Department of Defense
INSTRUCTION

NUMBER 1000.25
March 2, 2016

USD(P&R)

SUBJECT: DoD Personnel Identity Protection (PIP) Program

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Directive (DoDD) 1000.25 (Reference (a)) as a DoD Instruction (DoDI) to:

(1) Establish policy and assign responsibilities for the DoD PIP Program.

(2) Establish the Identity Protection and Management Senior Coordinating Group (IPMSCG) to oversee and integrate DoD-wide policy, capabilities, and strategy for:

(a) Managing identities within DoD.

(b) Sharing identity attributes with DoD asset owners and mission partners across the DoD Information Networks architecture in accordance with section 373(a)-(g) of Public Law 106-65 (Reference (b)).

b. Incorporates and cancels the IPMSCG Charter (Reference (c)) and the October 22, 2014 Department of Defense Chief Information Officer Memorandum (Reference (d)).

2. APPLICABILITY. This instruction applies to:

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

b. The Commissioned Corps of the U.S. Public Health Service (USPHS), under agreement with the Department of Health and Human Services, and the National Oceanic and Atmospheric Administration (NOAA), under agreement with the Department of Commerce.

3. POLICY. It is DoD policy that:

a. The PIP Program will use emerging technologies to support the protection of individual identity and to assist with safeguarding DoD physical assets, networks, and systems from unauthorized access based on fraudulent or fraudulently obtained credentials.

b. DoD identification (ID) cards will be issued to eligible individuals using the Real Time Personnel Identification System (RAPIDS) by authenticating their identity against the Defense Enrollment Eligibility Reporting System (DEERS) in accordance with Volumes 1 and 2 of DoD Manual 1000.13 (Reference (e)), and DoDI 1341.2 (Reference (f)).

c. DoD ID cards serve as the authoritative assertion of identity and are used as proof of DoD affiliation. DoD ID cards should be authenticated against DEERS, global directory services, or DoD Public Key Infrastructure (PKI) services in real-time whenever possible.

d. The authentication of users and the granting of logical and physical access is a combination of enterprise-wide and local functions that operate in accordance with this instruction, DoD 5200.08-R, DoDI 5200.08, DoDI 5200.46, DoDI 8500.01, and DoDI 8520.03 (References (g) through (k)).

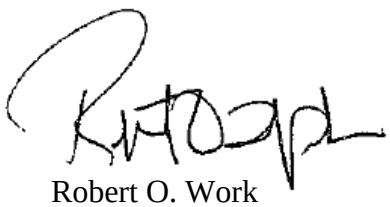
e. The IPMSCG oversees the PIP Program.

4. RESPONSIBILITIES. See Enclosure 2.

5. INFORMATION COLLECTION REQUIREMENTS. The personnel information transfer to PIP systems, referred to throughout this instruction, does not require licensing with a report control symbol in accordance with paragraph 1b(13), Enclosure 3, Volume 1 of DoD Manual 8910.01 (Reference (l)).

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

7. EFFECTIVE DATE. This instruction is effective March 2, 2016.



Robert O. Work
Deputy Secretary of Defense

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 19, 2004 (hereby cancelled)
(b) Section 373 (a)-(g) of Public Law 106-65, "National Defense Authorization Act for Fiscal Year 2000," October 5, 1999 (section titled "Use of Smart Card Technology in the Department of Defense").[1]
(c) DoD Chief Information Officer Memorandum, "Identity Protection and Management Senior Coordinating Group," October 22, 2014 (hereby canceled)
(d) DoD Chief Information Officer Memorandum, "Identity Management Senior Coordinating Group," January 12, 2004 (hereby canceled)
(e) DoD Manual 1000.13, Volumes 1 and 2, "DoD Identification (ID) Cards," January 23, 2014
(f) DoD Instruction 1341.2, "Defense Enrollment Eligibility Reporting System (DEERS) Procedures," March 19, 1999
(g) DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended
(h) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended
(i) DoD Instruction 5200.46, "DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)," September 9, 2014
(j) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(k) DoD Instruction 8520.03, "Identity Authentication for Information Systems." May 13, 2011
(l) DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014
(m) DoD Instruction 1336.05, "Automated Extract of Active Duty Military Personnel Records," July 28, 2009, as amended
(n) DoD Instruction 7730.54, "Reserve Components Common Personnel Data System (RCCPDS)," May 20, 2011
(o) DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," January 23, 2014
(p) Title 5, United States Code
(q) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
(r) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(s) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, as amended
(t) DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended
(u) DoD Manual 5200.01, Volumes 1-4, "DoD Information Security Program," February 24, 2012, as amended
(v) Joint Requirement Oversight Council Memorandum 091-09, "Public Key Infrastructure Capability Development Document," May 22, 2009[2]

