

UNDER SECRETARY OF DEFENSE 4000 DEFENSE PENTAGON WASHINGTON, D.C. 20301-4000

PERSONNEL AND READINESS

> April 22, 2014 Incorporating Change 1, May 13, 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS CHAIRMAN OF THE JOINT CHIEFS OF STAFF UNDER SECRETARIES OF DEFENSE DEPUTY CHIEF MANAGEMENT OFFICER DIRECTOR, COST ASSESSMENT AND PROGRAM **EVALUATION** DIRECTOR. OPERATIONAL TEST AND EVALUATION GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE ASSISTANT SECRETARIES OF DEFENSE DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER ASSISTANTS TO THE SECRETARY OF DEFENSE DIRECTOR, ADMINISTRATION AND MANAGEMENT DIRECTOR, NET ASSESSMENT DIRECTORS OF THE DEFENSE AGENCIES DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-type Memorandum (DTM) 14-005 – DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files

References: See Attachment 1.

<u>Purpose</u>. In accordance with the authority in DoD Directive (DoDD) 5124.02 (Reference (a)) and Secretary of Defense Correspondence Action Report (Reference (b)), this DTM:

- Establishes DoD policy for accessing Federal Bureau of Investigation (FBI) NCIC Files through IMESA.
- Provides for the use of NCIC information retrieved through IMESA for controlling entry to DoD installations in order to implement section 1069 of Public Law 110-181 (Reference (c)) and maintaining law and order on DoD installations.
- Provides for the use of NCIC information retrieved through IMESA for crime prevention in order to implement Title I of Public Law 109-248 (Reference

(d)), Public Law 101–647 (Reference (e)), and Title I of Public Law 107-56 (Reference (f)).

- Implements these standards within the United States to include Alaska, Hawaii, U.S. territories and possessions, and outside the United States, in accordance with host nation laws and Combatant Command guidance.
- This DTM is effective April 22, 2014; it must be converted to a new DoD instruction (DoDI). This DTM will expire effective April 22, 2015 2016.

<u>Applicability</u>. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff 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 Department of Defense (referred to collectively in this DTM as the "DoD Components").

Definitions. See Glossary.

<u>Policy</u>. It is DoD policy that:

- DoD Components will meet the physical and procedural access requirements established in this DTM, and identify mitigation measures for those instances when the minimum standards cannot be met.
- Criminal justice information (CJI) retrieved through IMESA will be used and acted upon in accordance with existing law enforcement procedures.
- Personally identifiable information (PII) collected and utilized in the execution of this DTM must be maintained under secure access to prevent any unauthorized use, disclosure, or loss. DoD Components will ensure that the collection, use, maintenance, and dissemination of PII complies with the requirements of DoDD 5400.11, DoD 5400.11-R, DoDI 5505.17, and DoDI 5400.16 (References (g), (h), (i), and (j)).
- Exception requests to DoD Directive 5200.27 (Reference (k)) must receive a DoD OGC legal review and be approved by the Director, Administration and Management.
- These standards are implemented in the continental United States to include Alaska, Hawaii, U.S. territories and possessions, and outside the United States in accordance with host nation laws, international agreements, and geographic Combatant Commander guidance.

Responsibilities. See Attachment 2.

Procedures. See Attachments 3 and 4.

<u>Releasability</u>. Unlimited. This DTM is approved for public release and is available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.

right

Acting Under Secretary of Defense for Personnel and Readiness

Attachments: As stated

ATTACHMENT 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, 2005¹
- (c) Section 1069 of Public Law 110-181, "National Defense Authorization Act for Fiscal Year 2008," January 28, 2008
- (d) Title I of Public Law 109-248, "Sex Offender Registration and Notification Act of 2006," July 27, 2006
- (e) Public Law 101–647, "The Crime Control Act of 1990," November 29, 1990
- (f) 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
- (g) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, as amended
- (h) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (i) 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
- (j) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009
- (k) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- (1) DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 19, 2004, as amended
- (m) DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)," October 1, 2007
- (n) DoD Directive 8521.01E, "Department of Defense Biometrics," February 21, 2008
- (o) Defense Federal Acquisition Regulation Supplement, current edition
- (p) DoD 5200.2-R, "Personnel Security Program," January 1987, as amended
- (q) Directive-type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, as amended
- (r) Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- (s) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 7, 1982
- (t) Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy, current version²
- (u) Section 552 of Title 5, United States Code

