ATTACHMENT B:

Narrative Statement for Modifying a System of Records Under the Privacy Act of 1974

for
Defense Biometric Identification Records System
OMB Control Number: 0702-0127
Paperwork Reduction Act (PRA) Submission
Reference Associated OMB Form 83-I

1. **System name and number**: Defense Biometric Identification Records System, A0025–2 PMG (DFBA) DoD

2. **Nature of proposed modifications for the system**: The Defense Forensics and Biometrics Agency (DFBA) participates as a partner in the Department of Defense (DoD) defense vetting enterprise for the biometric vetting portion of continuous vetting (CV) and continuous evaluation (CE), providing biometrics for automated records checks (ARC) in support of U.S. government vetting efforts. If this system were not available, DoD would be unable to share vital national security threat (NST) and known or suspected terrorist (KST) data with identity activity enterprise partners. As a result, DoD would in some cases be unable to positively identify external threat actors or insider threats.

The Department of the Army is proposing to revise the existing system of records by updating the categories of individuals, categories of records, authority for maintenance, purposes, and routine uses. The retention period for biometric records is increasing from 75 years to 110 years to match interagency partner retention. This notice also incorporates formatting changes established in OMB A-108 Circular, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act." All other changes to the notice are administrative in nature. The DoD is publishing this notice in its entirety as a supersession of all previous versions.

3. **Specific authority under which the system of records is maintained**:

Section 112 of Public Law (Pub. L.) 106-246, Emergency Supplemental Act of 2000; 10 U.S. Code (U.S.C.) Sections 113 and 3013; Pub. L. 108-458, The Privacy Act of 1974, as amended, ("Privacy Act") (5 U.S.C. 552a), Pub. L. 93-579; Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order (E.O.) 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans; E.O. 13764, Amending the Civil Service Rules, E.O. 13488 and E.O. 13467 to Modernize the Executive Branch-Wide Governance Structure and

Processes for Security Clearances; E.O. 9397, Numbering System for Federal Accounts; E.O. 9397 (SSN), as amended; Homeland Security Presidential Directive (HSPD)-6, Integration and Use of Screening Information; HSPD-11, Comprehensive Terrorist-Related Screening Procedures; National Security Presidential Directive (NSPD)-59/HSPD-24, Biometrics for Identification and Screening to Enhance National Security; National Security Presidential Memorandum (NSPM) 7, Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans; NSPM 9, Presidential Policy Directive 30, Hostage Rescue Activities; National Vetting Enterprise; 32 Code of Federal Regulations (CFR) Part 310 (84 FR 14728); DoD Directive (DoDD) 8521.01E, DoD Biometrics; DoDD 8500.1, Information Assurance; DoDD 5205.15E, Defense Forensics Enterprise (DFE); DoD 5200.08-R, Physical Security Program; DoDD 5110.10 Defense Prisoner of War/Missing Office Personnel Office (DPMO); DoDD 8500.01, DoDD 2310.07, Personnel Accounting—Losses Due to Hostile Acts; DoDI 2000.12, DoD Antiterrorism (AT) Program; DoDI 2310.05, Accounting for Missing Persons; DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); Cybersecurity; AR 10-90, DoD Executive Agent Responsibilities of Secretary of the Army; Army Regulation (AR) 25-2, Information Assurance; AR 190-8, Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees; AR 525-13, Antiterrorism; and USD(I) Directive-Type Memorandum (DTM) 09-012: Interim Policy Guidance for DoD Physical Access Control; AR 190-8, Enemy POW, Retained Personnel, Civilian Internees and Other Detainees; AR 525-13, Antiterrorism; Department of the Army General Order (DAGO) No. 2020-01, Assignment of Functions and Responsibilities Within DA, 06 March 2020; and USD(I) Directive-Type Memorandum (DTM) 09-012: Interim Policy Guidance for DoD Physical Access Control.

4. **Evaluation of the probable or potential effect on the privacy of individuals**: The privacy risks associated with DBIRS include the inappropriate denial of freedom of movement or access to logical and physical assets. These risks may result from unauthorized collection, use, disclosure and retention of personal information as well as insufficient data quality.

Unauthorized collection and use can occur when systems that provide information to DBIRS exceed their authority for collection. Once information is submitted, the following may occur: 1) errors or omissions in the data regarding an individual's citizenship may result in some United States person (USPER) records not being identified or handled appropriately; 2) contextual data may be inappropriately interpreted as derogatory; and 3) inaccurate biometric matching may result in false acceptance or false rejection. False acceptance may occur when a biometric system other than DBIRS incorrectly identifies a biometric subject or incorrectly authenticates an impostor against a claimed identity, such as allowing an individual who should not have access to a military installation onto a military installation. False rejection may occur when a biometric system other than DBIRS fails to identify a biometric subject or to verify the

legitimate claimed identity of a biometric subject, such as denying an individual who should have access to a military base from a military base.

