



Department of Defense

DIRECTIVE

NUMBER 1000.25

July 19, 2004

Certified Current as of April 23, 2007

USD(P&R)

SUBJECT: DoD Personnel Identity Protection (PIP) Program

- References:
- (a) DoD Directive 1000.22, "Uniformed Services Identification Cards," October 8, 1997 (hereby canceled)
 - (b) DoD Instruction 1000.23, "DoD Civilian Identification Cards," December 10, 1998 (hereby canceled)
 - (c) DoD Directive 1341.1, "Defense Enrollment and Eligibility Reporting (DEERS)," May 21, 1999 (hereby canceled)
 - (d) DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," December 5, 1997
 - (e) through (v), see enclosure 1

1. PURPOSE

This Directive:

1.1. Cancels references (a), (b), and (c), and establishes policy and assigns responsibility under the DoD Personnel Identity Protection (PIP) Program. The PIP shall be the Department of Defense's program for: addressing threats to the individual personal privacy of its Members, employees, and beneficiaries; establishing a secure and authoritative process for the issuance and use of identity credentials in the Department of Defense; and ensuring that DoD benefits and access to DoD physical and logical assets are granted based on authenticated and secure identity information.

1.2. Establishes policy for the implementation and operation of the PIP program to include use of authoritative identity information, issuance and use of DoD identity credentials, and operation of the Defense Enrollment and Eligibility Reporting System (DEERS), Real-time Automated Personnel Identification System (RAPIDS) and associated systems, Defense Biometric Identification System (DBIDS), Defense Cross-Credentialing Identification System (DCCIS), Defense National Visitors Center (DNVC), and the Defense Non-Combatant Evacuation (NEO) Operations Tracking System (DNNTS).

1.3. Renames the Identity Management Senior Coordinating Group as the Identity Protection and Management Senior Coordinating Group (IPMSCG) and establishes joint oversight of the IPMSCG.

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to the Office of the Secretary of Defense (OSD), the Uniformed Services, the Chairman of the Joint Chiefs of 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 in the Department of Defense, (hereafter referred to collectively as the "DoD Components").

2.2. This Directive also applies to the Commissioned Officers Corps of the U.S. Public Health Service under agreement with the Department of Health and Human Services; and the Commissioned Officers Corps of the National Oceanic and Atmospheric Administration under agreement with the Department of Commerce.

2.3. This Directive does not apply to civilian employees of the Intelligence Community (e.g., National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, and National Reconnaissance Office) unless their appropriate personnel data have been submitted and verified in DEERS.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Issuance of DoD identity credentials shall be accomplished using authentication of identity. The RAPIDS is used to issue the definitive credential of affiliation with the Department of Defense. It relies on the information stored in DEERS. The information stored in DEERS, provided by the DoD Components, shall remain the definitive data source of identity and the verification of affiliation with the Department of Defense. Once issued, the DoD credential shall serve as the definitive assertion of identity and shall be authenticated against the DEERS database, global directory services, or DoD PKI services in real time whenever possible. The DEERS/RAPIDS infrastructure shall be used for identity operations under the purview of the PIP. The granting of logical and physical access privileges remains a local policy and business operation function of the local facility, but must function in concert with PIP policy and procedures. RAPIDS shall perform the following functions:

4.1.1. Authenticate individuals to ensure that DoD identification credentials are provided only to those with a current and appropriate affiliation with the Department of Defense.

4.1.2. Capture uniquely identifying characteristics that bind an individual to the identity information maintained on that individual in DEERS and to the identification credentials issued by RAPIDS. These characteristics shall include, but are not limited to, digital photographs and fingerprints. DEERS shall be the sole authoritative repository for storing these characteristics. The DoD Components shall avoid updating and maintaining redundant repositories without a compelling justification.

4.1.3. Provide a distinct identification credential for use as proof of identity and DoD affiliation and may act as the Geneva Convention Card in accordance with DoD Instruction 1000.13 (reference (d)) and as an authorization card for Uniformed Services' benefits and privileges.

4.2. The Department of Defense shall distribute authorized benefits and entitlements as prescribed in reference (d), DoD Directive 1322.16, DoD Instruction 1322.17, 10 U.S.C. Chapter 55, DoD *Instruction* 1330.9, and DoD Directive 1330.17 (references (e) through (i)). The DEERS is designated as the automated information system to provide timely and accurate information on those eligible for these benefits and entitlements, to prevent and detect fraud and abuse in the distribution of these benefits and entitlements, and is the definitive centralized person data repository of identity and enrollment and eligibility verification data on members of the DoD Components, members of the Uniformed Services, and other personnel as designated by the Department of Defense, and their eligible family members. The DEERS shall collect and maintain other additional data on individuals, as needed, to ensure the efficient administration of DoD missions. The DEERS person data repository is protected by, and shall be maintained in accordance with the Privacy Act of 1974 (reference (j)), as implemented by DoD Directive 5400.11 and 45 C.F.R. Parts 160 and 164, "Health and Human Services Privacy Rule" (references (k) and (l)). DEERS shall perform the following:

4.2.1. Maintain enrollment and eligibility verification data from existing DEERS client applications and interfacing systems, as well as the DoD Components and non-DoD information systems in accordance with DoD Directive 8000.1 (reference (m)). The Defense Manpower and Data Center shall create/modify interfaces with personnel repositories to increase the timeliness of data synchronization to real-time data sharing with source DoD data repositories wherever feasible.