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 at www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

(v) National Science and Technology Council's Subcommittee on Biometrics, Biometrics Glossary, September 14, 2006³

³ Available at http://biometrics.gov/Documents/Glossary.pdf

ATTACHMENT 2

RESPONSIBILITIES

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

a. Oversees operational maintenance, sustainment, implementation, and expansion (as applicable) of the IMESA, and its connections to authoritative data sources.

b. Oversees:

(1) Maintenance of operational and security accreditation with the FBI's Criminal Justice Information Services (CJIS) through the CJIS Advisory Policy Board process.

(2) Criminal Justice Information (CJI) retrieved by the continuous vetting process.

(3) DoD law enforcement organization access to the CJI retrieved by the continuous vetting process.

c. Maintains:

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

(2) Connectivity to and use of NCIC CJI database mirror image files.

(3) The FBI CJIS as the data broker for other DoD organizations that need access to NCIC CJI data through establishment of memorandums of understanding.

(4) All paperwork, reviews, and processes required for PII collected and stored within IMESA, in accordance with References (g) and (h).

(5) Business rules to ensure that IMESA-derived base access decisions consider and align with personnel security responsibilities.

d. Uses data from the Defense Enrollment and Eligibility Reporting System (DEERS), including but not limited to biographic and biometric information, in accordance with DoDD 1000.25 (Reference (1)).

e. Coordinates with:

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

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

(3) The Under Secretary of Defense for Policy (USD(P)) for activities regarding military operations, special events, and support activities.

f. Provides:

(1) The IMESA Web-based Query capability for authorized users to conduct query searches against all the information contained in the IMESA to obtain criminal, terrorist, security, credential, and debarment data for their area of responsibility.

(2) A capability to log and track all hits in the IMESA and individuals who query the IMESA for auditing purposes.

2. $\underline{\text{USD}(I)}$. The USD(I):

a. Incorporates any updates to physical access control programs, processes, and systems, as required to implement the IMESA.

b. Coordinates with the USD(AT&L) and the USD(P&R) to:

(1) Provide oversight of the development of interfaces associated with controlling physical access as it relates to connecting approved, authoritative databases to the IMESA.

(2) Develop technical and interface requirements for card issuance, revocation notification, and system interoperability with physical access control systems (PACS) and the interoperability layer service (IoLS).

c. Coordinates with the USD(P) for activities regarding military operations, special events, and support activities

3. $\underline{\text{USD}(\text{AT\&L})}$. The $\underline{\text{USD}(\text{AT\&L})}$:

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

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

c. In coordination with the USD(I) and USD(P&R), develops the IoLS and IMESA capabilities to share identity data worldwide with authorized DoD installations to support PACS to authenticate approved credentials and an individual's authorization and fitness to enter.

d. Maintains the Defense Federal Acquisition Regulation Supplement (Reference (o)) as required to address access to FBI NCIC files through the DoD IMESA for the purpose of controlling entry by contractors to DoD installations.

e. Coordinates with the USD(P) for activities regarding military operations, special events, and support activities

4. <u>DoD CHIEF INFORMATION OFFICER (DoD CIO</u>). The DoD CIO provides identity management strategy and information technology policy and guidance that provide DoD Components automated capabilities to verify and authenticate identities, credentials, and an individual's fitness.

5. <u>DoD COMPONENT HEADS</u>. The DoD Component heads:

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

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

c. Ensure that privacy impact assessments are conducted in accordance with Reference (f), and that PII is collected by PACS in accordance with established privacy standards and References (g) and (h).

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

e. Ensure that procedures to implement processes in this DTM support established security clearance procedures in accordance with DoD 5200.2-R (Reference (p)).

