UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-5000

December 8, 2009
Incorporating Change 9, August 23, 2018

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control"

References: See Attachment 1

Purpose. In accordance with (IAW) the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), this DTM establishes DoD access control policy and the minimum DoD security standards for controlling entry to DoD installations and stand-alone facilities (hereafter referred to as installations) to implement section 1069 of Public Law 110-181 (Reference (b)).

- These standards and their implementation status shall be reported to Congress as required and the standards shall be implemented in the continental United States (CONUS) to include Alaska, Hawaii, its territories, and possessions no later than October 1, 2010, as resources, law, and capabilities permit.

- This DTM is effective ~~immediately~~ *December 8, 2009*, and shall be incorporated into DoD 5200.08-R (Reference (c)) and DoD Instruction (DoDI) 5200.08 (Reference (d)). This DTM shall expire effective ~~February 28, 2018~~ *February 28, 2019*.

Applicability. This DTM applies to OSD, the Secretaries of 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 with the Department of Defense (hereafter referred to collectively as the "DoD Components").

Definitions. See Glossary.

Policy. It is DoD policy that:

- Procedures for installation access shall be implemented using the minimum standards as outlined in this DTM.

- Access control standards shall include identity proofing, vetting to determine the fitness of an individual requesting and/or requiring access to installations, and issuance of local access credentials.

    - Documents listed in Attachment 4 of this DTM from the Department of Homeland Security Form I-9, "Employment Eligibility Verification" (see

http://www.dhs.gov/xabout/gc_1186413412271.shtm), will be used for identity proofing.

- Fitness of persons will be determined by U.S. Government (USG) personnel analysis and assessment of information obtained through USG authoritative data sources outlined in this DTM prior to being authorized unescorted access to installations.

- Reciprocal physical access for DoD-issued card holders is authorized in this DTM to non-controlled and/or non-restricted DoD installations unless otherwise determined by the installation commander and/or director. Installation commanders may limit reciprocal physical access based upon, but not limited to, local security requirements, increased force protection condition (FPCON) levels, emergencies, and contingencies.

- DoD-issued card holders as identified and authorized in this DTM should not be required to re-register at each installation (appropriate to their authorization for access) unless access is restricted and/or controlled based upon, but not limited to, higher security levels, increased FPCONs, or in compliance with local security requirements.

- The DoD minimum standard for controlling access at an entry point to an installation shall be implemented as delineated in this DTM.

- All unescorted persons entering DoD installations must have a valid purpose to enter, have their identity proofed and vetted, and be issued, or in possession of, an authorized and valid access credential.

- Physical access control systems (PACSs) shall be reviewed for their capability to support current legacy components, future architectural requirements, and support interoperability across the Department of Defense.

- Maximum use of approved commercial off-the-shelf technology solutions is encouraged.

- PACSs shall include capabilities to provide for a greater level of security in depth, as defined in Reference (c), and be scalable.

- Additional security measures shall be applied based on type of installation, security level, category of individuals, FPCONs, and level of access to be granted.

- DoD Components should meet the physical access requirements established in this DTM, to the maximum extent possible, for special events, circumstances, and activities, and identify mitigation measures for those instances when the minimum standards cannot be met.

- Personally identifiable information (PII) collected and utilized in the execution of this DTM must be safeguarded to prevent any unauthorized use, disclosure, and/or loss. DoD Components shall ensure that the collection, use, and release of PII complies with the requirements of DoDD 5400.11, DoD 5400.11-R, and DoDI 5400.16 (References (e), (f), and (g)).

Responsibilities. See Attachment 2.

Procedures. See Attachments 3 and 4. Attachment 3 provides guidance for installation physical access control. Attachment 4 provides guidance for authorized DoD identification and identity proofing documents.

Releasabilty. **Cleared for public release**. This DTM is available on ~~the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.~~ *the Directives Division Website at http://www.esd.whs.mil/DD/.*

James R. Clapper, Jr.

