

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT  
HOMELAND SECURITY INVESTIGATIONS**

**HSI Directive 14-01: Mandatory Booking of Arrestees Using EAGLE**

**Issue Date:** April 23, 2014  
**Effective Date:** April 23, 2014  
**Superseded:** U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations Directive 12-01, "Mandatory Booking of Arrestees Using EAGLE," dated January 4, 2012. (Note: Sections 3.12, 6.1, 6.4, and 7.10 of the Compliance Enforcement Handbook (HB) (OI HB 10-01), dated January 25, 2010, involving booking procedures, were superseded on January 4, 2012, by HSI Directive 12-01.)  
**Federal Enterprise Architecture Number:** 306-112-002b

- 1. Purpose/Background.** Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement (EAGLE) is the mandatory booking system for all subjects arrested by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). This Directive applies to all HSI employees and Task Force Officers (TFOs) in offices where EAGLE has been deployed. (Note: Information on EAGLE can be found on the Mobile Automated Biometric Information System (IDENT) SharePoint site at: **(b) (7)(E)**)

Previously, HSI submitted subjects' fingerprints to the Criminal Justice Information Services Division (CJIS) of the Federal Bureau of Investigation (FBI) for entry into the Integrated Automated Fingerprint Identification System (IAFIS). (Note: The Automated Fingerprint Identification Technology (AFIT) replaced IAFIS in the second quarter of FY 2011.) On July 13, 2011, HSI was notified by CJIS that they will no longer accept paper-based fingerprint cards (FD-249) after April 15, 2012. CJIS now requires that all fingerprint submissions be sent electronically. When HSI Special Agents (SAs) book a subject via EAGLE, fingerprints will be electronically submitted to CJIS and AFIT.

- 2. Policy.** Every arrest conducted by HSI must be entered into EAGLE. If a subject is arrested by HSI, the subject's information and fingerprints must be entered into EAGLE as soon as possible. HSI does not typically fingerprint juveniles under the age of 14, but in limited cases, juveniles should be booked if they have a criminal history or are being arrested for criminal charges and pose a risk. Every entry in EAGLE must contain a subject's biometrics and biographic information. HSI employees will interface with IDENT and AFIT via EAGLE. HSI SAs are still required to enter case management information in TECS, including criminal and administrative arrests. (See the Case Management Handbook (OI HB 08-02), dated February 1, 2008, or as updated.)

When HSI SAs enter an arrest into SEACATS, they must also enter it into EAGLE. HSI SAs are authorized to submit fingerprints to the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) IDENT if the arresting agency does not have access to IDENT.

For officer safety, only HSI SAs or designated law enforcement officers assisting HSI may handle and book (i.e., fingerprint) arrestees. Federal, state, local, or tribal law enforcement officers who make an arrest on behalf of HSI may use EAGLE but only to enter a subject's biometric and biographic information into the Enforcement Integrated Database (EID), IDENT, and AFIT. Any HSI employee or authorized user may use EAGLE to enter and/or query information for official purposes. Per Section 5.11 of OI HB 07-02, "All individuals detained by [HSI] SAs must be identified and the identities must subsequently be appropriately documented." All subjects must be identified and documented via EAGLE.

3. **Definitions.** The following definitions apply for the purposes of this Directive only:
  - 3.1. **AFIT** is an FBI system that holds specific fingerprint, biographic, and criminal history information of persons who have been apprehended or arrested by various law enforcement agencies.
  - 3.2. The **Biometric Support Center (BSC)** is a 24-hour center maintained by US-VISIT for the support of the Department of Homeland Security (DHS) and other law enforcement agencies. BSC provides support to HSI field offices in their use of: 1) IDENT Lookout Database enrollments; 2) Fingerprint Identification Verification; and 3) 10-print Search Only services.
  - 3.3. An **arrest** "is an actual or constructive restraint of an individual, performed with the intention of taking the individual into custody." See OI HB 07-02, Section 2.5. (See "Individual in custody").
  - 3.4. **Biometric data** includes, but is not limited to, name, date of birth, nationality, fingerprints, and other personal descriptive data.
  - 3.5. **EAGLE** is the primary database within HSI for booking, searching and entering a subject's biometric information into EID, IDENT, and AFIT. It is a mobile-capable application used to conduct fingerprint and biographic searches and to submit booking information to EID. EAGLE has two Biometric Search transactions and two Booking and Enrollment transactions. It uses existing service connections and planned connections to US-VISIT IDENT, Department of Justice Joint Automated Booking System (JABS), FBI CJIS AFIT, National Crime Information Center (NCIC), and Department of Defense Automated Biometric Identification System to update biometrically verified information in near real-time. This information is available for all approved users internal and external to DHS, and other law enforcement agencies.