4.2.2. Provide statistical and demographic data to support the DoD Components' peacetime and wartime missions.

4.2.3. Maintain casualty identification information and medical and personnel readiness information on Uniformed Services and other personnel as designated by the Department of Defense.

4.2.4. Serve as the personal data repository for generating Uniformed Service sponsor and family member benefits, entitlements, and identification credentials.

4.2.5. Serve as the National Enrollment Database for the Military Health System benefits eligibility and TRICARE enrollments for medical care services.

4.2.6. Maintain current and past eligibility information on Uniformed Service members, family members, and retirees for Government educational program eligibility in accordance with references (e) and (f) and serve as the Department of Defense's centralized personnel locator in accordance with 10 U.S.C. 113 (reference (n)).

4.2.7. Maintain unique identifying information associated with a person to authenticate identity and affiliation of DoD credential holders. These characteristics shall include, but are not limited to digital photographs and fingerprints.

4.3. The PIP Program shall use emerging technologies to support the protection of individual identity and to safeguard DoD physical assets and logical systems from unauthorized access based on fraudulent or fraudulently obtained credentials. Further, identification credentials shall be authenticated to ensure that they are currently valid and issued to the individuals presenting them, whenever possible.

4.3.1. Oversight for the PIP program shall be from the IPMSCG. The IPMSCG shall be a cohesive DoD-wide policy recommendation, requirements, strategy, and oversight group for managing the physical and virtual identities of all our personnel, support contractors, business partners, and other entities consistent with the Global Information Grid Architecture. It shall focus on Federal Sector and Department-wide interoperability standards, performance matrices; ways to exploit identity management tools as means for enhancing readiness, business processes, and security; and being cognizant of protecting entities' identifiable information. The following are examples of systems that meet PIP criteria:

4.3.1.1. DBIDS is a fully configurable force protection system and shall serve as a physical access control and critical property registration system. DBIDS implements the policies outlined in DoD *Instruction* 5200.08 and DoD Directive 8190.3 (references (o) and (p)) and is an approved system under the PIP. DBIDS is authorized to issue DoD identity credentials to those individuals needing physical access and not otherwise credentialed under reference (d).

4.3.1.2. The DNVC is the system for DoD facilities to authenticate DoD credential-carrying visitors using a web-based connection. DNVC is available to DoD law enforcement and force protection elements and is recognized as an approved system under the PIP.

4.3.1.3. The DCCIS shall provide mutual authentication of issued identity credentials between participating Federal Agencies and private sector business partners. Use of a federated identity system for recognition of credentials shall strengthen the security of the Department of Defense. DCCIS is an approved system under the PIP.

4.3.1.4. The Defense NEO DNTS assists the Combatant Commanders and the Joint Task Force Commanders during NEOs by providing a rapid registration and tracking system for evacuees. NTS satisfies the requirements of DoD Instruction 1400.32 and DoD Directive 3025.14 (references *(q)* and *(r)*).

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) shall:

5.1.1. Develop policy for the PIP, including minimum acceptable criteria for establishment and confirmation of personal identity, policy for the issuance of the DoD enterprise personnel identity credentials, and approve additional systems under the PIP.

5.1.2. Act as the Principal Staff Assistant for DEERS, RAPIDS, and the PIP program in accordance with DoD Directive 5000.1 (reference *(s)*), and appoint the Designated Approving Authority in accordance with DoD Directive 8500.1 (reference *(t)*) for all PIP systems.

5.1.3. Jointly with the Assistant Secretary of Defense (Network and Information Integration) (ASD(NII))/DoD Chief Information Officer (CIO) oversee the newly formed IPMSCG.

5.1.4. Establish other user groups, as necessary, composed of members of the DoD Components to advise on PIP systems.

5.2. The Deputy Under Secretary of Defense For Program Integration, under the USD(P&R) shall:

5.2.1. Develop policies and procedures for the oversight, funding, personnel staffing, direction, and functional management of the PIP.

5.2.2. Oversee other user groups, as established by USD(P&R).

5.2.3. Coordinate with the Principal Deputy Under Secretary of Defense for Personnel and Readiness, the Assistant Secretary of Defense for Health Affairs, and the Assistant Secretary of Defense for Reserve Affairs on changes to enrollment and eligibility policy and procedures pertaining to personnel, medical, and dental issues that impact on the PIP.