Attachments:
As stated

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

ATTACHMENT 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," ~~November 23, 2005~~ *October 24, 2014, as amended*
(b) Section 1069 of Public Law 110-181, "National Defense Authorization Act for Fiscal Year 2008," January 28, 2008
(c) DoD 5200.08-R, "Physical Security Program," April 9, 2007*, as amended*
(d) DoD Instruction 5200.08, "Security of DoD Installations and Resources *and the DoD Physical Security Review Board (PSRB)*," December 10, 2005*, as amended*
(e) DoD Directive 5400.11, "DoD Privacy Program, ~~May 8, 2007~~ *October 29, 2014*
(f) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(g) DoD Instruction 5400.16, "DoD Privacy Act Assessment (PIA) Guidance," ~~February 12, 2009~~ *July 14, 2015*
(h) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information *(SCI)*," ~~October 9, 2008~~ *April 21, 2016*
(i) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
(j) ~~DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000~~ *DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015*
(k) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
(l) DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RTD&E)," October 1, 2007
(m) DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," ~~December 5, 1997~~ *January 23, 2014*
(n) Federal Information Processing Standards Publication 201-1, "Personal Identity Verification for Federal Employees and Contractors," March 2006
(o) DoD Instruction 8510.01, ~~"DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007~~ *"Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended*

ATTACHMENT 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Establish a working group under the DoD Physical Security Review Board that is chaired by the Physical Security Division Chief to address privacy, security, and physical access control issues for the protection of personnel, information, resources, and installations. The working group will:

(1) Include, at a minimum, representation from the DoD Components, Physical Security Equipment Action Group (PSEAG), the Joint Security Chief Council, the Defense Privacy Office (DPO), and Service security expertise.

(2) Establish physical security access control standards and other physical access control related guidance consistent with policy and approved published standards to support interoperability.

(3) Recommend policy to manage physical access authorizations or denials for personnel entering their facilities.

b. Establish policy regarding the collection, reporting, processing, storage, retention, redress, and destruction of information concerning individuals or organizations not affiliated with the Department of Defense or governed by DoDI 5200.01 (Reference (h)) and DoDD 5200.27 (Reference (i)). Policy will also address requirements and applicable laws under References (e) through (g) and ~~DoDD 5015.2~~ *DoDI 5015.02* (Reference (j)), as appropriate.

c. Coordinate with the Under Secretary of Defense for Policy (USD(P)) and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) to support the conduct of vulnerability and balanced survivability assessments of physical access control programs, processes, and systems, as required.

d. Coordinate with the USD(AT&L) and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)):

(1) To provide oversight of the development of interfaces associated with controlling physical access.

(2) To develop technical and interface requirements for card issuance, revocation notification, and system interoperability with PACSs.

(3) On identification card topology and physical security features (e.g., holograms) to ensure compliance with resource, information security, and protection requirements.

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

a. Coordinate with the USD(I) to establish and provide an interface to the Foreign Visitor System – Confirmation Module (FVS-CM) to provide information on and confirm foreign visitor authorizations to visit DoD locations including research, development, test, and evaluation (RDT&E) sites, all DoD Components, DoD contractor sites, and other sensitive DoD facilities, pursuant to DoDD 5230.20 (Reference (k)).

b. Review physical security measures under FPCON levels to ensure compliance with this DTM.

3. USD(AT&L). The USD(AT&L) shall:

a. Coordinate RDT&E with the USD(I) in accordance with DoDI 3224.03 (Reference (l)) for electronic physical access control and related systems.

b. Provide biometrics technology support for physical security applications as required in accordance with References (c) and (l).

c. In coordination with the USD(I) and USD(P&R), develop middleware interface capability to electronically verify enrollment of persons in authoritative databases.

4. USD(P&R). The USD(P&R) shall:

a. Coordinate with the USD(I) and USD(AT&L) to make available an interface to authenticate the identities of DoD personnel with authoritative databases.

b. Coordinate with the USD(I) for changes to credentials that impact or require changes to physical security programs.

5. ~~ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/~~DoD CHIEF INFORMATION OFFICER (~~ASD(NII)/~~DoD CIO). The ~~ASD(NII)/~~DoD CIO shall coordinate with USD(I), USD(AT&L), and USD(P&R) to identify identity management requirements and IT solutions that provide DoD Components automated capabilities to verify and authenticate identities and identity credentials used in PACs.