6. <u>CHAIRMAN OF THE JOINT CHIEFS OF STAFF</u>. In addition to the responsibilities in section 5 of this attachment, the Chairman of the Joint Chiefs of Staff coordinates Combatant Commander requirements regarding these policy standards and provides recommendations to the USD(P&R) for policy and program consideration.

7. <u>COMBATANT COMMANDERS</u>. In addition to the responsibilities in section 5 of this attachment, the Combatant Commanders:

a. Identify joint and interagency information and data requirements to support the IMESA; development of theater-specific operational policy and concepts of operations; and development and integration of theater, campaign, and operational plans.

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

c. Coordinate identity management policy and acquisition programs that support the protection of DoD elements and personnel in their area of responsibility with the Secretaries of the Military Departments.

d. Identify, document, validate, prioritize, and submit to the Joint Staff the resource requirements necessary to achieve IMESA program objectives.

e. Work with the Joint Staff and the Service component commands to ensure provision of necessary program resource requirements.

ATTACHMENT 3

IMESA

1. <u>GENERAL</u>. In accordance with Reference (c) and DTM-09-012 (Reference (q)), the IMESA continuously vets the identities of everyone applying for or possessing a credential authorized to facilitate access to a DoD installation worldwide against authoritative data sources, such as the NCIC and the Terrorist Screening Database (TSDB), to determine if they are fit to enter.

a. Vetting of identities will start with biographic information and eventually evolve to include biometric data.

b. The PACS will support a DoD-wide and federally interoperable physical access control capability compliant with Homeland Security Presidential Directive-12 (Reference (r)).

2. IMESA CAPABILITIES

a. The IMESA will enable PACS to rapidly, electronically, and securely access authoritative digital identity data/information to support physical access management (i.e., access enrollment, credential verification, authorization, fitness assessment, and secure information sharing).

b. The IMESA will enable PACS to rapidly, electronically, and securely access authoritative digital identity data and information to support physical access management (e.g., access enrollment, credential verification, authorization, fitness assessment, and secure information sharing).

c. Continuous vetting will be conducted against authorized NCIC files. The informational products of the continuous vetting will be handled according to normal law enforcement procedures.

3. <u>CURRENT IMESA COMPONENTS</u>. The current components of IMESA are:

a. <u>Continuous Information Management Engine</u>. Advanced analytical vetting and matching software and its capabilities include but are not limited to:

(1) Deterministic vetting.

(2) Probabilistic vetting.

(3) Global name recognition.

b. <u>DEERS</u>. Data from individuals in DEERS with a credential authorized to facilitate access (active duty, retirees, dependents, civilians, U.S.-sponsored foreign military who possess a DoD identification card) will have information populated in the vetting software or system.

- c. Local Population Database
- d. NCIC File

e. <u>DoD Bars</u>. The IMESA will enable the sharing of installation bar information across all the Military Services. 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. It will be up to other installation commanders to determine whether they will also bar the individual from their respective installations and take the appropriate legal steps, as applicable.

f. <u>Non-DoD Credentials Approved to Facilitate Access to DoD Installations Credential</u> <u>Revocation Lists</u>. Certificate revocation lists for non-DoD federal personal identity verification (PIVs), DoD approved PIV-I's, and the transportation workers identification credential will be continuously vetted in the IMESA. Alerts on revoked credentials will be sent to the applicable PACS so installations can take the appropriate actions.

g. <u>IoLS</u>. The IoLS consists of services and software designed to connect different systems together to enable the sharing of information. The IoLS enables data sharing among all the PACS connected to it, as well as continuous credential vetting against authoritative databases.

- h. IMESA Query Tool
- i. IMESA Visualization Dashboard

(1) Through the Visualization Dashboard, the Defense Manpower Data Center (DMDC), under the authority, direction, and control of the Director, DoD Human Resources Activity (DoDHRA), will track and audit all NCIC felony arrest warrants obtained from the wanted persons mirror image file.

(2) The Visualization Dashboard provides a geo-spatial, near real time alerting and tracking capability of all the alerts retrieved by the IMESA. Specifically, it:

- (a) Displays all alerts occurring in the analytical vetting software.
- (b) Displays accuracy scores of each alert.
- (c) Provides links to additional information on each alert.
- (d) Provides the ability to track the routing of an alert from the IoLS to an

installation.

