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

JUL 26 2013

PERSONNEL AND
READINESS

MEMORANDUM FOR DIRECTOR, PERSONNEL AND READINESS INFORMATION MANAGEMENT

SUBJECT: Designation of Chief Information Officer for the Office of the Under Secretary of Defense for Personnel and Readiness

The Chief of Staff (CoS) for the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD (P&R)) is the Office of Primary Responsibility for all OUSD(P&R) information enterprise initiatives. I designate the Director, Personnel and Readiness Information Management (P&R IM), to be the Chief Information Officer (CIO) for OUSD(P&R). The Director, P&R IM, when acting as CIO will be acting on behalf of the P&R CoS, and will be accountable to the P&R CoS. Specific duties and responsibilities are identified in the attached. Additionally, you will be responsible and accountable for coordinating the activities of the various organizations within P&R to ensure consistency and completeness of the approach to, and execution of, activities relating to the attached responsibilities.

P. M. Tamburrino, Jr.
Chief of Staff

Attachment:
As stated

cc:
Assistant Secretary of Defense
for Health Affairs
Assistant Secretary of Defense
for Reserve Affairs
Assistant Secretary of Defense
for Readiness and Force Management
Director, Defense Human Resources Activity

The Personnel & Readiness Chief Information Officer Responsibilities and Duties

The Office of the Under Secretary of Defense, Personnel and Readiness (OUSD(P&R)) Chief Information Officer (CIO) shall:

Represent P&R in Department of Defense (DoD) CIO-led forums for governing DoD Information Enterprise (for example, DoD CIO Executive Business, Joint Information Environment EXCOM, and Office of the Deputy Chief Management Officer (ODCMO) Defense Business Council).

Promulgates written Agency-wide Information Technology governance and cyber policy.

Provide oversight for information solutions that shall provide reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents. Ensure that all DoD, Defense Information Systems Agency (DISA), and USCYBERCOM policies and technical advisories and requirements are accomplished as required.

Provide oversight for the Human Resource Management (HRM) Enterprise Architecture (EA), which is consistent with the DoD EA and the Business Enterprise Architecture. The HRM EA shall be maintained and applied to guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across the HRM community, and provide a sound basis for transition from the existing environment to the future.

Provide oversight for investments in information solutions that shall be managed through a capital planning and investment control process directed by and in accordance with guidance from ODCMO.

Ensure that all requirements delineated in applicable laws, regulations, and policies are applied throughout P&R.

Defense Information Assurance Certification and Accreditation Process (DIACAP):

Appoint a P&R Senior Information Assurance Officer (SIAO) to direct and coordinate the P&R Information Assurance program consistent with the strategy and direction of the DoD CIO/DISA.

Each CIO, supported by an appointed SIAO, is responsible for administration of the overall Certification and Accreditation process. This includes the integration of certification with other DIACAP activities, participation in the DIACAP Configuration Control and Management, visibility and sharing of the certification and accreditation status of assigned Information Systems, and enforcement of training requirements.

Federal Information Security Management Act (FISMA):

Certifies annual FISMA Compliance

Law and Statutes:

10 U.S.C. § 2222 "Defense business systems: architecture, accountability, and modernization"
40 U.S.C. Chapter 113 "Responsibility for Acquisitions of Information Technology"
44 U.S.C. Chapter 35 "Coordination of Federal Information Policy"
44 U.S.C. Chapter 36 "Management and Promotion of Electronic Government Services"
Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)
Federal Information Security Act (FISMA) of 2002
Office of Management and Budget Circular A-130, "Management of Federal Information Resources, November 28, 2000

DoD Policies:

DoDD 8000.01,"Management of the Department of Defense Information Enterprise," February 10, 2009
DoDD 8500.1, "Information Assurance (IA)," October 24, 2002
DODD 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
DoDI 8510.01, "Department of Defense Information Assurance Certification and Accreditation Process," November, 27, 2007