[1] Published as a note following section 113 of title 10, United States Code.
[2] Copies may be obtained by contacting the Defense Manpower Data Center at dodipmscg@mail.mil.

(w) Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
(x) Federal Chief Information Officers Council, "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance," December 2, 2011[3]
(y) Federal Information Processing Standards Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013
(z) DoD Chief Information Officer Memorandum, "Department of Defense Chief Information Officer Executive Board's Identity Council (IdC)," September 13, 2012[4]
(aa) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

[3] Copies may be obtained at http://www.idmanagement.gov/.
[4] Copies may be obtained by contacting the Defense Manpower Data Center at dodipmscg@mail.mil.

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). In addition to the responsibilities in section 8 of this enclosure, the USD(P&R):

a. Serves as the Principal Staff Assistant (PSA) for the PIP Program, and appoints the designated approving authority for these systems and this program.

b. Establishes policy for the PIP Program, including setting minimum acceptable criteria for the establishment and confirmation of personal identity and for the issuance of DoD personnel identity verification credentials, and approving additional systems under the PIP Program. Systems or capabilities under the purview of the PIP Program include, but are not limited to:

(1) DEERS and the RAPIDS, which will be used for identity management operations.

(2) A web service capability for DoD to connect to federal agencies and private sector business partners to share identity attributes.

(3) A capability to provide a rapid registration and tracking system for evacuees during non-combatant evacuations.

(4) A capability to issue and manage a DoD-wide credential that provides authentication services to self-service applications within DoD.

(5) A capability to support DoD identity and access management (IdAM) activities by making available, through web service interfaces, identity attributes stored within DEERS of DoD personnel.

c. In coordination with the Under Secretary of Defense for Intelligence (USD(I)) and in support of the DoD Physical Security Program, maintains the Identity Matching Engine for Security and Analysis to support the vetting of DoD credentialed personnel.

d. Coordinates with the appropriate DoD and OSD Components, such as the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Office of the USD(I), the Office of the Department of Defense Chief Information Officer (DoD CIO), and the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, (USD(C)/CFO), on PIP Program acquisition, communications, and funding, as required.

e. Jointly, with the DoD CIO:

(1) Oversees the IPMSCG.

(2) Reviews the governance structure and activities of the IPMSCG on an annual basis.

f. Coordinates with the USD(I) on PIP management, oversight, and implementation for intelligence, counterintelligence, and security programs.

g. Establishes user groups, as necessary.

2. ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS (ASD(HA)) AND ASSISTANT SECRETARY OF DEFENSE FOR MANPOWER AND RESERVE AFFAIRS (ASD(M&RA)). Under the authority, direction, and control of the USD(P&R) and in coordination with each other and the Director, DoD Human Resources Activity (DoDHRA), the ASD(HA) and the ASD(M&RA) develop guidance and procedures pertaining to healthcare and dental, personnel, and National Guard and Reserves policies, respectively, that impact the PIP Program.

3. DIRECTOR, DoDHRA. Under the authority, direction, and control of the USD(P&R) and in addition to the responsibilities in sections 8 of this enclosure, the Director, DoDHRA:

a. Develops procedures for the oversight, funding, personnel staffing, direction, and functional management of the PIP Program.

b. Coordinates with the ASD(R), the ASD(HA), and the ASD(M&RA) on personnel, healthcare, and National Guard and Reserve policies that impact the PIP Program.

c. Coordinates with the USD(I) on personnel, intelligence, counterintelligence and security policies.

d. Through the Director, Defense Manpower Data Center (DMDC):

(1) Participates and leads user groups, as established by the USD(P&R), and as necessary.

