Program Executive Office for Information Technology (PEO IT)

Defense Integrated Military Human Resources System (Personnel and Pay) (DIMHRS (Pers/Pay))

Privacy Impact Assessment

22 August 2004

Prepared by:
V.E. Carpenter, CAPT, USN
DIMHRS (Pers/Pay) Joint Program Manager
Program Executive Office for Information Technology (PEO IT)

<u>Do Not Distribute to DTIC or Other Data Repositories</u>
Distribution authorized to DoD components only.
Other requests shall be referred to:
Joint Program Management Office
2251 Lakeshore Drive
New Orleans, LA 70145

1 Purpose

In accordance with Office of Management and Budget (OMB) Memorandum M-03-22 Defense Integrated Military Human Resource System (Personnel and Pay) (DIMHRS (Pers/Pay)), defined as a major information system merging a significant amount of data, is required to conduct a Privacy Impact Assessment (PIA) for electronic information systems and collections.

The DIMHRS (Pers/Pay) PIA details what kind of personal information is contained within the DIMHRS (Pers/Pay) system, what is done with that information, and how that information is protected. There are many requirements for Department of Defense (DoD) Information Systems (IS) containing personal information based on extensive lists of privacy laws, regulations, and guidance. The DoD Privacy Office should be contacted as resource for questions related to the technicalities of privacy law.

This document will give a brief history of program initiation how the system is identified and then detail the following in Sections, four through eight:

- Type of information collected and from where
- How information is collected
- Who information is shared with
- How it is protected
- Criteria for data retention and destruction

DIMHRS (Pers/Pay) is currently in Critical Design Review. The focus for this assessment is on the development network. The PIA will be updated and focus shifted to the production environment once the design has been formally approved and system development and integration begins.

2 Background

In late 1995, a Defense Science Board Task Force on Military Personnel Information Management was convened to advise the Secretary of Defense on the best strategy for supporting military personnel and pay functions. The Task Force's report concluded that the DoD multiple Service-unique military personnel and pay systems caused significant functional shortcomings (particularly in the joint arena) and excessive development and maintenance costs. To address these shortcomings, the task force recommended that the DoD transition to a single, all Service and all Components, fully integrated personnel and pay system with common core software.

Once implemented, DIMHRS (Pers/Pay) will provide an end-to-end, integrated military personnel and pay systems for all military services including their Active, Reserve, and National Guard components. As the cornerstone of military personnel transformation, DIMHRS (Pers/Pay) is the vehicle to field and resource a fully integrated human resources system, while concurrently supporting reengineered business processes, replacing failing systems, reducing data collection burdens, enhancing readiness, and connecting Soldiers, Sailors, Airmen and Marines directly to their personnel and pay system.

3 System Identification

DIMHRS (Pers/Pay) is an Under Secretary of Defense (Personnel and Readiness (USD (P&R)) owned and operated program. DIMHRS (Pers/Pay) is registered as a DoD Information Technology (IT) program under identification number AV019665. Additionally, the program is registered with the Department of the Navy (DON) Chief Information Officer (CIO) as an ACAT 1AM Mission Essential program with DITSC identification number 19665.

4 Information Collection

DIMHRS (Pers/Pay) will be a single comprehensive system containing personnel, pay, and entitlement data for Military personnel, and their families, throughout a Service member's life. DIMHRS (Pers/Pay) will track family members in locations that are separate from their sponsors and in some instances, other family members, and even family pets, are tracked as non-combatant civilians in case of the need for evacuation. DIMHRS (Pers/Pay) will enable managers to search the full range of personnel (active, reserve and National Guard) to identify personnel with specific skills (whether military or civilian acquired) and to quickly form task force rosters.
DIMHRS (Pers/Pay) is expected to support approximately 3.1 million personnel.

5 Information Collection Mechanism

DIMHRS (Pers/Pay) will provide each Service member with a single, comprehensive record-of-service that will be available to the Service member, allowing individuals to update select personal information. The personnel records will be available to Service personnel chiefs, Combatant Commanders, military personnel and pay managers and other authorized users throughout the DoD and other federal agencies. This web-based human resource tool will be open for business 24 hours, daily.

DIMHRS (Pers/Pay) will provide data and system interoperability across multiple interfaces both internal and external. Interface requirements are noted in the DIMHRS (Pers/Pay) Operations Requirements Document (ORD). Documentation detailing the internal interfaces is available in the DIMHRS (Pers/Pay) Legacy Data Base. Appendix G of the ORD provides System Interface Descriptions for the overall program.

The multiple environments used to develop and implement DIMHRS (Pers/Pay) are being proposed and managed by Northrop Grumman. A high level description of the Development, Test, Continuity of Operations (COOP), and Production environments can be found in Sections 3 and 4 of the DIHMRS (Pers/Pay) System Security Authorization Agreement (SSAA).

6 Information Sharing

There are three defined DIMHRS (Pers/Pay) user types: military, civilian, and contractor. Military and Civilian users have service agreement in place that dictates their requirement to comply with privacy data requirements. The contractors, however, will be required to have a National Agency Check (NAC) and Non-disclosure agreement (NDA) in place in order to access the system.

7 Information Protection

Protection requirements that serve as the foundation for the DIMHRS (Pers/Pay) privacy practices are derived from DoDD 8500.2, IA Implementation, and are explicitly defined in the DIMHRS (Pers/Pay) Security Requirements Traceability Matrix (S-RTM). The S-RTM is applicable to the DIMHRS Development, Test, COOP and Production environments.

