmatch LSMS software checks the authenticated user if it is allowed to use the application. The private WAN link between DoS and the FBI is encrypted to secure transmission between the two organizations. Responses from FBI are only allowed for a specific e-mail address based on the ORI during the FBI request submission.

(f) How were the security measures above influenced by the type of information collected?

No additional security measures were implemented for the DS FBIC system. The existing mandates and rules of the State Department FAM/FAH which require the implementation of the NIST/OMB requirements specified in governing documents NIST SP 800-37, NIST SP 800-18, NIST-SP 800-34, and NIST-SP 800-53 have prepared the required secure environment for proper Assessment and Authorization (A&A) evaluation and approval. The steps began with system characterization (SCF) as "Moderate". The detailed security classification information of the SCF expanded applicable Security Controls to be applied to the DS FBIC implementation to include specific timed validations and verifications to ensure proper operation and security. The required expanded validation complemented the existing OpenNet controls implemented world-wide within the controlled SBU network environment. Limited/controlled access, positive user control, logging and auditing, and focused training are mandatory throughout the internal network, and are more sharply mandated to manage the DS FBIC operation.

9. Data Access

(a) Who has access to data in the system?
Access to the product is limited to a small number of DS personnel. In order to gain access to utilize the equipment an individual must be verified as a DS investigator having a legitimate need to use the device or a system administrator required to only add the appropriate personnel who can access the dedicated OpenNet workstation.

(b) How is access to data in the system determined?
The user is required to log in to the OpenNet workstation using their PIV card. The system administrator is required to only add the appropriate personnel who can access the

dedicated OpenNet workstation. The Crossmatch LSMS software is set to check the Active Directory Services to verify that the user is allowed to use the Crossmatch LSMS application.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Data access is restricted only to users who can access the Crossmatch LSMS application. As mentioned in Section 9 (b), the system administrator is required to only add the appropriate personnel who can access the dedicated OpenNet workstation.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

As stated in Section 8 (f), there are numerous management, operational and technical security controls compliant with DS Security in place to protect the data as part of OpenNet. These are in accordance with the Federal Information Security Modernization Act (FISMA) of 2014 and the information assurance standards published by the National Institute of Standards and Technology (NIST). Controls include regular security assessments, physical and environmental protection, 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) and audit reports.

In terms of controls placed on OpenNet and the Crossmatch LSMS, the user is required to log in to the OpenNet workstation using their PIV card. The system administrator is required to only add the appropriate personnel who can access the dedicated OpenNet workstation. The Crossmatch LSMS software is set to check the Active Directory Services to verify if the user is allowed to use the Crossmatch LSMS application.