Department of Defense
INSTRUCTION

NUMBER 5525.19
May 4, 2016

USD(P&R)

SUBJECT: DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB)

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5124.02 (Reference (a)), Secretary of Defense Correspondence Action Report (Reference (b)), and Annex D of the Memorandum of Understanding between the Federal Bureau of Investigation (FBI) and DoD (Reference (c)), this instruction:

a. Incorporates and cancels Directive-type Memorandum (DTM) 14-005 (Reference (d)) to update established policy and assigned responsibilities for accessing the CJI and TSDB through IMESA.

b. Provides for the use of CJI and terrorist screening information retrieved through IMESA to support the DoD physical security program in DoD Instruction (DoDI) 5200.08 (Reference (e)) and DTM 09-012 (Reference (f)); personnel security program in DoDI 5200.46 (Reference (g)); insider threat program in DoDD 5205.16 (Reference (h)); antiterrorism program in DoDI 2000.16 (Reference (i)); and maintenance of law and order on DoD installations.

c. Provides for DoD's use of CJI and terrorist screening information retrieved through IMESA for crime prevention, antiterrorism, and implementation of personnel screening to comply with Title I of Public Law (P.L.) 109-248 (Reference (j)), P.L. 101-647 (Reference (k)), and Title I of P.L. 107-56 (Reference (l)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. It is DoD policy that:

a. CJI and terrorist screening information retrieved through IMESA will be used and acted upon in accordance with established FBI procedures, by DoD law enforcement agencies.

b. Personally identifiable information (PII) collected and used in the execution of this instruction will be maintained under secure access to prevent any unauthorized use, disclosure, or loss. The collection, use, maintenance, and dissemination of PII must comply with the requirements of DoDD 5400.11, DoD 5400.11-R, DoDI 5505.17, DoDI 5400.16, and Volume 4 of DoDM 5200.01 (References (m), (n), (o), (p), and (q)).

c. Requests for exception to DoDD 5200.27 (Reference (r)) policy regarding PII of non-DoD affiliated personnel must receive an Office of the General Counsel of the Department of Defense legal review and be approved by the Deputy Chief Management Officer of the Department of Defense.

d. The standards contained in this instruction are implemented in the United States to include Alaska, Hawaii, U.S. territories and possessions, and outside the United States, in accordance with national, international, and host nation laws, and applicable agreements and arrangements with host nations.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosures 3, 4, and 5.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction is effective May 4, 2016.

Peter Levine
Acting Under Secretary of Defense
for Personnel and Readiness

Enclosures:

1. References
2. Responsibilities
3. IMESA
4. NCIC Procedures in Conjunction With IMESA
5. TSDB Procedures in Conjunction With IMESA

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES 6

ENCLOSURE 2: RESPONSIBILITIES 8

UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). 8
USD(P) 9
USD(I) 9
USD(AT&L) 10
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE (DoD CIO) 10
DoD COMPONENT HEADS 10
SECRETARIES OF THE MILITARY DEPARTMENTS 11
SECRETARY OF THE NAVY 11
CJCS 11
CCDRS 11

ENCLOSURE 3: IMESA 12

GENERAL 12
IMESA CAPABILITIES 12
CURRENT IMESA COMPONENTS 12

ENCLOSURE 4: NCIC PROCEDURES IN CONJUNCTION WITH IMESA 14

NCIC OPERATIONS 14
ADMINISTRATIVE CONTROLS 18
NCIC BASED ACCESS FITNESS ADJUDICATIONS 18

ENCLOSURE 5: TSDB PROCEDURES IN CONJUNCTION WITH IMESA 19

GENERAL 19
TSDB OPERATIONS 19
KST REDRESS PROCESS 24
ADMINISTRATIVE CONTROLS 25

GLOSSARY 26

PART I: ABBREVIATIONS AND ACRONYMS 26
PART II: DEFINITIONS 27

FIGURES

1. Handling Code 1 Caveat.....20
2. Handling Code 2 Caveat.....21
3. Handling Code 3 Caveat.....21
4. Handling Code 4 Caveat.....22

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008
(b) Secretary of Defense Correspondence Action Report, "Lead for Integrating DoD Crime Databases into a Federal System," August 2, 2005[1]
(c) Annex D, "Terrorist Screening Information," to the Memorandum of Understanding Between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities, February 22, 2012[2]
(d) Directive-type Memorandum 14-005, "DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files," April 22, 2014, as amended (hereby cancelled)
(e) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended
(f) Directive-type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, as amended
(g) DoD Instruction 5200.46, "DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)," September 9, 2014
(h) DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014
(i) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006, as amended
(j) Title I of Public Law 109-248, "Sex Offender Registration and Notification Act (SORNA) of 2006," July 27, 2006
(k) Public Law 101–647, "The Crime Control Act of 1990," November 29, 1990
(l) Title I of Public Law 107-56, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," October 26, 2001
(m) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
(n) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(o) DoD Instruction 5505.17, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities," December 19, 2012
(p) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015
(q) DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
(r) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense," January 7, 1980
(s) DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)," October 1, 2007
(t) DoD Directive 8521.01E, "Department of Defense Biometrics," February 21, 2008
(u) DoD 5200.2-R, "Personnel Security Program," January 1987, as amended
(v) Unified Command Plan 2011, April 6, 2011
(w) Homeland Security Presidential Directive 24
(x) Federal Information Processing Standards Publication 201-2, August 2013