(e) Displays alerts occurring at installations or PACS geo-spatially in near

real time.

(f) Provides access to the visualization dashboard through a secure webbased interface.

(3) Access to the Visualization Dashboard will be limited to organizations with authorized access to NCIC data, i.e., agencies with an FBI Originating Agency Identifier (ORI). Other organizations and individuals seeking dashboard access will submit their request and access justification through DMDC to the Director, Law Enforcement Policy and Support, DoDHRA.

ATTACHMENT 4

NCIC PROCEDURES IN CONJUNCTION WITH IMESA

1. NCIC OPERATIONS

a. <u>Performing Physical Access Control Queries Through NCIC Terminal for Non-federal</u> <u>Government and Non-DoD-issued Card Holders Who Are Provided Unescorted Access</u>. Normal FBI CJIS NCIC operating procedures will be followed when using the NCIC terminal to vet visitors seeking unescorted access to DoD installations and stand-alone facilities. This includes validating the currency and validity of the outstanding arrest warrant with NCIC within prescribed times, and contacting the outstanding arrest warrant originating law enforcement agency to determine disposition of the arrest warrant subject.

b. <u>NCIC Wanted Persons File Matches Through IMESA Continuous Vetting</u>. The IMESA searches numerous authoritative data sources to continuously vet DoD and installation local populations in order to provide DoD officials with the most up to date information in making informed physical access control decisions.

(1) Matches on DoD and local population identities from these authoritative data sources 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 are required to:

(a) Run all IMESA-obtained NCIC outstanding arrest warrant matches through an active NCIC terminal to determine the currency and validity of the outstanding arrest warrant.

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

(3) In most cases, the IMESA continuous vetting capability will alert installation law enforcement to outstanding arrest warrants before the individual in question is physically present. No hit confirmation will be necessary for an individual matched solely by the IMESA continuous vetting capability, when the location of the individual is not known and the individual is not available to be identified in person. Once an individual is encountered attempting to access the installation, installation law enforcement will follow normal NCIC hit confirmation procedures.

(4) The query tool allows authorized users to conduct searches against all the information contained in the IMESA to obtain criminal, terrorist, security, credential, and debarment data for their area of responsibility.

(5) Additionally, this query method provides a manual method to obtain advance information regarding the installation's population so authorized law enforcement agencies can proactively search for terrorist, criminal, or security threats.

(6) Manual adjudication will include the following procedures:

(a) At least once per shift, authorized organizations from each installation will run matches obtained from the IMESA query through the NCIC terminal to verify validity and currency of the outstanding arrest warrant.

(b) Authorized organizations 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 locally approved law enforcement procedures.

(c) Authorized organizations will make contact with the outstanding arrest warrant originating law enforcement agency to obtain disposition instructions.

(d) Authorized organizations will contact the appropriate officials on the installation and determine if the individual is going to be barred, and implement the appropriate actions according to locally approved and codified instructions and procedures.

(e) Should a match first occur when the individual is at an installation entry control point, the individual will be detained according to locally approved law enforcement procedures until a standard NCIC check is conducted.

(f) Should the match first occur during registration at a visitor control center, standard NCIC operating procedures for running checks will be followed.

(g) If the appropriate officials on the installation determine the individual is going to be barred, a Joint Personnel Adjudication System (known as "JPAS"), check should be conducted. If the person has or had applied for a security clearance, the appropriate security manager shall be notified.

c. <u>NCIC Matches For Installations Without an NCIC Terminal</u>. Some DoD installations and agencies do not have connection to an NCIC terminal; therefore, they will utilize the IMESA Web Based Query Tool to check installation and agency DoD and local populations against the NCIC Felony Wants and Warrants File. Installations will check the IMESA for NCIC felony wants and warrants at least once every 24 hours.

(1) When matches occur through the query tool, the installation law enforcement activity must run the matched names a second time through an NCIC terminal within 4 hours of the initial match and follow standard NCIC procedures.

(2) This validation check through an NCIC terminal may require DoD installations and agencies to develop memorandums of agreement with local law enforcement agencies or other nearby installations that have access to an NCIC terminal. Once a match is

validated, authorized installation law enforcement personnel will contact the originating agency to determine disposition.