(2) Serves as the IPMSCG Executive Secretariat.

(3) Coordinates recommended changes supporting the PIP Program with the IPMSCG, as necessary.

(4) Operates PIP systems and provides the technical and functional management of the PIP Program, as designated.

(5) Coordinates recommended changes supporting the PIP Program with the IPMSCG, as necessary.

4. USD(I). In addition to the responsibilities in section 8 of this enclosure, the USD(I):

a. Oversees the PIP implementation for intelligence, counterintelligence, and security programs.

b. Coordinates with the USD(P&R) and DoD CIO on activities regarding management and oversight of PIP implementation for intelligence, counterintelligence, and security programs.

5. DoD CIO. In addition to the responsibilities in section 8 of this enclosure, the DoD CIO:

a. Oversees the implementation of the PIP Program for logical access throughout DoD.

b. Coordinates with the USD(P&R) and USD(I) on activities regarding management and oversight of PIP implementation for intelligence, counterintelligence, and security programs.

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

d. Jointly, with the USD(P&R):

(1) Oversees the IPMSCG.

(2) Reviews the governance structure and activities of the IPMSCG on an annual basis.

6. USD(AT&L). In addition to the responsibilities in section 8 of this enclosure, the USD(AT&L) coordinates with the USD(P&R) and USD(C)/CFO on PIP system acquisition, communications, and funding.

7. USD(C)/CFO. In addition to the responsibilities in section 8 of this enclosure, the USD(C)/CFO coordinates with the USD(P&R) and USD(AT&L) on PIP system acquisition, communications, and funding.

8. OSD AND DoD COMPONENT HEADS. The OSD and DoD Component heads identified in Enclosure 3 will:

a. Appoint representatives to serve on the IPMSCG.

b. Provide timely and accurate personnel information from their authoritative personnel systems to PIP systems, as necessary.

9. UNIFORMED SERVICES HEADS. The uniformed services heads will provide timely and accurate personnel information from their authoritative personnel systems to PIP systems, as necessary, in accordance with DoDI 1336.05 and DoDI 7730.54 (References (m) and (n)).

ENCLOSURE 3

IPMSCG

1. MEMBERSHIP. The IPMSCG consists of representatives at the general or flag officer level (or Senior Executive Service equivalent) from the Military Departments, affected PSAs within OSD, and DoD Components.

a. Chair. The DoD CIO, or designated representative, serves as IPMSCG Chair.

b. Members. Membership includes representatives from the:

(1) Department of the Army.

(2) Department of the Navy. The Department will provide three representatives: one from the Department of Navy Chief Information Office, one from the Navy, and one from the U.S. Marine Corps.

(3) Department of the Air Force.

(4) USCG.

(5) National Guard Bureau.

(6) Joint Staff, whose representative will represent the Combatant Commanders and serve as the interface between the IPMSCG and the Joint Capabilities Integration and Development System process on identity protection and management issues, as required.

(7) Office of the USD(AT&L).

(8) Office of the Under Secretary of Defense for Policy.

(9) Office of the USD(C)/CFO.

(10) Office of the USD(P&R), whose representative will be the focal point for PIP policy and programs and will jointly serve as the OSD lead for identity management efforts with the DoD CIO and USD(I) in accordance with DoDI 1000.13 (Reference (o)).

(11) Office of the USD(I), whose representative will be the focal point for PIP policy and programs for intelligence, counterintelligence and security policies and personnel.

(12) Office of the Deputy Chief Management Officer (ODCMO) of the Department of Defense.

(13) Office of Cost Assessment and Program Evaluation.

(14) Office of the Director, Operational Test and Evaluation.

(15) Office of the General Counsel of the Department of Defense.

(16) United States Cyber Command.

(17) United States Strategic Command.

(18) Office of the Intelligence Community Chief Information Officer.

(19) National Security Agency/Central Security Service.

(20) Defense Information Systems Agency.