Established policies and procedures minimize potential privacy risks. DBIRS promotes the authorized use of personal information by only accepting data and search requests from authorized agencies and by limiting search responses to match/no match with associated, unverified biographical information. DoD subject matter experts are available to determine whether contextual data associated with a match is derogatory. DBIRS promotes data quality by comparing data types from more than one source when updating the data, using the highest quality biometrics for matching and continually testing algorithms to improve system biometric matching capabilities.

DBIRS secures personally identifiable information (PII) and other data with multiple layers of logical access controls. Storage systems are physically isolated from external access and are logically located behind three firewalls. A network-based intrusion detection system and a host-based intrusion detection system have been implemented. In addition, rigorous physical access controls have been implemented, including security personnel and biometric identification systems.

Due to the level of safeguarding, the risk to individual privacy is minimal. Appropriate safeguards are in place for the collection, use, and safeguarding of information.

5. **Routine use compatibility**: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, as amended, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. **Law Enforcement (Investigations)**: To the appropriate federal, state, local, territorial, tribal, or foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

b. **Department of Justice Litigation**: To any component of the Department of Justice for the purpose of representing the DoD, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

c. **Legal Proceedings**: In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the

proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

d. **Records Management Inspections**: To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

e. **Congressional Affairs**: To a member of Congress or staff acting upon the member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

f. **Breach Disclosure**: To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

g. **Breach Response**: To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

h. **Performance**: To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary, to accomplish an agency function related to this system of records.

i. **Continuous Evaluation**: To Defense Security Services and other participants in the defense vetting enterprise for purposes of continuous evaluation (CE) as defined in EO

13764 as a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility in order to leverage a set of automated record checks and business rules to assist in the ongoing assessment of an individual's continued eligibility. CE is intended to complement continuous vetting efforts already occurring within DoD.

j. **Terrorist and National Security Threat Screening**: To any Federal, State, tribal, local, territorial, foreign, or multinational agency, entity or organization that is engaged in, or is planning to engage in, terrorism screening, or national security threat screening, authorized by the U.S. Government, for the purpose of development, testing, or modification of information technology systems used or intended to be used during or in support of the screening process; whenever practicable, however, DFBA, to the extent possible, will substitute anonymized or de-identified data, such that the identity of the individual cannot be derived from the data.

k. **Continuity of Operations**: To those federal agencies that have agreed to provide support to DFBA for purposes of ensuring the continuity of DFBA operations.

l. **Quality Assurance and Redress**: To any Federal, State, tribal, local, territorial, foreign, multinational agency or task force, or any other entity or person that receives information from the U.S. Government for terrorism screening purposes, or national security threat screening purposes, in order to facilitate DFBA's or the recipient's review, maintenance, and correction of DFBA data for quality assurance or redress purposes, and to assist persons misidentified during a screening process. To any person or entity in either the public or private sector, domestic or foreign, when reasonably necessary to elicit information or cooperation from the recipient for use by DFBA in the performance of an authorized function, such as obtaining information from data sources as to the thoroughness, accuracy, currency, or reliability of the data provided so that DFBA may review the quality and integrity of its records for quality assurance or redress purposes, and may also assist persons misidentified during a screening process.

m. **Personnel Recovery**: To Federal, State, tribal, local, foreign or international agencies, task forces or organizations, for the purposes personnel recovery as authorized by law or policy.

6. **OMB public information collection requirements**:

OMB collection required: Yes

OMB Control Number: 0702-0127

Title of collection: Automated Biometric Identification System (ABIS)

Date Submitted to OMB if pending: N/A

Expiration Date (if approved): 09/30/2017

Information Required by DPCLTD: (Not submitted to OMB)

7. **Name of IT system**: Defense Biometric Identification Records System, DITPR # 15478/DA207770.

8. **Is the system, in whole or in part, being maintained, (maintained, collected, used, or disseminated) by a contractor?** Yes

SYSTEM NAME AND NUMBER: Defense Biometric Identification Records System (DBIRS), A0025–2 PMG (DFBA) DoD

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Defense Forensics and Biometrics Agency, 1000 Custer Hollow Road, Clarksburg, WV 26306-0001.