6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Coordinate with the USD(I) on the security of DoD installations and resources in accordance with Reference (a), (c), and (d).

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

c. Ensure that privacy impact assessments are conducted in accordance with Reference (g).

7. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff shall coordinate Combatant Commander requirements regarding these policy standards and provide recommendations to the USD(I) for policy and program consideration.

ATTACHMENT 3

PHYSICAL SECURITY ACCESS CONTROL STANDARDS

1. ACCESS CONTROL. Access control is designed to restrict and/or control entrance to property and/or installations to only those authorized persons and their conveyances. Persons authorized access shall be either escorted or unescorted. Commanders or directors will employ personnel access control measures at an installation perimeter to enhance security and protection of personnel, resources, and installations.

2. PROOFING AND VETTING. The access control standards shall include identity proofing; determining the fitness of an individual requesting and/or requiring access to DoD facilities; and vetting.

a. Federal personal identity verification (PIV) and DoD-issued card holders require identity proofing and vetting to determine fitness and eligibility for access.

(1) Persons possessing a DoD-issued Common Access Card (CAC) are vetted to DoD Personnel Security standards in subparagraphs 2.a.(1)(a) and (b) of this attachment and shall be considered identity proofed.

(a) DoD Civilian Personnel and/or Contractors. National Agency Check with Inquiries (NACI) or Office of Personnel Management (OPM) Tier I standards, when implemented.

(b) DoD Military Personnel. National Agency Check with Law and Credit or OPM Tier II standards, when implemented.

(2) Persons possessing a DoD-issued card IAW DoDI 1000.13 (Reference (m)) are identity proofed at card issuance sites from federally authorized identity documents and shall be considered identity proofed.

(3) Persons possessing Federal PIV credentials that conform to Reference (h) are vetted and adjudicated by Government security specialists on NACI or OPM Tier I standards, when implemented, and shall be considered identity proofed.

(4) The Transportation Worker Identification Credential (TWIC) holders vetting, adjudication, and issuance process is comparable to the NACI and/or National Agency Check with Law and Credit or, when implemented, OPM Tier I standard, and shall be considered identity proofed.

(5) Vetting and adjudication for persons receiving USG identification credentials as listed in subparagraphs 2.a.(1), (3), and (4) of this attachment occurs prior to permanent card

issuance. Persons in possession of these identification cards and/or credentials shall be considered vetted for unescorted access for the purposes of this DTM.

(6) Determination of fitness and vetting for DoD-issued identification and privilege cards (subparagraph 2.a.(2) of this attachment) should not be required for unescorted access, as the issuing office verifies the individual's direct affiliation with the Department of Defense, or a specific DoD sponsor, and eligibility for DoD benefits and entitlements.

b. Non-Federal Government and non-DoD-issued card holders who are provided unescorted access require identity proofing and vetting to determine fitness and eligibility for access.

(1) Persons requesting access shall provide justification and/or purpose for access to DoD facilities.

(2) Persons requesting access that are not in possession of an approved, Government issued card shall provide a document listed in Attachment 4. The documents presented shall be reviewed by an authorized Government representative for the purposes of identity proofing.

(3) The local commander and/or director shall determine the recurring requirement and frequency for additional checks of non-Federal Government and non-DoD-issued card holders based upon local security requirements using Government authoritative databases only as prescribed herein.

(4) Installation government representatives shall query the following government authoritative data sources to vet the claimed identity and to determine fitness, using biographical information including, but not limited to, the person's name date of birth, and social security number:

(a) The National Crime Information Center (NCIC) database.

(b) The Terrorist Screening Database.

(c) Other sources as determined by the DoD Component or the local commander and/or director. These can include but are not limited to:

1. Department of Homeland Security (E-Verify).

2. Department of Homeland Security (U.S. VISIT).

3. Department of State Consular Checks (non-U.S. citizen).

4. The FVS-CM.

(5) Only personnel delegated by the installation commander shall perform access control duties that include:

(a) Identity proofing.

(b) Vetting and determination of fitness.

(c) Access authorizations and privileges.

(6) Installation personnel will issue the appropriate card and/or pass, as authorized.

c. Commander(s) and/or directors(s) of installations are authorized to conduct random proofing and vetting on persons requiring access to their assigned installations, as necessary and appropriate.