(21) Defense Privacy and Civil Liberties Division, ODCMO.

(22) Defense Forensics and Biometrics Agency (DFBA), or the DoD program lead for biometrics, as assigned.

(23) DMDC, or the DoD program lead for smart cards, as assigned.

(24) DoD PKI Program Management Office (PMO), or the DoD program lead for PKI, as assigned.

(25) Joint Information Environment Technical Synchronization Office, or the DoD program lead for IdAM, as assigned.

c. Other Attendees. At the discretion of the Chair, other individuals and organizations may be invited to attend, observe, or contribute to IPMSCG meetings and activities.

2. MEMBERSHIP RESPONSIBILITIES

a. Chair. The Chair:

(1) Leads all IPMSCG meetings.

(2) Approves IPMSCG meeting agendas.

(3) Considers the issues, problems, and equities presented during meetings, and provides guidance or directs specific actions.

(4) Establishes subcommittees and work groups, as required.

b. Members. IPMSCG members:

(1) Designate the appropriate, qualified GS-14, GS-15, O-5, or O-6 representative to the DoD Identity Council (IdC).

(2) Ensure appropriate coordination within the larger organization.

(3) Provide requested information, data, and comments as required by the Chair.

c. Executive Secretariat. In coordination with representatives from PKI PMO, DFBA, and Joint Information Environment Technical Synchronization Office, the Executive Secretariat:

(1) Develops and coordinates agenda items, activity reports, status briefs, and information papers with the Chair and IPMSCG members.

(2) Schedules IPMSCG meetings at the direction of the Chair.

(3) Provides advanced materials for the Chair and IPMSCG members.

(4) Prepares documents reflecting the recommendations and decisions of the IPMSCG members for the Chair.

(5) Tracks and reports the status of actions to the Chair.

(6) Prepares and distributes synopses of meetings and decision papers to IPMSCG members.

(7) Supports the research, identification, evaluation, and preparation of technical reports, white papers, or other documentation on issues requiring resolution or attention, as directed by the Chair.

3. PROCEDURES. The IPMSCG:

a. Meets at least four times a year and at other times as directed by the Chair.

b. Recommends actions in the area of DoD's biometric, smart card, PKI efforts, and other identity management technologies and programs throughout the DoD.

c. Develops the DoD identity protection and management vision and strategy, recommends necessary policy statements, and serves as the advocate for identity protection and management for the DoD.

d. Reviews and prioritizes identity protection and management functional capabilities, strategies, and objectives in coordination with the DoD Components and other stakeholder groups.

e. Advances the integration and execution of DoD identity protection and management efforts.

f. Recommends, promotes, integrates, and uses federal, national, and international standards and common commercial practices for all identity protection and management tools (e.g., smart cards, PKI, and biometrics) for physical and logical access to maximize interoperability among information systems and applications to enable industry to meet DoD technology needs.

g. Directs configuration management of identity protection and management solutions, including tools and applications.

h. Leverages identity protection and management best practices and solutions to enhance readiness, improve warfighting and warfighting support processes, and ensure necessary security and privacy.

i. Develops and uses outcome-based performance metrics in implementing identity protection and management solutions.

j. Provides guidance to identity protection and management (e.g., DMDC for smart cards, PKI PMO for PKI, DFBA for biometrics, and Joint Information Environment Technical Synchronization Office for DoD IdAM). Reviews and endorses program management documentation.

k. Reviews identity protection and management reports or findings from external authorities (including, but not limited to, the Government Accountability Office and Congress). If necessary, coordinates responses or reviews reports and recommendation for designated OSD lead PSA to external organization on identity protection and management topics.

l. Ensures security and privacy issues are addressed in the DoD's identity protection and management efforts in the collection, use, maintenance, and dissemination of personally identifiable information in accordance with References (g), (h) and (i), and section 552a of Title 5, United States Code, DoDD 5400.11, DoD 5400.11-R, DoDI 5200.01, and DoDI 5200.02 (References (p) through (t), and Volumes 1 through 4 of DoDM 5200.01 (Reference (u))

m. Uses a risk management framework to analyze alternatives and make appropriate recommendations.