5.2.4. Develop policies and procedures to support the functional requirements of PIP, DEERS, and the DEERS client applications and interfacing client systems.

5.2.5. Secure funding in support of new requirements to support the PIP or the enrollment and eligibility functions of DEERS/RAPIDS.

5.3. The Director, Defense Manpower Data Center, under the USD(P&R) shall:

5.3.1. Provide the technical and functional management of the PIP Program, DEERS, and other PIP systems and maintain the standards for identity transaction interfaces.

5.3.2. Operate PIP systems as designated.

5.3.3. Serve as the authoritative source for identity confirmation.

5.3.4. Assign and maintain the unique, non-Social Security Number-based identifiers on DoD affiliated individuals.

5.4. The Under Secretary of Defense (Intelligence) shall:

5.4.1. Provide a Joint Personnel Adjudication System interface for DEERS for the exchange of relevant clearance identity information on DoD affiliated personnel.

5.4.2. Oversee the implementation of the PIP for all physical access locations throughout the Department of Defense.

5.5. The Assistant Secretary of Defense (Network and Information Integration) (ASD(NII))/DoD CIO shall:

5.5.1. Provide a source for digital certificates for linkage to the identity credentials to improve the functionality of PIP systems, as required.

5.5.2. Jointly oversee the IPMSCG.

5.5.3. Oversee the implementation of the PIP for all logical access throughout the Department of Defense.


5.6. The Heads of the DoD Components shall:

5.6.1. Comply with the provisions of this Directive and provide timely and accurate personnel information from their definitive personnel systems to DEERS.

5.6.2. Ensure RAPIDS operators, authorized to issue DoD identity credentials, are qualified under the provisions of DoD Instruction 8500.2 and DoD Instruction 1341.2 (references (u) and (v)).

6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2

- E1. References, continued
- E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Directive 1322.16, "Montgomery GI Bill (MGIB) Program," June 18, 2002
- (f) DoD Instruction 1322.17, "Montgomery GI Bill Selected Reserve (MGIB-SR)," November 29, 1999
- (g) Chapter 55 of title 10 United States Code
- (h) DoD *Instruction* 1330.09, "Armed Services Exchange Policy," November 7, 2005
- (i) DoD Directive 1330.17, "Military Commissaries," March 13, 1987
- (j) Section 552 of title 10, United States Code
- (k) DoD Directive 5400.11, "DoD Privacy Program," December 13, 1999
- (l) Parts 160 and 164 of title 45, Code of Federal Regulations, "Health and Human Services (HIPAA) Privacy Rule," current edition
- (m) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002
- (n) Section 113 of title 10, United States Code
- (o) DoD *Instruction* 5200.08, "Security of DoD Installations and Resources," December 10, 2005
- (p) DoD Directive 8190.3, "Smart Card Technology," August 31, 2002
- (q) DoD Instruction 1400.32, "DoD Civilian Work Force Contingency and Emergency Planning Guidelines and Procedures," April 24, 1995
- (r) DoD Directive 3025.14, "Protection and Evacuation of U.S. Citizens and Designated Aliens In Danger Areas Abroad (Short Title: Noncombatant Evacuation Operations), November 5, 1990
- (s) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
- (t) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
- (u) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (v) DoD Instruction 1341.2, "Defense Enrollment and Eligibility Reporting System (DEERS) Procedures," March 19, 1999

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. DoD Credential Holders

E2.1.1.1. Eligible Family Members. Individuals who have a family association to a sponsor in accordance with reference (v).

E2.1.1.2. Uniformed Service Members. Active and retired.

E2.1.1.3. Eligible DoD Contractors. An employee or individual under contract or subcontract to the Department of Defense, designated as providing services or support to the Department that requires logical and/or physical access to the Department's assets.

E2.1.1.4. DoD Civilian. A Federal civilian employee of the Department of Defense, or on loan to the Department of Defense, directly or indirectly hired and paid from appropriated or nonappropriated funds, under permanent or temporary appointment.

E2.1.1.5. Eligible Affiliates. Individuals belonging to groups that are affiliated with the Department of Defense.

E2.1.1.6. Physical Access Only Designees. Commercial service personnel and visitors with specific business on DoD installations and buildings.

E2.1.1.7. Those designated by law, regulation or agreement.

E2.1.2. Personnel Identity Protection. A business process that authenticates individual identity. This process involves:

E2.1.2.1. A binding of the identity to an identity protection system through the issuance of a DoD credential.

E2.1.2.2. The linkage of the credential to the individual through use of uniquely identifying characteristics and a personal identification number; and

E2.1.2.3. Digital authentication of the identification credential linkage to the individual.