SYSTEM MANAGER: Director, Defense Forensics and Biometrics Agency, DAPM-FB, 2800 Army Pentagon, Washington DC 20310-2800.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Section 112 of Pub. L. 106-246, Emergency Supplemental Act of 2000; U.S.C. Sections 113 and 3013; Pub. L. 108-458, The Privacy Act (5 U.S.C. 552a), Pub. L. 93-579; Intelligence Reform and Terrorism Prevention Act of 2004; E.O. 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans; E.O. 13764, Amending the Civil Service Rules, E.O. 13488 and E.O. 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances; E.O. 9397, Numbering System for Federal Accounts; E.O. 9397 (SSN), as amended; HSPD)-6, Integration and Use of Screening Information; HSPD-11, Comprehensive Terrorist-Related Screening Procedures; National Security Presidential Directive (NSPD)-59/HSPD-24, Biometrics for Identification and Screening to Enhance National Security; National Security Presidential Memorandum (NSPM) 7, Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans; NSPM 9, Presidential Policy Directive 30, Hostage Rescue Activities; National Vetting Enterprise; 32 CFR Part 310 (84 FR 14728); DoDD 8521.01E, DoD Biometrics; DoDD 8500.1, Information Assurance; DoDD 5205.15E, DFE; DoD 5200.08-R, Physical Security Program; DoDD 5110.10, DPMO; DoDD 8500.01, DoDD 2310.07, Personnel Accounting—Losses Due to Hostile Acts; DoDI 2000.12, DoD AT Program; DoDI 2310.05, Accounting for Missing Persons; DoDI 5200.08, Security of DoD Installations and Resources and the DoD PSRB; Cybersecurity; AR 10-90, DoD Executive Agent Responsibilities of Secretary of the Army; AR 25-2, Information Assurance; AR 190-8, Enemy POW, Retained Personnel, Civilian Internees and Other Detainees; AR 525-13, Antiterrorism; and USD(I) DTM 09-012: Interim Policy Guidance for DoD Physical Access Control; AR 190-8, Enemy POW, Retained Personnel, Civilian Internees and Other Detainees; AR 525-13, Antiterrorism; DAGO No. 2020-01, Assignment of Functions and Responsibilities Within DA, 06 March 2020; and USD(I) DTM 09-012: Interim Policy Guidance for DoD Physical Access Control.

PURPOSE(S) OF THE SYSTEM: The system facilitates biometric identification (i.e., automated identity verification, by reference to their measurable physiological and/or behavioral characteristics), of individuals who seek access to DoD property, installations, or information; individuals who pose a threat to DoD personnel, assets or missions, or to national security; individuals who are captured, detained, or otherwise encountered by DoD forces during military operations; and individuals for whom DoD has the responsibility to recover or account during or as a result of DoD operations. Information is collected to support DoD military missions, detainee affairs, personnel recovery, identification of remains, force protection, antiterrorism, special operations, stability operations, homeland defense, counterintelligence, and intelligence efforts around the world (excluding those intelligence activities identified in the note in Categories of Records). System records are a major element of DoD's Biometrically Enabled Watchlist (BEWL) of individuals nominated based upon previous encounters of special concern to DoD. The system is the DoD entry point into the biometric enterprise system for purposes of continuous vetting (CV) and continuous evaluation (CE).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Persons covered include all military, civilian, and contractor personnel; individuals requiring or requesting access to DoD, DoD-controlled, and/or DoD contractor operated, controlled or secured data, information systems, equipment, facilities or installations; individuals who have been declared missing or prisoners of war; individuals who are being detained or held hostage by hostile forces or are suspected of being held under such circumstances within an area of DoD operations; individuals recovered from hostile control by DoD personnel or as a result of DoD operations; individuals within the purview of the DoD personnel recovery mission which supports U.S. military, DoD civilian, and DoD contractor personnel while hostilities are ongoing; individuals within the purview of the DoD personnel accounting mission which supports U.S. military, DoD civilian, and DoD contractor personnel once hostilities cease; individuals in DoD custody as a result of military operations overseas or due to maritime intercepts; individuals otherwise encountered by DoD forces during military operations; individuals lawfully assessed by appropriate authority in accordance with applicable law and policy to pose a potential threat to DoD personnel, installations, assets, information and/or operations; individuals who are the subject of pending queries against the subject record system; individuals identified during a biometric screening process as a possible identity match to the subject of an existing record within the system (i.e., data regarding persons for whom DoD has good reason to believe there is potential substantive justification for retention but have not yet been able to absolutely confirm); individuals who are misidentified as a possible identity match to the subject of an existing record within the system (i.e., misidentified persons); individuals who are the subject of a redress inquiry that is pending resolution; and other persons encountered throughout the full range of military operations.