3. MINIMUM STANDARDS FOR CONTROLLING PHYSICAL ACCESS TO INSTALLATIONS

a. The DoD minimum standard for controlling physical access to an installation shall be:

(1) Where electronic PACSs are not appropriate due to limited access control or mission requirements, a physical and visual inspection of cards as authorized in this DTM shall be conducted by security forces and/or guards at physical entry and/or access control points. This inspection includes:

(a) Visual match of the photograph on the card to the person presenting the identification.

(b) Comparison and visual review of the card for unique topology and security design requirements. The visual check of the card will include verifying authenticity by checking the anti-counterfeit and/or fraud protection measures embedded in the credential.

(2) When funding becomes available, installations will procure an electronic PACS that provides the capability to rapidly and electronically authenticate credentials and individuals authorization to enter an installation. The PACS must support a DoD-wide and federally interoperable access control capability that can authenticate USG physical access credentials and support access enrollment, authorization processes, and securely share information.

b. Types of access include:

(1) Unescorted individuals.

(2) Escorted individuals.

c. Other considerations for controlling access include, but are not limited to:

(1) Escort qualifications, responsibilities, and authorizations.

(2) Sponsorship qualifications, responsibilities, and authorizations.

(3) Access privileges at each security level and each FPCON.

(4) Mission-essential employee designation, if applicable.

(5) Emergency response designation, if applicable.

(6) Day and time designation for access.

(7) Locations authorized for access.

d. DoD Components should provide reciprocal physical access to installations for DoD-issued card holders authorized by this DTM. Commanders may limit reciprocal physical access based upon, but not limited to, local security requirements, increased FPCON levels, and emergencies.

e. DoD Components may incorporate a DoD defined Trusted Traveler procedure for use during FPCONs NORMAL, ALPHA, and BRAVO into their implementation policy as local security conditions permit. The Trusted Traveler procedure is governed and implemented locally and is not recognized from installation to installation.

(1) The Trusted Traveler procedure allows a uniformed service member or Government employee with a valid CAC, a military retiree (with a valid DoD identification credential), or an adult dependent (with a valid DoD identification credential) to present their identification token for verification while simultaneously vouching for any vehicle occupants. The number of personnel a Trusted Traveler is allowed to vouch for and/or sponsor at any one time will be determined by the local installation commander or their designated representative.

(2) Members identified as Trusted Travelers are responsible for the actions of all occupants for whom they vouch and for meeting all security requirements for escort as established by the Service or installation commander.

4. PACS AND COMPONENTS

a. In order to meet the DoD goal of enhancing security for DoD installations, personnel, information, and resources, PACSs and their components shall:

(1) Query government authoritative data sources for the vetting of persons requiring access.

(2) Support DoD-wide and Federal Government-wide interoperability for Federal PIV IAW Reference (g).

(3) Validate and authenticate government issued identification.

(4) Integrate with other physical security systems and equipment.

b. In addition to the security systems goals outlined in subparagraphs 4.a.(1) through (4) of this attachment, PACSs and associated components:

(1) Shall be reviewed for their capability to support legacy PACSs and components.

(2) Shall provide for scalable capabilities.

(3) Shall provide a secure capability to query and receive information to vet individuals seeking access to installations by checking an individual's biographic information against government authoritative data sources and watch lists to determine an individual's fitness and eligibility for access. Biometrics may be added to the biographic information check when infrastructure, capability, and resources are available and mission requirements dictate their use.

(4) Shall provide a capability to exchange controlled information across the physical security enterprise with other USG security, law enforcement, and intelligence sources.

(5) Shall provide the capability to report and to receive information for revoked, lost, or stolen identification cards, debarments, restricted persons, and other information pertaining to the security and protection of DoD installations, persons, and resources.

(6) Shall provide capability to check Federal PIV and DoD-issued cards to verify their authenticity and for electronic authentication against physical access control lists in the PACS database.

(7) Shall provide capability to maintain local logging and reporting of persons enrolled in PACS, entering the installation, and denied access.

(8) Shall provide capability to store an updated access control list every 12 hours (or dependent on local requirements), which can be accessed offline by authorized security personnel during losses of communication to PACS databases.

