GSA

GSA Office of Governmentwide Policy

MEMORANDUM FOR JUDITH SPENCER
SYSTEM OWNER
IDENTITY MANAGEMENT DIVISION (MEI)

THRU: WILLIAM G. MORGAN
INFORMATION SYSTEM SECURITY MANAGER (ISSM)
OFFICE OF THE CHIEF INFORMATION OFFICER (IO)

FROM: MARY J. MITCHELL Mary J Mitchell
DESIGNATED APPROVAL AUTHORITY (DAA)
DEPUTY ASSOCIATE ADMINISTRATOR
OFFICE OF TECHNOLOGY STRATEGY (ME)

SUBJECT: Security Accreditation Decision for the Cybertrust Shared Service Provider System (CYBSSPS)

1. References:

   a) OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

   b) NIST Special Publication 800-37: Guide for Security Certification and Accreditation of Federal Information Systems, May 2004.

   c) Cybertrust Shared Service Provider System (CYBSSPS) Certification and Accreditation Submittal Package, October 5, 2006.

   d) Request for Authority to Operate (ATO) Decision for the Cybertrust Shared Service Provider System (CYBSSPS), October 5, 2006.

2. Reference (a) mandates that all major applications and general support systems used by Federal agencies be authorized to operate in writing by a management official. Therefore, the CYBSSPS system was required to have an internal and external security assessment conducted on it and a review of this Certification and Accreditation (C&A) documentation by the Designated Approving Authority (DAA).

3. I have reviewed the Cybertrust Certification and Accreditation package submitted by Cybertrust on October 5, 2006. Based on the review of the Cybertrust Certification and Accreditation package, I hereby authorize operation of the CYBSSPS system for three years.

4. Cybertrust must take the necessary administrative action(s) to reformat the Certification and Accreditation package within 45 days of the granting of this Authority to Operate (ATO) to be in accordance with the GSA IT Security Guidelines, to ensure transparency in the format of Certification and Accreditation packages from various sources.

The following recommendations are incorporated into the accreditation decision letter to reinforce core industry best practices associated with the C&A life cycle process. These recommendations do not imply that there are any outstanding deficiencies in the CYBSSPS *system beyond that specified in item 4 above.*

a. The C&A package is a "living document", it is therefore recommended that Cybertrust institute a reliable mechanism to keep C&A documentation current throughout the life-cycle of the CYBSSPS system.

b. Issues arising from items c. through e. below that impact the overall security of the CYBSSPS system should be promptly integrated in the POAM and addressed in a timely manner.

c. During the C&A period, Cybertrust must continue to monitor the system in accordance with the provisions detailed in NIST Special Publications 800-37. It is recommended that the Cybertrust perform routine internal and external scans on a monthly basis complemented by an annual in-depth penetration testing as a part of the monitoring process.

d. Consistent with GSA operational security framework, it is recommended that Cybertrust also employ the Open Web Application Security Project (OWASP) security tools to facilitate Cybertrust system life-cycle application security vulnerabilities penetration testing.

e. It is further recommended that risks/vulnerabilities identified in the annual WebTrust compliance audit that assesses the adequacy and effectiveness of the controls employed by Certification Authorities (CAs) be discussed with the GSA Cybertrust Program Manager and ISSM as applicable.

5. The point of contact for the operation of the CYBSSPS system is Judith Spencer, Identity Management Division (MEI), GSA Central Office, 1800 F Street NW, Washington, DC 20405, (202) 208-6576.

Mary J Mitchell
Approved by

Oct 16, 2006
Date