(3) Each installation without a PACS is required to upload its local population database and to provide updates (e.g., additions, deletions, or changes) of local population records at least once every 24 hours.

(4) This procedure will provide the IMESA information on personnel that are part of the segment of the installation's population not maintained in the DEERS database and provide the installation the most up to date information on inquiries regarding the local population segment.

(a) The IMESA Query Tool web link may be provided by DMDC, upon request.

(b) Users will use this web link to request system access and obtain user

training.

d. The NCIC Known or Appropriately Suspected Terrorist (KST) File

(1) DoD and local population datasets are continuously vetted against the KST

file.

(2) There are three KST File Handling Codes. The Terrorist Screening Center (TSC) has identified potential terrorist suspects by labeling them with various codes that are then attached to the NCIC response which is sent to requesting law enforcement agencies. Comments and contact information may also be found that will further direct response to the identified subject.

(a) <u>Handling Code 1</u>

 $\underline{1}$. All Handling Code 1 notifications (identified by a red light) will be handled by the PACS or installation law enforcement at the entrance of the installation or DoD facility.

<u>2</u>. This code will read: "Approach with caution. The individual is the subject of an arrest warrant. If a warrant is returned, detain the individual pursuant to normal procedures and immediately contact the TSC (1-866-872-9001). If a warrant is not returned, use caution and immediately contact the TSC for additional direction without otherwise extending the scope and duration of the encounter."

(b) <u>Handling Code 2</u>

<u>1</u>. All Handling Code 2 notifications (identified by a yellow light) will be sent to the applicable Service Military Criminal Investigative Organization (MCIO), Defense Agency, or DoD Field Activity. The MCIO, Defense Agency, or Field Activity

will make the TSC contact. If applicable, the MCIO, Defense Agency, or Field Activity should devise policy on the requirement to brief installation leadership or equivalent and factors of allowing or denying entry onto the installation or facility.

<u>2</u>. This code will read: "Approach with caution. There may be a detainer available from the Department of Homeland Security for this individual. Immediately contact the TSC (1-866-872-9001) to ascertain if a detainer is available. Please question the individual to assist the TSC in identifying the individual without otherwise extending the scope or duration of the encounter."

(c) <u>Handling Code 3</u>

<u>1</u>. All Handling Code 3 notifications (identified by a green light) will be sent to the applicable Service MCIO, Defense Agency, or Field Activity. The MCIO, Defense Agency, or Field Activity will make the TSC contact. If applicable, Service MCIOs, Defense Agencies, or Field Activities should devise policy on the requirement to brief installation leadership or equivalent and factors of allowing or denying entry on to the installation or facility.

<u>2</u>. This code will read: "Approach with caution. Contact the TSC (1-866-872-9001) 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 extending its scope or duration. Do not detain or arrest this individual unless there is evidence of a violation of federal, State, or local statutes."

(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 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 according to DoD 5240.1-R (Reference (s)).

(d) Barment will be accomplished so that the individual does not become aware that he or she may be in the NCIC KST File.

(4) NCIC KST matches through IMESA continuous vetting will follow guidance provided in section 1 of this attachment.

(5) NCIC matches through the IMESA Query Tool will follow guidance provided in section 3 of Attachment 3.

(6) Administrative controls for other NCIC files will follow guidance provided in section 4 of Attachment 3.

e. 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.

(3) Legal restrictions on the authorized use of NSOR information narrows the scope of use of that information.

(4) DMDC will provide all NSOR matches to the respective 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 notification will be managed and accomplished by the approved organizations for each Service as codified in writing by the Director, Law Enforcement Policy and Support, DoDHRA.

(6) Use of the IMESA Query Tool will be limited to those organizations with authorized access to NCIC data, i.e., agencies with an FBI ORI.

(7) A separate policy issuance will be published to govern policy and procedures for identification, monitoring, and tracking of DoD affiliated personnel with sex offender convictions.

f. <u>Other NCIC Files</u>. IMESA access to and the use of information retrieved from other NCIC files will follow, at a minimum, the basic tenants of this issuance, normal law enforcement protocols, and the guidelines of FBI CJIS Security Policy (Reference (t)).

