National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date : September 20, 2007

Reply to
Attn of : Office of Inspector General (OIG)

Subject : Management Letter #07-12, Contingency Planning for Information Technology Systems

To : Allen Weinstein, Archivist (N)

The purpose of this memorandum is to formally bring to your attention conditions that could impact NARA's ability to recover information technology (IT) systems that are essential to the agency's mission in the event of a disaster or emergency situation.

Public Law 107-347, "The Federal Information Security Management Act (FISMA)," requires all Federal agencies to develop, document, and implement an information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Previous OIG Report No. 06-09, "Review of NARA's Information Security Program," July 31, 2006, identified IT contingency planning and disaster recovery as inadequate to support NARA's critical systems and recommendations were made to strengthen the contingency plans. Unfortunately, the recommended corrective measures were not adopted and contingency plans were not revised. During the ongoing audit of NARA's compliance with the FISMA, we reviewed the individual contingency plans developed for each information system and interviewed the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) regarding those plans.

We identified a significant risk to agency operations because adequate plans do not exist and coordination among NARA Senior Managers has not been established to ensure IT systems critical to NARA's mission can be recovered quickly and effectively following a service disruption or disaster. Specifically, NARA Senior Management identified several systems in the NARA Continuity of Operations Plan (COOP) as essential to their operations in the event of a regional or national emergency. According to the CIO, she lacks the organizational posture and baseline resources necessary to ensure that "critical" or "essential" systems will be available in the event of a regional or national emergency.

[redacted]

Redactions made pursuant to FOIA Exemption b(2)

[redacted] Redactions made pursuant to FOIA Exemption b(2) [redacted]

We bring this to your attention because the CIO has defined a lack of organizational authority and capacity to establish policy for ensuring that business owner's have established COOPs to ensure agency operations can continue in the event IT systems are not available for long periods of time. We believe it to be imperative that this issue be resolved promptly in order for NARA to develop, document, and implement plans that minimize the agency's risk and afford NARA the opportunity to recover critical IT services following an emergency. This issue will be further addressed in the forthcoming FISMA audit report.

We suggest that you begin discussions with pertinent senior managers to clarify appropriate roles and responsibilities. We look forward to your response as to how you plan to address this condition. Should you have any questions, please contact me on (301) 837-1532.

Paul Brachfeld
Inspector General