Awareness and training for all developers and others affected by the privacy plan include local awareness and training, and user consent forms to acknowledge user responsibilities for protecting data. In order to monitor the user compliance with these required rules of behavior, there are periodic audits of Developer IT assets under the direction of Commander, Naval Network Warfare Command (COMNAVNETWARCOM).

Privacy Act controls for the DIMHRS Development Network (DDN) are defined under the following areas:

- Managerial
- Operational
- Technical

These controls have been incorporated into the DIMHRS (Pers/Pay) DoD Information Technology Security Certification and Accreditation Process (DITSCAP) framework with supporting processes to ensure compliance.

7.1 Management Controls

7.1.1 Risk Management

The DIMHRS (Pers/Pay) continually manages Program risk through the Risk Management Control Board (RMCB). This overarching board responds to and mitigates potential risks to the Program. The DDN SSAA contains a Residual Risk Assessment based on preliminary design analysis and initial vulnerability assessment of the DDN. An assessment of data confidentiality, integrity and authorization, and mitigation measures and controls were included in this analysis. Only Government employees and military personnel can authorize release of Privacy Act data to developers.

7.1.2 Certification and Accreditation

The DDN has been Certified and Accredited in accordance with the DITSCAP.

7.2 Operational Controls

7.2.1 Personnel Controls

As per DoD PKI requirements, all DDN users are required to have a DoD CAC. Developers are required to attend Navy Marine Corps Intranet (NMCI) Developer Seat training and to sign user responsibility statement. The rules of behavior and requirements for DIMHRS Science and Technology (S&T) seats are no different than other S&T seats except DIMHRS S&T seats can only communicate with the DIMHRS server Community of Interest (COI) (i.e.; Development and Implementation Server COI).

The user responsibility statement includes policies and procedures for handling, storing, and disseminating sensitive information. In particular, the following terms are mandated:

- Protect all media used on the system by properly classifying, labeling, controlling, transmitting, and destroying it in accordance with security requirements.
- Protect all data viewed on screens or produced as output to the highest classification level approved for processing on the system until the data has been reviewed and verified to be unclassified.

7.2.2 Physical Controls

Physical access to the DDN servers is restricted to authorized individuals. DDN servers are located in a controlled area; protected by a card entry system, monitored by a video surveillance system and all visitors must be escorted into the facility and signed in by authorized personnel.

7.2.3 Security Training

All Developers and Joint Program Management Office (JPMO) staff are required to attend initial and yearly Security Awareness Training and Education (SATE). The SATE training includes proper handling procedures and protection of sensitive information. Users are required to sign and submit user responsibility forms, which include statements on the handling of sensitive information.

7.3 Technical Controls

The DDN is part of the NMCI infrastructure and existing NMCI Information Assurance mechanisms are in place and operational. Access to the DDN servers, containing sensitive information, is only allowed to NMCI Development workstations. No External access to the DDN is allowed. Each developer seat is inside a protected COI. This COI utilizes Virtual Local Access Network (VLAN) and router Access Control Lists (ACL) to protect NMCI.

7.3.1 Access Management

The DDN design includes mechanisms for access management, password management, identity data management, audit and reporting, administrative management. In particular, only authorized and approved DIMHRS (Pers/Pay) S&T developer seats will access DIMHRS server COI environment (i.e. the DDN) via Access Control Lists (ACLs). Configuration management process maintains a status of all instances (databases) of personal information and data-access privileges within the DDN is maintained.

7.3.2 Identification and Authentication

I&A, including auditing mechanisms, is enabled to confirm that only authorized users have access to sensitive information and systems.

Allocation of passwords is managed and password security policies are enforced. Developers reside on NMCI developer seats and must abide by NMCI standards and guidelines as they pertain to such issues as password make-up, password aging, and password protection.

7.3.3 Assessments

Periodic assessments of access rights and privileges are performed within the DDN. These include both NMCI and local developer network assessments in coordination with local DIMHRS (Pers/Pay) security personnel.

8 Information Retention and Destruction

DoD 5015.2-STD provides implementing and procedural guidance on the management of records in the Department of Defense. It sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by the DoD Components in the implementation of their records management programs; defines required system interfaces and search criteria to be supported by the RMA's and describes the minimum records management requirements that must be met, based on current National Archives and Records Administration (NARA) regulations.

DoD Directive 5015.2 details the procedures for disposition of data at the end of its retention period as well as how long destruction reports will be maintained.

Appendix A – References

DoD 5400.11-R, “Department of Defense Privacy Program,” August 1983

E-Government Act of 2002 (H.R. 2458/S. 803), Presidential signature December 17, 2002 – Section 208

Office of Management and Budget **(OMB) Memorandum, M-03-22**, September 26, 2003

DoD 5015.2-STD, “Department of Defense Design Criteria Standard for Electronic Records Management Software Applications,” July 19 2002

DoD Directive 5015.2, "Department of Defense Records Management Program," March 6, 2000

DoD 8500.2, "Department of Defense Information Assurance (IA) Implementation," February 6, 2003

DIMHRS (Pers/Pay) ORD, "Defense Integrated Military Human Resource for Personnel and Pay, Operational Requirements Document," Draft - January 30, 2004

DIMHRS (Pers/Pay) SSAA, "Defense Integrated Military Human Resource for Personnel and Pay, System Security Authorization Agreement” August 30, 2002