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

Report Title: Review of NARA's Information Security Program
Report Number: 06-09
Date Issued: August 9, 2006

Review of NARA's Information Security Program

The overall objective of our review was to determine if the National Archives and Record Administration is making satisfactory progress establishing an information security program that includes appropriate controls required by federal legislation. Specifically, we sought to determine whether or not NARA (a) has up-to-date, documented security policies; (b) has documented procedures and controls to implement the policies; (c) has implemented the security procedures and controls, and reinforced them through training; (d) routinely tests and reviews the adequacy and effectiveness of its procedures and controls; and (e) has successfully integrated the policies, procedures, and controls into a comprehensive security program that is an integral part of its organizational culture.

Our review revealed that (a) NARA's network perimeter/firewall security needs improvement; (b) the agency's computer network operating system software and electronic message software do not ensure a secure computing environment for the agency's computer network users; (c) NARA officials have not established a 24-hours-per-day/7-days-per-week computer security incident response capability; performed any testing to ensure that the computer incident response team will function in the most efficient and effective manner possible; or conducted post incident activities in accordance with the guidance in National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, and the NARA *Computer Security Incident Handling Guide*; (d) in the area of contingency planning, NARA's recovery strategy for quickly and effectively restoring its mission critical IT systems after a severe service disruption or disaster is inadequate; contingency plans were not prepared for two of NARA's IT systems; the NH Disaster Recovery Plan was inadequate (i.e., critical information was missing from the plan) and, of 28 mission critical and non-mission critical IT systems reviewed, none had a plan for testing its contingency plan, nor had any testing been accomplished; and (e) improvement is needed in NARA's security certification and accreditation process, specifically, the preparation, maintenance, and update of system security plans; preparation of plans of action and milestones; and tasks associated with the continuous monitoring process.

We made 12 recommendations that, when implemented by management, will assist the agency in establishing an information security program that meets the Federal Information Security Management Act and the National Institute of Standards and Technology requirements, and will eliminate the need to report information security as a material weakness in the FMFIA report. Management concurred with two recommendations, partially concurred with two recommendations, and nonconcurred with eight recommendations in the report. The report is currently being reviewed by the Archivist of the United States.