NOTE: Because this report assesses potential vulnerabilities in IT security, only a summary of the report is posted.

Report Title: Audit of NARA's System Administrator Rights and Controls
Report Number: 06-11
Date Issued: September 27, 2006

Audit of NARA's System Administrator Rights and Controls

The Office of the Inspector General (OIG) performed an audit of the NARA's system administrator rights and controls. The audit was designed to determine whether the appropriate controls, oversight, policies, and procedures are implemented over system administrator accounts in order to ensure that NARA systems and information are properly secured and reasonably controlled. System administrator rights and controls exist to ensure that only legitimate system administrators can perform operations critical to controlling rights among other programs and users.

Our audit revealed that NARA's controls over system administrator accounts were weak and needed immediate improvement. The inadequate controls governing system administrator rights and controls result in increased risk of system degradation due to potential mismanagement, human error, or system compromise by persons seeking to harm NARA's servers and infrastructure devices.

Specifically, we noted weaknesses governing the removal of previously disabled system administrator accounts; the enforcement of NARA password policies for system administrator passwords; users having root access on some servers; system logs, including the lack of logging, ineffective log parameters, log overwrites, inconsistent log sizes, and logs not backed up or saved; the number of system administrators on servers; the ability of system administrators to create an access control list of users and their rights for review as directed by the NARA Technical Controls IT Handbook; the process of ensuring that system administrators have a user level account in addition to their administrator account; and the policies and procedures governing field sites and the related systems administration.

We made nine recommendations to improve NARA's system administrator rights and controls and enhance controls over information technology security. Management agreed with all but two recommendations and initiated corrective action.