n. Establishes and disestablishes identity protection and management work groups and sub-work groups as appropriate. Manages, reviews, and approves the efforts and products of these work groups.

o. Establishes the process to coordinate identity protection and management documents (e.g., implementation guides and protection profiles).

p. Ensures that identity protection and management efforts comply with the cybersecurity component of the DoD Information Networks architecture.

q. Oversees the Joint Requirements Oversight Council (JROC)-delegated responsibilities for the requirements review and approval process for the DoD PKI program. The IPMSCG considers cost, schedule, and performance impacts during requirements analysis and ensures any changes to requirements are fully analyzed to properly inform program management and risk decision making. In accordance with the Joint Requirements Oversight Council Memorandum 091-09 (Reference (v)):

(1) Oversees and integrates DoD-wide policy, capabilities, and strategy for managing physical and virtual identities within the DoD and sharing those attributes with DoD asset owners and mission partners across the DoD Information Networks architecture.

(2) Oversees and approves the DoD PKI program's requirements validation process within the boundaries set by the JROC.

(3) Reviews and approves requirements prioritization.

(4) Aligns oversight activity with planning, programming, budgeting, and execution processes, and provides feedback to the JROC if the cost, schedule, and performance of the DoD PKI program cannot be executed within the boundaries established by the JROC

r. Maintains a configuration management process for the CAC and its related components to monitor DoD compliance with Homeland Security Presidential Directive 12, Federal Chief Information Officers Council Roadmap, and Federal Information Standards Publication 201-2 (References (w) through (y)).

s. Monitors the CAC and identity protection related activities outlined in Reference (o).

t. Oversees the activity of DoD IdC in accordance with the DoD IdC Charter (Reference (z)).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HA)	Assistant Secretary of Defense for Health Affairs
ASD(M&RA)	Assistant Secretary of Defense for Manpower and Reserve Affairs
DEERS	Defense Enrollment Eligibility Reporting System
DFBA	Defense Forensics and Biometrics Agency
DMDC	Defense Manpower Data Center
DoD CIO	Department of Defense Chief Information Officer
DoDD	DoD directive
DoDHRA	Department of Defense Human Resources Activity
DoDI	DoD instruction
ID	identification
IdAM	identity and access management
IdC	Identity Council
IPMSCG	Identity Protection and Management Senior Coordinating Group
JROC	Joint Requirements Oversight Council
NOAA	National Oceanic and Atmospheric Administration
ODCMO	Office of the Deputy Chief Management Officer
PIP	personnel identity protection
PKI	Public Key Infrastructure
PMO	Program Management Office
PSA	Principal Staff Assistant
RAPIDS	Real-time Automated Personnel Identification System
USCG	United States Coast Guard
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer,

	Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USPHS	United States Public Health Services

PART II. DEFINITIONS

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

authoritative data source. A recognized or official data production source with a designated mission statement, or source, or product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources.

DEERS. The authoritative data repository for identity information. DEERS will be used to verify an individual's identity, affiliation with the DoD, and eligibility for benefits, privileges, and entitlements.

DoD credentialed person. Individual seeking to possess or possessing DoD ID cards, other federal agencies' Reference (w)-compliant credentials, or locally-issued, physical access only badges who are authorized access to DoD installations or bases.

DoD Information Networks. Defined in Joint Publication 1-02 (Reference (aa)).

IdAM. The policies, processes, architectures, standards, systems, and data that integrate person and non-person entity digital identity management, credentialing, authentication, authorization, and access management.

identity management. A business function that securely authenticates an individual, device, application or service to validate identity, DoD affiliation, and validity of a credential.

personally identifiable information. Defined in Reference (p).

PIP. A business process that authenticates individual identity. This process involves:

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

The linkage of the ID credential to the individual through use of uniquely identifying characteristics and a personal ID number.

Digital authentication of the ID credential linkage to the individual.

uniformed services. The Army; Navy; Air Force; Marine Corps; USCG; the Commissioned Corps of NOAA; and the Commissioned Corps of the USPHS, Department of Health and Human Services.