



U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED
WASHINGTON, DC 20401

Memorandum

Office of Information Technology & Systems

DAA-2013-7-29-PKI

DATE: July 29, 2013

TO: U.S. GPO Deputy Public Printer

REPLY TO

ATTN OF: Charles Riddle

Tracee Bowley, Deputy CIO

U.S. GPO Chief Information Officer (CIO)
U.S. GPO Designated Approval Authority (DAA)

SUBJECT: Security Accreditation and Authority to Operate – U.S. GPO Principal Certification Authority and Subordinate Certification Authority

A Security Certification review of the U. S. Government Printing Office (GPO) Principal Certification Authority (PCA) and Subordinate Certification Authority (SCA) and their constituent level components, located at 732 North Capitol Street, NW, Washington DC (with offsite backup system components located at the Alternate Computing Facility), was conducted in accordance with official NIST guidance and requirements along with GPO IT Security Policy (GPO Directive 825.33B) requirements, since it had been three (3) years from the date of the previous Authority to Operate (ATO). I have carefully reviewed the results of the Security Certification documentation.

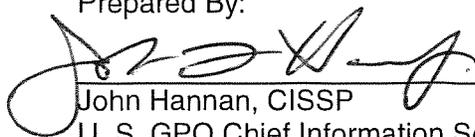
Based on the information provided in the Security Certification documentation, I have determined that the confirmed weaknesses in the GPO PCA and SCA and the plans to resolve, mitigate and address those weaknesses result in a level of residual risk to the operations and assets of the GPO that are acceptable. Accordingly, I am issuing an Authority to Operate (ATO) for the GPO PCA and SCA.

This accreditation is contingent on the continued application of the security controls in place. This accreditation is valid for a period of three (3) years from the issue date of this memorandum unless a significant change occurs to the GPO PCA or SCA systems, which will require the System to be re-accredited.

The senior official in charge of the GPO PCA and SCA is responsible for ensuring that any significant change in the system's configuration (hardware, software and/or firmware) or operating environment is analyzed to determine its impact on the system's security, and that appropriate action is taken to maintain the system security at a level consistent with this ATO.

The GPO Public Key Infrastructure (PKI) Operational Authority and the GPO Chief Information Security Officer (CISO) shall retain a copy of this ATO letter along with the supporting documentation.

Prepared By:


John Hannan, CISSP
U. S. GPO Chief Information Security Officer

7/29/13
Date