[1] Available from the Director, Office of Law Enforcement Policy and Support, DoDHRA, 4800 Mark Center Drive, Suite 06J25-01, Alexandria, VA, 22350-4000
[2] Available by calling ASD(HD) (DCMA) at 703-697-6420

(y) National Crime Information Center, "NCIC 2000 Operating Manual," December 1999
(z) Directive-type Memorandum 15-003, "Registered Sex Offender (RSO) Identification, Notification, and Monitoring in DoD," March 26, 2015, as amended
(aa) Chapter 12 of Title 8, United States Code
(ab) Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy, current version[3]
(ac) United States Northern Command Force Protection Instruction 10-222, "USNORTHCOM Force Protection and Antiterrorism Program," September 30, 2013
(ad) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 7, 1982
(ae) Attorney General and Secretary of Defense Memorandum of Understanding on Terrorist Watchlist Redress Procedures (Redress MOU), September 19, 2007[4]
(af) National Science and Technology Council's Subcommittee on Biometrics, Biometrics Glossary, September 14, 2006[5]

[3] Available at www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center
[4] Available by calling ASD(HD) (DCMA) at 703-697-6420
[5] Available at http://biometrics.gov/Documents/Glossary.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R):

a. Oversees:

(1) In coordination with the Under Secretary of Defense for Intelligence (USD(I)), the operational maintenance, sustainment, implementation, and expansion (as applicable) of the IMESA, and its connections to authoritative data sources.

(2) Maintenance of operational and security accreditation with the FBI's Criminal Justice Information Services (CJIS) through the CJIS Advisory Policy Board process and the operational and security policies of the Terrorist Screening Center (TSC).

(3) In coordination with the USD(I), CJI and terrorist screening data retrieved by the continuous vetting process.

(4) DoD law enforcement organization access to the CJI and operational and security policies of the terrorist screening data retrieved by the continuous vetting process.

b. Maintains:

(1) Memorandums of understanding with the FBI CJIS regarding DoD's use of CJI housed in the FBI CJIS, for the IMESA process.

(2) Connectivity to and use of National Crime Information Center (NCIC) CJI database mirror image files.

(3) Memorandums of understanding with the FBI CJIS as the data broker for DoD organizations that need access to NCIC information, for the IMESA process.

(4) In coordination with the USD(I), all paperwork, reviews, and processes required for PII collected and stored within IMESA, in accordance with References (m), (n), (o), (p), and (q).

(5) In coordination with the USD(I), business rules to ensure that IMESA-derived base access decisions involving derogatory criminal or terrorist information support and align with personnel security adjudication responsibilities.

c. Develops:

(1) Tracking procedures for IMESA gained information for auditing purposes.

(2) DoD non-travel redress procedures for terrorist screening data.

(3) Training guidance and procedures for proper use and safeguards of terrorist screening data.

(4) Terrorist screening data encounter management policy in accordance with Reference (c).

d. Coordinates with:

(1) The USD(I) for oversight and maintenance responsibilities, and for changes to digital DoD personnel identity data and credentials standards that impact or require changes to personnel security and physical security programs.

(2) The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the USD(I) to make an interface available to authenticate the identities of DoD personnel with authoritative databases.

(3) The Under Secretary of Defense for Policy (USD(P)), USD(I), and USD(AT&L) regarding the use of information gained through the IMESA process for support to military operations, special events, and support activities.

2. USD(P). The USD(P):

a. Determines the use of the TSDB for military operations, force protection, and combatting terrorism.

b. Represents DoD to the FBI and other federal departments and agencies regarding DoD use of the TSDB.

c. Determines which DoD organizations are authorized access to the TSDB.

d. Coordinates with the USD(P&R), USD(AT&L), and USD(I) regarding the use of information gained through the IMESA process for military operations, special events, and support activities.

3. USD (I). The USD(I):

a. Identifies and approves the databases to be used for IMESA in support of physical access, insider threat, and security of installations and resources.

b. Provides direction for the use of IMESA supporting security and protection of installations and resources.

c. Identifies and approves federal and State issued identification cards to be used for physical access and, where required, the associated procedures and requirements for IMESA use in DoD's physical security program under Reference (e).

d. Coordinates with the USD(P), USD(P&R), and USD(AT&L) regarding the use of information gained through the IMESA process for support to military operations, special events, and support activities.

e. Coordinates with the USD(AT&L), USD(P&R), and Chief Information Officer of the Department of Defense (DoD CIO) to:

(1) Oversee the development of interface requirements and systems integration for using approved authorized authoritative databases in IMESA for security, insider threat, and intelligence programs, as applicable.

(2) Develop business rules and technical and interface requirements for DoD's Federal Personal Identity Verification Card, the Common Access Card (CAC), and other DoD ID cards for use with IMESA in accordance with Reference (e).

4. USD(AT&L). The USD(AT&L):

a. Coordinates research, development, test, and evaluation with the USD(I) and USD(P&R) in accordance with DoDI 3224.03 (Reference (s)) for IMESA.

b. Provides oversight for biometric policy, technology, and standards in accordance with DoDD 8521.01E (Reference (t)).

c. Coordinates with the USD(P), USD(P&R), and USD(I) regarding the use of information gained through the IMESA process for military operations, special events, and support activities.

5. DoD CIO. The DoD CIO provides cybersecurity and information technology policy and guidance for the IMESA, its employment, and its use with other systems to ensure protection of controlled unclassified information, compatibility, and interoperability.