(9) Shall read contact and contactless technology IAW the Federal Information Processing Standards Publication 201-1 (Reference (n)). Contactless technology will be the primary technology used, as it provides for more rapid throughput and supports less wear and tear on the reader and the card.

(10) Shall provide capability to take, store, and forward to guard stations a facial image and/or digital photograph obtained during registration to perform visual match of the person presenting the credential, card, or pass.

(11) Shall comply with the requirements of DoDI 8510.01 (Reference (o)) regarding certification and accreditation.

(12) Shall include an emergency power source.

(13) May provide capability to interface with Service vehicle registration systems, as appropriate.

(14) May provide capability to match the biometric presented (i.e., facial image, and fingerprint) to the individual and to the vetted claimed identity in the PACS.

(15) May provide keypad for personal identification number (PIN) usage or for additional levels of security.

(16) May provide capability to incorporate radio frequency identification tags technology.

(17) Should provide a capability to support two-factor authentication (visual, mechanical, and/or electronic) to provide higher levels of assurance, as dictated by risk, cost, or when otherwise required.

5. ADDITIONAL SECURITY REQUIREMENTS. DoD Components may authorize additional security requirements based upon the type of installation, security level, category of individuals requiring access, FPCONs, and level of access to be granted, as necessary. Installation commanders and/or directors will determine local requirements for personnel under the age of 18 who require non-recurring access and are not in possession of an authorized identification or identity source documents listed in this DTM.

6. SPECIAL EVENTS, CIRCUMSTANCES, OR ACTIVITIES. Requirements for physical access for special events, circumstances, or activities shall be determined in the implementation policy of the DoD Components and will include compensatory measures when the requirements of the DTM cannot be met.

7. LOCAL EMERGENCY RESPONSE/ASSISTANCE. Procedures for local emergency first responders' physical access requirements shall be developed and implemented by installation commanders.

ATTACHMENT 4

IDENTITY PROOFING DOCUMENTS AND AUTHORIZED IDENTIFICATION

1. ACCEPTABLE IDENTIFICATION DOCUMENTS. Applicants will provide a valid and original form of identification from those listed in section 2 of this attachment for the purpose of proofing identity for enrollment into a PACS or issuance of a visitor pass. Prior to acceptance, personnel processing an applicant will screen documents for evidence of tampering, counterfeiting, or other alteration. Documents that appear questionable (e.g., having damaged laminates) or otherwise altered will not be accepted. Altered documents will be held until appropriate authorities are notified, and disposition procedures are authorized.

2. ACCEPTABLE IDENTITY SOURCE DOCUMENTS. All documents must be current.

a. U.S. passport or U.S. passport card.

b. Permanent resident card or Alien Registration Receipt Card (INS Form I-551).

c. Foreign passport with a temporary (I-551) stamp or temporary (I-551) printed notation on a machine readable immigrant visa.

d. Foreign passport with a current arrival-departure record (INS Form I-94) bearing the same names as the passport and containing an endorsement of the alien's nonimmigrant status, if that status authorizes the alien to work for the employer.

e. Employment authorization document that contains a photograph (INS Form I-766).

f. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with INS Form I-94 or INS Form I-94A bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, as long as the endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form.

g. Driver's license or identification card issued by a State or outlying possession of the United States, provided it contains a photograph and biographic information such as name, date of birth, gender, height, eye color, and address.

h. Identification card issued by Federal, State, or local government agencies, provided it contains a photograph and biographic information such as name, date of birth, gender, height, eye color, and address.

i. School identification card with a photograph.

j. U.S. Military or draft record.

k. U.S. Coast Guard Merchant Mariner Card or TWIC.

l. Native American tribal document.

m. For persons under the age of 18 who are unable to present a document listed in paragraphs 2.a. through m. of this attachment:

(1) School record or report card.

(2) Day care or nursery school record.

(3) Birth certificate.

3. AUTHORIZED IDENTIFICATION TO FACILITATE PHYSICAL ACCESS

a. Identification documents authorized to facilitate physical access to installations include:

(1) The DoD CAC.

(2) DoD Uniformed Services Identification and Privileges Cards issued in accordance with Reference (m).