- 3.6.** **EID** is the ICE database repository for enforcement applications. This database is used by ICE, U.S. Customs and Border Protection, and U.S. Citizenship and Immigration Services.
- 3.7.** The **Enforcement Case Tracking System (ENFORCE)** is a group of applications designed to interface with EID for processing enforcement-related activities. Some of the applications contained in ENFORCE include: ENFORCE Apprehension Booking Module (EABM), General Counsel Electronic Management System (GEMS), IDENT, and Worksite Enforcement Activity Reporting System (commonly referred to as LYNX).
- 3.8.** The **ENFORCE EABM** is the principal user interface with EID and is an incident-based application that standardizes the collection and reporting of enforcement data across DHS.
- 3.9.** The **FBI Number (FNU)** is the primary identifier assigned to a criminal subject used by the FBI and AFIT for identification and tracking.
- 3.10.** **IAFIS** was a component of the FBI Privacy Act System of Records, known as the “Fingerprint Identification Records System” (FIRS) (Justice/FBI-009), available at **(b) (7)(E)**.
- 3.11.** **IDENT** is an automated DHS system that permits the capture and search of biometric information for subject identification. IDENT collects biometric, limited biographic, and encounter-related data. (See Privacy Act; IDENT System of Records, 72 Fed. Reg. 31080, 31082 (June 5, 2007).
- 3.12.** **Individuals in custody**, refer to “persons or groups of people who have been detained, arrested, or seized and/or transported as a result of such action by HSI SAs in the performance of their official duties. It should be noted that the term ‘custody’ could have legal ramifications for triggering the rights established in Miranda v. Arizona. For the purposes of this Handbook, an ‘individual in custody’ may not necessarily be in ‘custody’ for Miranda purposes.”
- 3.13.** **Investigative detention** is a brief detention of a subject that does not constitute an arrest upon reasonable suspicion (i.e., supported by articulable facts, not merely a hunch that the subject was involved in a crime. The detention may last only long enough to confirm or dispel the suspicion of criminal activity.
- 3.14.** **10-Print Live-Scan System/Equipment** is a live-scan system that captures fingerprints electronically and transmits them to AFIT.
- 3.15.** **US-VISIT** contains biometrically-enhanced security measures that begin outside the United States and continue through a subject’s arrival and departure from the United States.

**4. Responsibilities.**

- 4.1. The Executive Associate Director of HSI is responsible for the oversight of policy and procedures established by this Directive.
- 4.2. Special Agents in Charge (SACs) are responsible for implementing the provisions of this Directive within their areas of responsibility (AORs). Additionally, SACs are responsible for ensuring that all HSI employees and TFOs working with HSI comply with this Directive.
- 4.3. All HSI employees and TFOs working with HSI are responsible for complying with the provisions of this Directive.

**5. Procedures.**

- 5.1. During the booking process via EAGLE, HSI SAs or other designated law enforcement officers assisting HSI, i.e., task force officers, **(b) (7)(E)**
  
- 5.2. When booking an arrested subject in EAGLE, HSI SAs or other designated law enforcement officers should use the following transactions:

**(b) (7)(E)**

- 5.3. HSI SAs and TFOs working with HSI will not use biometrics taken from a prior subject's arrest to perform a "SUBMIT BOOKING" and "ENROLL" or a "SEARCH" and

“ENROLL.” Authorized users must use biometrics collected during a current arrest. This requirement prevents inaccurate records from being entered into IDENT, AFIT, NCIC, and JABS for an arrested subject.

- 5.4. After searching a subject and entering the required booking information via EAGLE, HSI SAs and other authorized users will **(b) (7)(E)**

- 5.5. Once a subject is booked via EAGLE, **(b) (7)(E)**

- 5.6. Authorized users may elect to utilize EAGLE to scan a subject’s fingerprints electronically, obtain a biometric verification on prior arrests and other encounters with DHS and/or state, local, tribal, or other federal law enforcement agencies. Consent to search a subject’s fingerprints is required except in the following circumstances:

**(b) (7)(E)**

- 5.7. Information obtained via EAGLE can provide valuable information by verifying a subject’s identity and identifying connections to past encounters with DHS, arrests, and/or known associates. Fingerprint scanning may be done during or after a subject is in

custody immediately following the arrest.