6. DoD COMPONENT HEADS. The DoD Component heads:

a. Coordinate with the USD(P&R) on requirements and implementation of the IMESA.

b. Establish guidance and procedures to comply with the policy requirements contained in this instruction and implement as resources permit.

c. Ensure that privacy impact assessments are conducted in accordance with Reference (p), and that PII is collected by physical access control systems (PACS) in accordance with established privacy standards and References (m) and (n).

d. Comply with all FBI CJIS and TSC operational and security policies in the use and handling of CJI and terrorist screening data derived as part of the DoD IMESA process.

e. Ensure supplemental guidance procedures to implement the policy and processes contained in this instruction comply with and support applicable security vetting, clearance, investigation, and adjudication procedures in accordance with References (f) and (g), and DoD 5200.2-R (Reference (u)).

f. Establish an installation physical encounter protocol for known or appropriately suspected terrorists (KSTs) to ensure that installation command and supporting criminal investigative organizations are told of the encounter, subsequent direction or guidance from the FBI TSC, and disposition of the encounter.

7. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 6 of this enclosure, the Secretaries of the Military Departments coordinate the use of CJI and terrorist screening information to support the protection of DoD elements and personnel with the USD(I), CJCS, and appropriate Combatant Commanders (CCDRs).

8. SECRETARY OF THE NAVY. In addition to the responsibilities in sections 6 and 7 of this enclosure, the Secretary of the Navy operates the IMESA virtual encounter information management process for the DoD, through the Naval Criminal Investigative Service (NCIS) Multiple Threat Alert Center (MTAC), pursuant to Reference (c).

9. CJCS. In addition to the responsibilities in section 6 of this enclosure, the CJCS coordinates CCDR requirements regarding the use of CJI and terrorist screening information obtained through the IMESA process and provides recommendations to the USD(I), USD(P), and USD(P&R) for IMESA policy and program consideration.

10. CCDRs. In addition to the responsibilities in section 6 of this enclosure, the CCDRs:

a. Identify joint and interagency information and data requirements to support the IMESA; develop theater-specific operational policy and concepts of operations; and develop and integrate theater, campaign, and operational plans, pursuant to the 2011 Unified Command Plan (Reference (v)).

b. Make recommendations to the USD(P), USD(AT&L), USD(P&R), USD(I), and DoD CIO on related identity management policies regarding functional needs and systems as required. Advise on strategic, operational, and tactical lessons learned with respect to the acquisition, installation, and employment of interagency CJI and terrorist data sources and systems.

c. Work with the Joint Staff and the Service component commands to ensure provision of necessary program resources to implement the IMESA process.

ENCLOSURE 3

IMESA

1. GENERAL. In accordance with the requirements of Reference (f), the IMESA queries the PII of a DoD credentialed individual seeking access to a DoD installation against authoritative data sources of information, such as the NCIC and TSDB; and other approved authoritative databases, to identify derogatory information and determine fitness for access.

a. IMESA vets the identities of individuals who possess an authorized DoD credential and are seeking access to a military installation, and for a subsequent 5-year period or until the DoD identification card is revoked or relinquished.

b. Vetting of identities will be with biographic information and evolve to use biometric data, as resources become available, to identify and screen KSTs and other persons who pose a threat to national security, as needed in accordance with Homeland Security Presidential Directive-24 (Reference (w)).

c. PACS must be compliant with References (e) and (f) and use of Federal Information Processing Standards Publication 201-2 (Reference (x)) compliant personal identity verification (PIV) cards, including the CAC.

2. IMESA CAPABILITIES

a. The IMESA will support electronic authentication of PIV and CAC cards against the public key infrastructure certificates, verify other DoD Identification cards against the Defense Enrollment Eligibility Reporting System (DEERS), and securely access DoD authoritative and other digital identity data and information to support physical access management (i.e., credential authentication, identification card validation, and fitness determinations, where authorized and applicable).

b. Continuous vetting will be conducted against approved CJI and terrorist screening biographic information as appropriate and authorized for the populations delineated in DoD physical security policy in accordance with Reference (e). Continuous vetting information will be handled in accordance with Reference (c), normal law enforcement information handling procedures, and Reference (q).

3. IMESA COMPONENTS. The components of IMESA are:

a. Continuous Information Management Engine (CIME). The CIME provides advanced analytical vetting and matching software and its capabilities to include:

(1) Deterministic vetting.

(2) Probabilistic vetting.

(3) Global name recognition.

b. DEERS. Individuals who have accessed a DoD facility or installation will have their information populated in the CIME vetting software or system.

c. Local Population Database. Individuals with a valid reason to access the installation, who are not already recorded in DEERS, and who possess a credential authorized to facilitate access to a DoD installation in accordance with References (e) and (f), and have had their credential processed through a visitor center or PACS at least once, will have their information populated in the CIME vetting software or system.

d. CJI and Terrorist Screening Files. NCIC and TSDB are described in Enclosures 4 and 5, respectively.

e. DoD Barments. The IMESA will support the sharing of installation barment information across all the DoD Components, as appropriate. If an individual who is barred from one installation attempts to access another DoD installation, his or her barment will be visible to that second installation. The IMESA will provide this barment information upon subsequent encounter of the barred individual. A barment by one commander does not constitute authority to bar access to another installation. Commanders who elect to bar the individual from their installation must follow the requirements established in Reference (f), and consult with their legal advisor before taking any adverse action.

f. Federal and State Credentials Approved Under DoD Physical Security Policy to Facilitate Access to DoD Installations and Certificate Revocation Lists. Federal PIV cards, DoD approved PIV-interoperable cards, and the Transportation Workers Identification Credential will be authenticated against the certificate revocation lists accessed through the IMESA. Alerts on revoked credentials will be sent to the applicable PACS and appropriate action taken to deny access or grant a temporary installation pass.

g. Interoperability Layer Service (IoLS). The IoLS consists of services and software designed to connect different systems to enable information sharing. The IoLS enables data sharing among all the PACS connected to it, as well as continuous credential vetting against authoritative databases.