2. <u>ADMINISTRATIVE CONTROLS</u>. Those DoD installations and agencies that use the IMESA query tool will be required to follow the guidelines in Reference (t), similar to the guidelines for having an actual NCIC terminal. Only trained and certified personnel with authorization to access NCIC information will be allowed query tool access.

a. Each installation will designate in writing an authorized organization and list of individuals to conduct the IMESA Web Based Query and provide the information to DMDC. DMDC will maintain the master list of these individuals. Installations will also send any updates to the organization or individual list as they occur.

b. The following guidelines also apply:

(1) The system will be configured to allow access only to authorized users.

(2) DMDC and the agency using the system must retain audit records for at least 365 days. Once the minimum retention time period has passed, DMDC and the agency will continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, but is not limited to, retention and availability of audit records relative to subpoenas, law enforcement actions, and requests made in accordance with section 552 of Title 5, United States Code (Reference (u)) (also known as the "Freedom of Information Act").

(3) The agency must retain all personnel training records for as long as the member has access to the system and up to the period of an audit.

<u>GLOSSARY</u>

PART I. ABBREVIATIONS AND ACRONYMS

CJI	criminal justice information
CJIS	Criminal Justice Information Services
DEERS	Defense Enrollment Eligibility Reporting System
DMDC	Defense Manpower Data Center
DoD CIO	DoD Chief Information Officer
DoDHRA	DoD Human Resource Activity
DoDI	DoD instruction
DoDD	DoD directive
DTM	directive-type memorandum
FBI	Federal Bureau of Investigation
IMESA	Identity Management Capability Enterprise Services Application
IoLS	interoperability layer service
JPAS	Joint Personnel Adjudication System
KOT	
KST	known or appropriately suspected terrorist
MCIO	military original investigative organization
MCIO	military criminal investigative organization
NCIC	National Crime Information Center
NSOR	National Sex Offender Registry
ORI	Originating Agency Identifier
PACS	physical access control system
PII	personally identifiable information
PIV	personal identity verification
PIV-I	personal identity verification-interoperable

TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
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

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this DTM.

<u>access control list</u>. A list containing, at a minimum, the names of individuals authorized access and their subsequent authorities of sponsorship (e.g., privileges, times and dates for access, unescorted or escorted designation). In an electronic PACS, these items are logically stored in the PACS database.

<u>access credential</u>. A physical artifact issued by the federal, State, or local government that attests to one's right to credit or authority. The access credential contains and depicts characteristics, authorizations, and privileges for physical access and internal security controls.

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

<u>application</u>. A hardware or software system implemented to satisfy a particular set of requirements.

<u>architecture</u>. A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability, and federal, State, or local laws).

<u>authentication</u>. A process that matches presented information to the established origin of that information.

<u>biographic information</u>. 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, U.S. Government National Science and Technology Subcommittee on Biometrics Glossary, Reference (v).

barment. Denial of access to a DoD installation.

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

<u>federal PIV</u>. 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 (p).

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

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

<u>identity proofing</u>. The process of providing or reviewing federally authorized acceptable documentation for authenticity.

<u>IMESA</u>. A system that continuously vets identities against authoritative data sources to determine fitness.

<u>IMESA Query Tool</u>. A web based capability that allows authorized users to conduct data query searches against all the information contained in the IMESA.

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

<u>NCIC Mirror Image File</u>. A mirror image copy of the NCIC Wanted Persons File that will be continuously updated. Initially the IMESA will search for felony arrest warrants and misdemeanor arrest warrants for domestic violence. Subsequently, the file will expand the arrest warrant scope and bring on additional NCIC files, as applicable.

<u>physical access control</u>. The process of physically controlling personnel and vehicular entry to installations, facilities, and resources. Access will be either unescorted or escorted.

<u>physical security</u>. 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.

<u>PII</u>. Information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specific individual.

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

<u>screening</u>. 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.

<u>TSDB</u>. 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.

<u>vetting</u>. 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.