CATEGORIES OF RECORDS IN THE SYSTEM: This system includes identity records established to support automated identification, authentication, or verification including biometric information and related biographic, contextual, and other information, reports, and data in paper and/or electronic format. Records include biometric information, such as images, photos and templates of biological (anatomical and physiological) and/or behavioral characteristics that can be used for automated recognition, including, fingerprints, palm prints, facial images, iris images, DNA, and voice samples. Biographic information including name, date of birth, place of birth, height, weight, eye color, hair color, race, gender, social security number, and similar relevant information; and contextual information including organization, telephone number, office symbol, security clearance, level of access, and location of collection. User information including subject interest codes; user identification codes; globally unique identifiers; data files retained by users; assigned passwords; magnetic tape reel identification; abstracts of computer programs and names and phone numbers of contributors, and similar relevant information; Information concerning DoD-affiliated persons who are being detained or held hostage by hostile forces, or non-DoD affiliated USPER known or suspected to be held under such circumstances in an area of DoD operations, such as biographic data, casualty reports, and debriefing reports; Information from and electronic images of international federal, state, tribal, or state issued individual identity documents.

Note: This system expressly does not maintain any record or information that is subject to Executive Order 12333, United States intelligence activities; DoDD 5240.01, DoD Intelligence Activities; DoD-M 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities; or AR 381-10, U.S. Army Intelligence Activities.

RECORD SOURCE CATEGORIES: Information in this system may be provided by the individual; from Military Departments, Combatant Commands, or other DoD component systems; the Department of Justice, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security, the Department of State, or foreign governments in accordance with applicable law, policy, agreements, and published routine uses.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING:

CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To any Federal, State, tribal, local, territorial, foreign, or multinational agency, entity or organization that is engaged in, or is planning to engage in, terrorism screening, or national security threat screening, authorized by the U.S. Government, for the purpose of development, testing, or modification of information technology systems used or intended to be used during or in support of the screening process; whenever practicable, however, DFBA, to the extent possible, will substitute anonymized or de-identified data, such that the identity of the individual cannot be derived from the data.

b. To any Federal, State, tribal, local, territorial, foreign, multinational agency or task force, or any other entity or person that receives information from the U.S. Government for terrorism screening purposes, or national security threat screening purposes, in order to facilitate DFBA's or the recipient's review, maintenance, and correction of DFBA data for quality assurance or redress purposes, and to assist persons misidentified during a screening process.

c. To Federal, State, tribal, local, foreign or international agencies, task forces or organizations, for the purposes personnel recovery as authorized by law or policy.

d. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary, to accomplish an agency function related to this system of records.

e. To the appropriate federal, state, local, territorial, tribal, or foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

f. To any component of the Department of Justice for the purpose of representing the DoD, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

g. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

h. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

i. To a member of Congress or staff acting upon the member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

j. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

k. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic storage media and paper printouts.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Name, SSN, biometric identifier (fingerprints, facial image, iris image).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system will be retained and disposed of in accordance with the records schedule approved by the National Archives and Records Administration. In general, records in the Automated Biometric Identification System are destroyed 110 years after the end of the calendar year in which the record was submitted or last updated, or when they are no longer needed for

military operations or DoD business functions, whichever is later. Destroy electronic media by shredding or degaussing; destroy paper printout by shredding or burning.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Computerized records are maintained in a controlled area accessible only to authorized personnel. Physical entry is restricted by the use of locks and guards, and is permitted only to authorized personnel. Physical and electronic access is restricted to designated individuals requiring such access in the performance of official duties. Access to computerized data is restricted by use of common access cards (CAC), and is permitted only to users with authorized accounts. The system and electronic backups are maintained within controlled facilities that employ physical restrictions and safeguards, such as security guards, identification badges, key cards, and locks.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system should address written inquiries to FOIA Officer, Defense Forensics and Biometrics Agency, DAPM-FB, 2800 Army Pentagon, Washington DC 20310-2800. The requester should provide full name, current address and telephone number, and signature. In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format: If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

CONTESTING RECORD PROCEDURES: The Army's rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 505, the Army Privacy Program, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Director, Defense Forensics and Biometrics Agency, 251 18th Street South, Suite 244, Arlington, VA 22202-3532. The requester should provide full name, current address and telephone number, and signature. In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he or she would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source. Exempt materials from other sources listed above may become part of the case records in this system of records. To the extent that copies of exempt records from other sources listed above are entered into these case records, the Department of the Army hereby claims the same exemptions, (j)(2) and (k)(2), for the records as claimed by the source systems, specifically to the extent that copies of exempt records may become part of these records from JUSTICE/FBI–019 Terrorist Screening Records System, the Department of the Army hereby claims the same exemptions for the records as claimed at their source (JUSTICE/FBI–019, Terrorist Screening Records System).

An exemption rule for this exemption has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 505. For additional information contact the system manager.

HISTORY: This system of records notice supersedes all versions previously published in the Federal Register (February 17, 2015 80 FR 8292; September 22, 2009, 74 FR 48237; April 17, 2009, 74 FR 17840; March 28, 2007, 72 FR 14534; February 25, 2005, 70 FR 9288)