ENCLOSURE 4

NCIC PROCEDURES IN CONJUNCTION WITH IMESA

1. NCIC OPERATIONS

a. Performing Physical Access Control Queries Through an Installation Law Enforcement NCIC Terminal for Non-Federal Government and Non-DoD-issued Card Holders Who Are Provided Unescorted Access. Normal FBI CJIS NCIC operating procedures will be followed when using the NCIC terminal to vet visitors who do not have an authorized identification card; have not been previously vetted against NCIC as prescribed in Reference (f); and are seeking routine unescorted access to DoD installations and stand-alone facilities.

(1) NCIC inquiry message key QWI inquiries (full criminal history background checks, with no fingerprints required) are authorized for individuals identified in DoD physical security policy as not vetted.

(2) Normal installation law enforcement NCIC checks will be used to validate the currency and validity of NCIC information within prescribed times, and requires contacting the originating law enforcement agency (LEA) to determine disposition of the subject, based on information received before making an access denial decision.

b. NCIC Wanted Persons File Matches Through IMESA Continuous Vetting

(1) Matches on DoD and local population identities from the NCIC Wanted Persons File will be sent to the installation PACS through an IMESA security alert message.

(2) The IMESA does not have an automated system to notify originating jurisdictions when DoD and local population matches occur. Therefore, installations law enforcement agencies are required to follow standard NCIC 2000 Operating Manual (Reference (y)) procedures by:

(a) Running all physical encounter IMESA-obtained NCIC outstanding arrest warrant matches through an active installation law enforcement NCIC terminal to determine the currency and validity of the outstanding arrest warrant and the subject of the arrest warrant, before making an access denial decision.

(b) Contacting the outstanding arrest warrant originating law enforcement agency to determine disposition of the arrest warrant subject.

(c) Detaining the subject until disposition is resolved through arrangements for extradition or release. If detention is required beyond a reasonable time for warrant disposition or extradition, coordination should be made with a local LEA to assume responsibility for the detention.

(3) In most cases, the IMESA continuous vetting capability will alert installation LEAs to outstanding arrest warrants prior to the next physical encounter. Hit confirmation procedures for continuous vetting alerts are as follows:

(a) When the location of the individual is not known and the individual is not available to be identified in person, a hit confirmation is not required.

(b) Once an individual is encountered attempting to access the installation, the installation law enforcement agency will follow its normal NCIC hit confirmation procedures.

(4) In the case of manual adjudication of the unresolved list of active arrest warrants:

(a) At least once per shift, the installation LEA will run matches obtained from the IMESA query through its NCIC terminal (National Law Enforcement Telecommunication System or Justice Network) to verify the validity and current status of the outstanding arrest warrant.

(b) The installation LEA will determine if any of the subjects on their installation have an arrest warrant. If an individual with an arrest warrant is on the installation, organizations will detain the subject according to DoD normal law enforcement procedures. Procedures for detention beyond a reasonable period to dispose of the active warrant are described in Paragraph 1.b.(2)(c) of this enclosure.

(c) The installation LEA will make contact with the outstanding arrest warrant originating LEA to obtain disposition instructions.

(d) The installation LEA will contact the appropriate officials on the installation, determine if an individual is to be denied access, and implement the appropriate actions according to approved and codified DoD Component instructions and procedures.

(e) If a match first occurs when the individual is at an installation entry control point, the installation LEA will detain the individual in accordance with normal law enforcement procedures until a standard NCIC check is conducted.

(f) The installation LEA will follow the standard NCIC operating procedures for running a check if the match first occurs during registration at a visitor control center.

(g) If an active arrest warrant is confirmed, the installation LEA will coordinate with the personnel security office to conduct a Joint Personnel Adjudication System (JPAS) check. The appropriate command security manager for the individual will be notified for further coordination and appropriate action.

(h) The installation LEA will notify the responsible MCIO for arrest warrants related to crimes falling within MCIO jurisdiction.

c. The NCIC KST File

(1) DoD will vet population datasets against the full TSDB, rather than the NCIC KST file (a subset of the TSDB).

(2) NCIC KST hits may still be received during vetting of non-federal government and non-DoD-issued card holders who are provided unescorted access to DoD installations.

(3) Procedures for responding to KST hits on these individuals are the same as for TSDB hits and are described in Paragraph 2.d.of Enclosure 5 of this instruction.

d. The NCIC National Sex Offender Registry (NSOR) File

(1) DoD and local population datasets are periodically vetted against the NSOR file.

(2) NSOR matches will be used for identification, monitoring, and tracking DoD-affiliated personnel with sex offender convictions, not for access determinations.

(3) Legal restrictions established by the Sex Offender Registration and Notification Act (SORNA) jurisdictions on the authorized use of NSOR information narrows the scope of use of that information.