(3) USG-issued, authenticated Federal PIV credentials.

(4) TWIC.

b. For other persons requiring unescorted access, installation commanders shall use locally produced, temporary issue, visitor identification. Commanders must ensure that an expiration date and time group is assigned to these temporary credentials.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

~~ASD(NII)/~~ DoD CIO	~~Assistant Secretary of Defense for Networks and Information Integration/~~DoD Chief Information Officer
CAC	Common Access Card
CONUS	continental United States
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DPO	Defense Privacy Office
DTM	Directive-Type Memorandum
FPCON	force protection condition
FVS-CM	Foreign Visitor System – Confirmation Module
IAW	in accordance with
NACI	National Agency Check with Inquiries
NCIC	National Crime Information Center
OPM	Office of Personnel Management
PACS	Physical Access Control System
PII	personally identifiable information
PIN	personal identification number
PIV	personal identity verification
PSEAG	Physical Security Equipment Action Group
RDT&E	research, development, test, and evaluation
TWIC	Transportation Workers Identification Credential
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
USG	United States Government

PART II. DEFINITIONS

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

access control. See "physical access control."

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

access credential. 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/or depicts characteristics, authorizations, and privileges for physical access and internal security controls.

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

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

architecture. 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).

authentication. A process that matches presented information to the established origin of that information.

biographic information. Facts of, or relating to, a person that asserts and/or supports the establishment of their 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, birthmarks, etc.

biometrics. A general term used to alternatively describe a characteristic or process. Stored electronic information pertaining to a biometric can be in terms of raw or compressed pixels, or in terms of some characteristic (e.g., patterns).

controlled area. A controlled space extending upward and outward from a specified point. Installations are generally considered controlled areas for the purposes of national defense. Commanders and/or directors may further designate controlled areas within an installation based upon geographic attributes and unit dispersal. Controlled areas generally designate areas wherein sensitive operations occur or controlled unclassified and sensitive information is stored and access is limited to specific persons.

DoD issued card. Cards (other than the DoD CAC) authorized by Reference (m) of this DTM.

escorted individuals. Persons who require access, without determination of fitness, who must be accompanied by a sponsor with authorization to escort the individual. The escort requirement is mandated for the duration of the individual's visitation period.

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 (n).

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

identity proofing. The process of providing or reviewing federally authorized acceptable documentation (INS Form I-9) for authenticity.

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

physical electronic security system interoperability. The ability of two or more systems or components to exchange information or electronic data and to use the information that has been exchanged.

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.

Physical Security Access Control Identity and Information Management System. A system comprised of one or more systems or applications that controls the ability of people or vehicles to enter a protected area by means of visual, manual, or electronic (or a combination of the three) authentication and authorization at entry points, and manages identity information for controlling physical access to eligible, authorized persons.

PII. Information that can be used to distinguish or trace an individual's identity, such as their 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.

reciprocal physical access. Mutual recognition of physical access privileges granted by an installation commander.

restricted access area. An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry and/or movement. Restricted areas are designated and authorized by the installation and/or activity commander and/or director, properly posted, and employ multiple physical security measures.

screening. The physical process of reviewing a person's presented biographic and other identifiable information, as appropriate, to determine their authenticity, authorization, and credential verification against a government data source through authorized and secure channels at anytime 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.

security in depth. A combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force. Examples include the use of perimeter fences, employee and visitor entry and/or exit controls, sensors and intrusion detection systems, closed circuit video monitoring, security patrols during working and non-working hours, or other safeguards that mitigate vulnerabilities.

Trusted Traveler. A procedure that allows for uniformed service members and spouses, DoD employees, and retired uniformed service members and spouses to vouch for occupants in their immediate vehicle, provided the Trusted Traveler vehicle operator possess a valid identification card and has a clear NCIC check. Trusted Travelers are entirely responsible for the actions of all occupants in their vehicle and for meeting all local security requirements for escort as established by requirements of the installation commander. Additional implementation guidance will be incorporated into physical security policy.

unescorted individuals. Personnel who have been identity proofed and favorably vetted in accordance with this DTM are eligible for unescorted access within the installation; but are, however, still subject to any controlled or restricted area limitations, as appropriate.

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