**(b) (7)(E)**

- 5.8.** If, at any time during a consensual encounter, consent is withdrawn, a warrant may be necessary to take a subject's fingerprints. HSI SAs should take note of the following: In *Davis v. Mississippi*, 394 U.S. 721 (1969), the Supreme Court held that the taking of fingerprints is covered by the Fourth Amendment prohibition against unreasonable searches and seizures, and that fingerprints obtained as a result of an *illegal detention* are improperly admitted into evidence. In *Davis*, the defendant's detention was not based on a warrant or probable cause, and therefore constitutionally invalid. However, the court also indicated, "Detention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search." In his concurrence, Justice Harlan stated, "There may be circumstances... where compelled submission to fingerprinting would not amount to a violation of the Fourth Amendment, even in the absence of a warrant..." The necessity for a search warrant when obtaining fingerprints depends on the circumstances surrounding the lawfulness of the detention. The detention must be based on reasonable suspicion; otherwise it is likely constitutionally invalid.
- 5.9.** If a subject has been issued an arrest warrant, HSI SA must contact the responsible agency that filed the Warrant with CJIS prior to releasing the subject. A proper notification to the ORI agency will consist of the following: verifying the warrant is for the subject and valid; verifying the subject's current location and to what court or jurisdiction he or she will be turned over; and extradite the subject from the location of detention or arrest. HSI SAs will record this notification and any actions taken in a Report of Investigation and/or on a "Record of Deportable/Inadmissible Alien (DHS Form I-213)."
- 5.10.** HSI SAs can obtain a subject's fingerprints from the following sources:
- A. The FBI CJIS Expedited Services Unit at **(b) (7)(E)**
  - B. Alien Files maintained by DHS;
  - C. State, local, tribal, foreign, and other federal law enforcement and regulatory agencies;
  - D. Latent print processing from evidence submitted to HSI's Forensic Document Laboratory (FDL) or another law enforcement forensic laboratory; and
  - E. DHS US-VISIT BSC at **(b) (7)(E)** or by sending an email, via Microsoft Outlook, to: BSC Mailbox.

- 5.11. The FDL’s Fingerprint Section provides support to HSI field offices by applying scientific expertise in multiple investigative disciplines. The FDL Fingerprint Section has access to the US-VISIT database for searching fingerprints and HSI SAs should contact the FDL’s Fingerprint Section for assistance related to fingerprinting issues.
- 5.12. The BSC provides HSI SAs with the ability to submit single, partial, latent, and non-standard CJIS 14-type fingerprints electronically to search against US-VISIT and other databases. As needed, HSI SAs should contact the BSC to request fingerprint services. The fingerprint services BSC provides are: identifying the prints of unknown deceased persons, testifying in court, and validation of fingerprint matches.
- 5.13. In cooperation with the U.S. National Central Bureau of the International Criminal Police Organization (INTERPOL) and US-VISIT, the HSI Counterterrorism and Criminal Exploitation Unit has developed a biometric-based program to identify foreign fugitives who have entered the United States. U.S. law does not permit the arrest of an individual based solely on the existence of a Red Notice from INTERPOL. U.S. law enforcement officers, including HSI SAs, are required to obtain provisional arrest warrants or develop probable cause that leads to an arrest for a violation of U.S. law.

## **6. Authorities/References.**

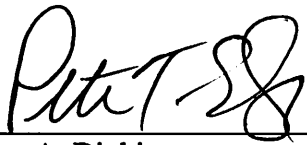
- 6.1. 8 U.S.C. § 1302 “Registration of aliens.”
- 6.2. 8 U.S.C. § 1304(e), Forms for registration and fingerprinting.
- 6.3. 8 U.S.C. § 1357(f), “Powers of immigration officers and employees.”
- 6.4. 8 C.F.R. § 236.5 “Fingerprints and photographs.”
- 6.5. Privacy Act; IDENT System of Records, 72 Fed. Reg. 31080, 31082 (June 5, 2007).
- 6.6. Privacy Act of 1974; United States Immigration and Customs Enforcement—008 Search, Arrest, and Seizure Records System of Records, 73 Fed. Reg. 74732, 74735 (Dec. 9, 2008)
- 6.7. Privacy Act of 1974; Department of Homeland Security United States Immigration and Customs Enforcement--011 Immigration and Enforcement Operational Records System of Records, 75 Fed. Reg. 23274, 23279 (May 3, 2010).
- 6.8. ICE Directive 10066.1 (former number: 7-3.0, “Consular Notification of Detained or Arrested Foreign Nationals” (Feb. 13, 2006)
- 6.9. OI HB 07-02, “Arrest Procedures Handbook” (Oct. 4, 2007)
- 6.10. OI HB 08-02, “Case Management Handbook” (Feb. 1, 2008)

6.11. OI HB 10-01, "Compliance Enforcement Investigations Handbook" (Jan. 25, 2010)

6.12. FBI CJIS Notification Letter, date June 24, 2011.

7. **Attachments.** None.

8. **No Private Right.** These guidelines and priorities are not intended to, do not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter.

  
\_\_\_\_\_  
FOR  
EAD James A. Dinkins  
Executive Associate Director  
Homeland Security Investigations