(4) The Defense Manpower Data Center (DMDC) will provide all NSOR matches to the respective military criminal investigative organizations (MCIOs) of the Military Departments or designated law enforcement agency of the Defense Agencies or DoD Field Activities with whom the identified individual is associated.

(5) Installation and facility notification will be managed and accomplished by respective MCIOs of the Military Departments or designated law enforcement agencies of the Defense Agencies in accordance with DTM 15-003 (Reference (z)).

e. Foreign Fugitive File

(1) There are two types of records in the foreign fugitive file:

(a) Canadian records containing information on persons wanted for violations of the Criminal Code of Canada based upon Canada-wide warrants.

(b) International Criminal Police Organization (INTERPOL) records containing information on persons wanted by authorities in other countries.

(2) Warrants issued in foreign countries are not executable in the United States.

(3) If an INTERPOL record identifier (i.e., ORI/DCINTER00) is received in response to an inquiry, installation law enforcement will:

(a) Contact INTERPOL's U.S. National Central Bureau (USNCB) (via the contact data provided in the return message of a positive hit on a foreign fugitive) to confirm the hit.

(b) Verify with the originating agency identifier (ORI) of the record that the warrant is still outstanding, confirm the person inquired upon is identical with the subject of the record, and obtain extradition information.

(c) Include USNCB contact information in the record response.

f. Identity Theft File

(1) The identity theft file serves as a means for a LEA to "flag" stolen identities and identify the imposter when encountered by law enforcement on DoD installations.

(2) The LEA will receive a response listing the victim profile, including the password, thereby providing the officer with the information necessary to verify that the person encountered is the victim or that the person may be using a false identity.

(3) The LEA should know that the individual cannot be arrested or detained based solely upon the information provided in the positive response from the identity theft file. The response should be considered along with additional information or circumstances surrounding the encounter before the LEA takes action.

(4) When a LEA receives a record response to an IMESA NCIC query containing identity theft information and the person inquired upon does not appear to be identical with the subject of the identity theft file record or does not know the assigned password, the inquiring agency must contact the ORI of the record to confirm the record information prior to taking official action based on the record information.

g. Immigration Violators File

(1) The immigration violator file contains records on criminals:

(a) Who have been deported for drug trafficking, firearms trafficking, or serious violent crimes and on foreign-born individuals who have violated some section of the Immigration and Nationality Act in accordance with Chapter 12 of Title 8, United States Code (Reference (aa)).

(b) Who have been deported and then reenter the United States without permission or remain in the United States after being ordered, removed, or excluded.

(2) When an LEA receives a record in response to an IMESA NCIC inquiry and the whereabouts of the person inquired upon are known and the person inquired upon appears to be identical to the subject of an Immigrations and Customs Enforcement (ICE) Agency record, the agency must confirm the alien's status with the ICE at (877) 999-5372. After confirmation, the ICE will provide direction regarding the arrest or detention of the subject.

(3) Confirmation is not required by ICE when an LEA receives a record in response to an IMESA NCIC inquiry and the whereabouts of the person inquired upon are not known.

h. Protective Order File

(1) The protective order file contains court orders that are issued to prevent acts of domestic violence against a person or to prevent a person from stalking, intimidating, or harassing another person. Orders are issued by civil and criminal State courts. It also contains military protective orders issued by a military commander.

(2) When an LEA receives a record(s) in response to an NCIC inquiry, it must confirm the hit by contacting the agency that entered the protective order to:

(a) Ensure that the person or property inquired upon is identical to the person identified in the record.

(b) Ensure that the protective order is still in effect.

(c) Obtain a decision regarding the information regarding the terms, conditions, and service of a protective order from the issuing jurisdiction or military commander.

(3) LEA will notify the installation command of the protective order.

i. Other NCIC Files. DoD IMESA access to and the use of information retrieved from other NCIC files will follow, at a minimum, the basic tenets of this issuance, normal law enforcement protocols pertinent to the file in question, and the guidelines of FBI CJIS Security Policy (Reference (ab)).

2. ADMINISTRATIVE CONTROLS. Those DoD installations and agencies that use the IMESA to access CJI will be required to follow the guidelines in Reference (ab).

a. Only personnel trained and certified to access and use NCIC information, pursuant to Reference (ab), will be authorized to handle NCIC information in the DoD IMESA process.

b. Installation and Defense Agency LEAs must retain all personnel training records for as long as the member has access to the system and up to the period of the next audit.

3. NCIC BASED ACCESS FITNESS ADJUDICATIONS

a. Fitness to enter a DoD installation, based on the receipt of derogatory CJI, will be adjudicated by trained personnel, based on Department and Military Service or Defense Agency supplemental policy.

b. The process for managing repetitive hits of derogatory CJI, in the continuous vetting process, when the subject individual has been adjudicated fit to access an installation after his or her first derogatory CJI report, will be performed at the installation level.

ENCLOSURE 5

TSDB PROCEDURES IN CONJUNCTION WITH IMESA

1. GENERAL

a. TSBD Ownership. The TSDB is maintained and operated by the TSC, a multiagency center administered by the FBI.

b. TSDB Access and Use. Pursuant to Reference (c), the DoD is authorized access to and use of TSDB records and data, as appropriate, and to the full extent permitted by law, to support its law enforcement, physical security, personnel security, insider threat, anti-terrorism, or national security vetting processes.

