



DEPARTMENT OF DEFENSE  
6000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-6000

JAN 24 2007

CHIEF INFORMATION OFFICER

**MEMORANDUM FOR CHIEF INFORMATION OFFICERS, MILITARY  
DEPARTMENTS  
CHIEF INFORMATION OFFICER, JOINT STAFF  
CHIEF INFORMATION OFFICERS, COMBATANT  
COMMANDS  
CHIEF INFORMATION OFFICERS, UNDER  
SECRETARIES OF DEFENSE  
CHIEF INFORMATION OFFICER, DIRECTOR,  
ADMINISTRATION AND MANAGEMENT  
CHIEF INFORMATION OFFICERS, DEFENSE AGENCIES  
CHIEF INFORMATION OFFICERS, FIELD AGENCIES**

**SUBJECT: Compliance and Review of Logical Access Control in Department of Defense  
(DoD) Processes**

Access controls are one of several processes used to protect DoD data and implement the Defense-in-Depth Strategy across the enterprise. The Joint Task Force - Global Network Operations (JTF-GNO) Communications Tasking Order (CTO) 06-02, dated January 17, 2006, mandated the use of DoD Public Key Infrastructure (PKI) certificates as defined in DoDI 8520.2<sup>1</sup> for the Non-classified Internet Protocol Router Network (NIPRNET) and NIPRNET web-based systems and applications. In keeping with the Department's desire to achieve net-centricity, the use of PKI authentication does not eliminate the need to properly configure mandatory/discretionary access controls on private web servers, web-based systems and applications, and web portals. The use of these controls is especially important with regards to non-US persons (e.g., Foreign Exchange Officers), as certificate-based authentication requires these personnel be issued DoD PKI certificates if they are authorized to log on to the network.

The system owners/administrators must validate their access control procedures for user and privileged access to the NIPRNET and NIPRNET web-based systems. These procedures must include:

- A rules-based process for determining which personnel are authorized access (e.g., all DoD employees, members of a specific community of interest, and/or entities acting in a specific role), mapping personal certificate information to authorization(s), and removing authorizations when access is no longer needed or authorized. As the capability to do dynamic rules-based access control

<sup>1</sup> All DoD issuances cited in this memorandum may be found at <http://www.dtic.mil/whs/directives/>

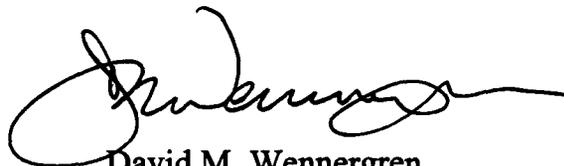


becomes available, Designated Approving Authorities (DAAs) should authorize its use as appropriate.

- Process for granting authorization/access to DoD information systems (e.g., NIPRNET, web-based systems) per DoD 5200.1-R, DoD 5200.2-R and DoDI 8500.2.
- Mechanisms instituted to allow appropriate non-US users to access information cleared for release to the represented foreign nation, coalition, or international organization per applicable DoD policy (e.g., DoDD 5230.11, DoDD 5230.20, DoDI 5230.27).
- When applicable, contacting legal counsels for assistance in formulating appropriate access control guidelines or decisions.

The DoD Public Key Enabling (PKE) website (<https://gesportal.dod.mil/sites/dodpke>) provides information on various software tools that can be used to implement effective certificate-based authentication and rules-based authorization processes including verification of citizenship. Each Service also has a PKE technical team that can provide system owners/administrators technical guidance about implementing certificate-based authentication and authorization. Washington Headquarters Service provides the PKE technical expertise for DoD agencies

As systems are converted to PKI certificate-based authentication per the JTF-GNO CTO 06-02, each Component CIO must ensure compliance with current access control policy and implementation of auditing procedures for establishment and maintenance of proper access control mechanisms. The Director, Information Assurance Policy (IAP), Robert Lentz, (703) 695-8705, [robert.lentz@osd.mil](mailto:robert.lentz@osd.mil), will coordinate and monitor compliance.



David M. Wennergren  
Deputy Chief Information Officer