2. TSDB OPERATIONS

a. IMESA Integration. The TSDB is included as an authoritative government source file in the DoD IMESA process authorized by this instruction.

b. Encounter Management. DoD Components will manage information for physical and virtual encounters involving TSDB derived information.

c. Encounter Information Management

(1) DoD will operate a 24-hours-per-day, 7-days-a-week (24/7) capability to act as the FBI TSC 24/7 Watch's focal point for management of KST encounter information, pursuant to Reference (c).

(2) The NCIS MTAC performs the encounter information management function for the DoD in managing KST encounter information as described in Paragraphs d. and e. of this section.

(3) Force protection threat information collected as part of the KST encounter process may be shared with the United States Northern Command (USNORTHCOM) Law Enforcement Threat Information Cell in accordance with USNORTHCOM Instruction 10-222 (Reference (ac)). Originating LEAs control the threat information shared with USNORTHCOM.

d. Physical Encounter Process

(1) A physical encounter with a KST, at an installation access control point, will be managed by installation law enforcement, with the assistance of the appropriate MCIO as required.

(2) The TSC has identified potential terrorist suspects by labeling them with various codes that are attached to the TSB response, which is sent to the requesting LEA. Comments and contact information may also be found that will further direct response to the identified subject.

(a) Handling Code 1

1. All Handling Code 1 notifications will be handled through the PACS by installation or DoD facility LEAs at the entrance of the installation or facility.

2. Handling Code 1 Caveat will read as shown in Figure 1.

Figure 1. Handling Code 1 Caveat

This individual is associated with terrorism and is the subject of an arrest warrant, although the warrant may not be retrievable via the searched identifiers. If an arrest warrant for the individual is returned in your search of NCIC, detain the individual pursuant to your department's procedures for handling an outstanding warrant, and immediately contact the Terrorist Screening Center (TSC) at (866) 872-9001 for additional direction. If an arrest warrant for the individual is not returned, use caution and immediately contact the TSC at (866) 872-9001 for additional direction, without otherwise extending the scope or duration of the encounter. Unauthorized disclosure of terrorist watchlist information is prohibited. Do not advise this individual that they may be on a terrorist watchlist. Information that this individual may be on a terrorist watchlist is property of the TSC and is a federal record provided to your agency that may not be disseminated or used in any proceeding without the advance authorization of the TSC.

(b) Handling Code 2

1. All Handling Code 2 notifications will be sent to the applicable installation or facility LEA. The LEA will make the TSC contact. If applicable, the MCIO, Defense Agency, or Field Activity should devise guidance on the requirement to brief installation leadership or equivalent on specific investigative case factors for allowing or denying entry onto the installation or facility.

2. Handling Code 2 Caveat will read as shown in Figure 2.

Figure 2. Handling Code 2 Caveat

This individual is of investigative interest to law enforcement regarding association with terrorism and there may be a detainer available from the Department of Homeland Security for this individual. Immediately contact the Terrorist Screening Center (TSC) at (866) 872-9001 to ascertain if a detainer is available for the individual and to obtain additional direction. Please question this individual to assist the TSC in determining whether the individual encountered is the subject of a detainer without otherwise extending the scope or duration of the encounter. Unauthorized disclosure of terrorist watchlist information is prohibited. Do not advise this individual that they may be on a terrorist watchlist. Information that this individual may be on a terrorist watchlist is property of the TSC and is a federal record provided to your agency that may not be disseminated or used in any proceeding without the advance authorization of the TSC.

(c) Handling Code 3

1. All Handling Code 3 notifications will be sent to the applicable installation or facility LEA. The LEA will make the TSC contact. If applicable, the MCIO, Defense Agency, or Field Activity should devise guidance on the requirement to brief installation leadership or equivalent on specific investigative case factors for allowing or denying entry onto the installation or facility.

2. Handling Code Caveat 3 will read as shown in Figure 3.

Figure 3. Handling Code 3 Caveat

Do not advise this individual that they may be on a terrorist watchlist. Contact the Terrorist Screening Center (TSC) at (866) 872-9001 during this encounter. If this would extend the scope or duration of the encounter, contact the TSC immediately thereafter. Attempt to obtain sufficient identifying information during the encounter, without otherwise extending the scope or duration of the encounter, to assist the TSC in determining whether or not the name or identifier(s) queried belongs to an individual identified as having possible ties with terrorism. Do not detain or arrest this individual unless there is evidence of a violation of federal, State, or local statutes. Unauthorized disclosure is prohibited. Information that this individual may be on a terrorist watchlist is the property of the TSC and is a federal record provided to your agency only for intelligence and lead purposes. This record, and any information contained within it, may not be disclosed or used in any proceeding without the advance authorization of the TSC.

(d) Handling Code 4

1. All Handling Code 4 notifications will be sent to the applicable Service MCIO, Defense Agency, or Field Activity. The MCIO, Defense Agency, or DoD Field Activity will make the TSC contact. If applicable, the MCIO, Defense Agency, or Field Activity should devise guidance on the requirement to brief installation leadership or equivalent on specific investigative case factors for allowing or denying entry onto the installation or facility.

2. Handling Code 4 Caveat will read as shown in Figure 4.

Figure 4. Handling Code 4 Caveat

Do not advise this individual that they may be considered a person who may be of national security interest. Contact the Federal Bureau of Investigation (FBI) at (866) 872-9001 during this encounter. If this would extend the scope or duration of the encounter, contact the FBI immediately thereafter. Attempt to obtain sufficient identifying information during the encounter, without otherwise extending the scope or duration of the encounter, to assist the FBI in determining whether or not the name or identifier(s) you queried belongs to an individual identified as a former military detainee. Do not detain or arrest this individual unless there is evidence of a violation of federal, State, or local statute(s). Unauthorized disclosure is prohibited. Information that this individual may be a person who may be of national security interest is the property of the FBI and is a federal record provided to your agency only for intelligence and lead purposes. This record, and any information contained within it, may not be disclosed or used in any proceeding without the advance authorization of the FBI.

(3) When using the NCIC terminal to vet individuals requesting entry, the direction provided by the returned handling code will be followed at the point of encounter. In addition:

(a) Under no circumstances will the individual be advised that he or she may be on a terrorist watch list.

(b) Encounter information will be provided to the respective Installation Commander, Military Service, Defense Agency, or DoD Field Activity and United States Northern Command, under prescribed reporting procedures.

(c) Encounter information regarding U.S. persons provided to defense intelligence components will be handled in accordance with DoD 5240.1-R (Reference (ad)).

(d) Denial of entry will be accomplished in a manner that does not inform the individual that he or she may be in the NCIC KST file.

(4) Installation LEAs will provide installation command and supporting criminal investigative organizations immediate notification of the KST physical encounter, subsequent direction or guidance from the FBI TSC, and disposition of the encounter.

(5) DMDC will provide the MTAC a parallel notification of the KST information returned to the installation as an IMESA TSDB match.

(6) Installation law enforcement will provide final disposition information of the KST physical encounter to the MTAC.

e. Virtual Encounter Process

(1) A virtual encounter with a KST will be managed by the NCIS MTAC.

(2) DMDC will provide the virtual encounter "hit" to NCIS MTAC for action.

(3) NCIS MTAC will:

(a) Contact the FBI TSC with the KST information.

(b) Receive and act on FBI TSC guidance and requests for further information.

(c) Conduct necessary analysis on the KST information.

(d) Notify the appropriate MCIO or supporting LEA with KST information.

(4) The MCIO or supporting LEA will:

(a) Notify installation and facility command and LEA of KST information and guidance provided by FBI TSC and NCIS MTAC.

(b) Support command in accomplishment of actions requested by FBI TSC while ensuring consideration for the installation commander's force protection concerns.

(c) If MCIO, notify the organization's liaison officer at the National Joint Terrorism Task Force Military Operations Support Team.

(5) Installation or facility commands will determine appropriate actions to be taken based on guidance received, law enforcement resources available, and maintenance of security of the installation or facility.

(6) Installation or facility commands will report disposition of any actions taken through the installation's MCIO or LEA to the NCIS MTAC.

(7) DoD notification must include all available PII identifiers concerning the individual collected during the encounter to enable TSC to make a final adjudication.

(8) If the TSC determines that an individual does not match a TSDB record, the TSC will advise the NCIS MTAC. TSC will retain an electronic record of all referrals from DoD in its encounter management database in accordance with existing retention schedules for this system.

(9) If the TSC determines that an individual is a positive or inconclusive match, the TSC will immediately notify the FBI's Terrorist Screening Operations Unit (TSOU). TSOU will coordinate the proper operational response, if any, between the DoD, the FBI, the nominating agency, and other relevant agencies or entities. This will not restrain or delay any immediate operational response that the DoD Components may take in rare or emergency circumstances to further the immediate security.

(10) After the operational response has been coordinated, the DoD will share with TSC the results of any actions taken during an encounter with the positive or inconclusive TSDB match (e.g., denial of entry to military installations).

(11) For all positive and inconclusive matches, terrorist identity information is shared via the IoLS so that the DoD and FBI may update their respective systems accordingly.

3. KST REDRESS PROCESS

a. General. The KST redress process provides for a timely and fair review of individuals' complaints and the identification and correction of any errors in the TSDB. It consists of two parts. The first part covers redress for individuals nominated to the KST watchlist by the DoD. The second part covers redress for individuals discovered to be a KST through the DoD IMESA process.

b. DoD Nominated Individuals. Redress adjudication for individuals nominated as a KST by DoD will be performed by the Defense Combating Terrorism Center, Defense Intelligence Agency (DIA), pursuant to Attorney General-DoD Redress Memorandum of Understanding (Reference (ae)). The Defense Combating Terrorism Center will coordinate directly with the National Counterterrorism Center for adjudications.

c. KST Physical and Virtual IMESA Hit Individuals

(1) At no time during the physical or virtual KST encounter process will the subject of the KST hit be notified, directly or indirectly, that he or she is on the KST watch list. A redress process cannot be based on an individual's knowledge of being a KST.

(2) Redress and the redress process for IMESA generated KSTs will be keyed to negative adjudications for access to a DoD installation or facility and be available to individuals for that purpose only. DMDC will establish and manage an automated redress process for this purpose.

(3) Redress for other negative adjudications (i.e., fitness for duty, suitability for security clearance) will occur through the redress processes established by functional communities responsible for managing those adjudications.

4. ADMINISTRATIVE CONTROLS. Those DoD installations and agencies that receive IMESA-accessed TSDB information will be required to follow the guidelines in Reference (c).

a. Only personnel trained and certified to access and use TSDB information, pursuant to Reference (c), will be authorized to handle TSDB information in the DoD IMESA process.

b. Installation and Defense Agency LEAs must retain all personnel training records for as long as the member has access to the system and up to the period of the next audit.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CAC	common access card
CCDR	Combatant Commander
CIME	Continuous Information Management Engine
CJCS	Chairman of the Joint Chiefs of Staff
CJI	criminal justice information
CJIS	Criminal Justice Information Services
DEERS	Defense Enrollment Eligibility Reporting System
DIA	Defense Intelligence Agency
DMDC	Defense Manpower Data Center
DoD CIO	Chief Information Officer of the Department of Defense
DoDD	DoD Directive
DoDHRA	DoD Human Resources Activity
DoDI	DoD Instruction
DTM	Directive-type memorandum
FBI	Federal Bureau of Investigation
ICE	Immigrations and Customs Enforcement
INTERPOL	International Criminal Police Organization
IMESA	Identity Matching Engine for Security and Analysis
IoLS	interoperability layer service
JPAS	Joint Personnel Adjudication System
KST	known or appropriately suspected terrorist
LEA	law enforcement agency
MCIO	military criminal investigative organization
MTAC	Multiple Threat Alert Center
NCIC	National Crime Information Center

NCIS	Naval Criminal Investigative Service
NSOR	National Sex Offender Registry
ORI	originating agency identifier
PACS	physical access control system
PII	personally identifiable information
PIV	personal identity verification
P.L.	Public Law
SORNA	Sex Offender Registration and Notification Act
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSOU	FBI Terrorist Screening Operations Unit
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USNORTHCOM	United States Northern Command

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this instruction.

applicant. An individual requesting physical access to a facility or installation.

application. A hardware or software system implemented to satisfy a particular set of requirements.

barment. Denial of access to a DoD installation.

biographic information. Facts of, or relating to, a person that assert and support the establishment of the person's identity. The identity of U.S. citizens is asserted by their social security number and given name. Other biographic information may include, but is not limited to, identifying marks such as tattoos and birthmarks.

biometrics. A general term used alternatively to describe a characteristic or a process.

As a characteristic: A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.

As a process: Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics in accordance with U.S. Government National Science and Technology Council's Subcommittee on Biometrics Glossary (Reference (af)).

certificate revocation list. A list which pairs individuals with their digital certificate status and enumerates revoked certificates, along with the reasons for revocation.

deterministic vetting. Data matching based on a direct data correlation.

federal PIV. A physical artifact issued by the Federal Government to an individual that contains a photograph, cryptographic keys, and a digitized fingerprint representation so that the claimed identity of the card holder can be verified by another person (human readable and verifiable) or a computer system (readable and verifiable). This card is conformant with the standards prescribed in Reference (g).

fitness. Level of character and conduct determined necessary for the basis of physical access control decisions.

force protection threat information. Defined in Reference (ac).

global name recognition. The ability to look for variations in multi-cultural name spellings to determine matches.

hit. Information received in return from an inquiry into a CJI or terrorist screening information system.

hit confirmation. Verifying the validity of the information received from an NCIC Wanted Persons File inquiry - the identity of the individual, the currency of the arrest warrant, and the disposition of the individual (extradition or release).

identity proofing. The process of providing or reviewing federally authorized acceptable documentation for authenticity.

IMESA. An application that continuously vets identities against authoritative data sources to support fitness determinations for installation access, and law and order on installations.

KST hits. The return of information from an NCIC KST File inquiry identifying the subject of the inquiry as a KST.

local population database. Data collected and maintained from all individuals with a valid reason to access the installation, who are not already recorded in DEERS, and who possess a credential authorized to facilitate access to a DoD installation in accordance with Reference (s), and have had their credential processed through a visitor center or PACS at least once.

physical access control. The process of physically controlling personnel and vehicular entry to installations, facilities, and resources.

physical security. That part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. Designed for prevention and provides the means to counter threats when preventive measures are ignored or bypassed.

PII. Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, and other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual alone, or when combined with other personal identifying information.

probabilistic vetting. Data matching based on certain criteria, characteristics, or thresholds.

QWI inquiry. An NCIC inquiry message which provides the authorized user with the capability to access both the Interstate Identification Index (for criminal history) and NCIC simultaneously with one inquiry.

screening. The physical process of reviewing a person's presented biographic and other identifiable information, as appropriate, to determine its authenticity and authorization, and to conduct credential verification against a government data source through authorized and secure channels at any time during the person's period of physical access eligibility. This assessment identifies derogatory actions that can be determined as disqualifying issues for current or continuing physical access eligibility standards and requirements for the resource, asset, or installation.

TSDB. The U.S. Government's authoritative consolidated database that contains terrorist identifiers concerning individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism or terrorist activities.

TSDB encounter. An event in which an individual is identified to be a Positive Match, a Potential Match, or an Inconclusive Match to an individual who has been designated in the TSDB as a KST.

TSDB physical encounter. A face-to-face meeting with a KST at an installation access control point.

TSDB virtual encounter. An electronic match (i.e., the individual identified as a KST has submitted their DoD identification at some point in the past, is now in the subscribed population, and an electronic match is produced during the periodic machine-to-machine identity matching).

Transportation Workers Identification Credential. Transportation Security Administration issued identification credential for access to secure areas of the nation's maritime facilities and vessels.

vetting. An evaluation of an applicant's or a card holder's character and conduct for approval, acceptance, or denial for the issuance of a physical access control credential.