

Final Assessment Report 07-09, September 27, 2007 “Report on GPO’s Compliance with the Federal Information Security Management Act (FISMA)”

FISMA requires that each executive branch agency develop, document, and implement an agency-wide program for providing information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Although a legislative branch agency, GPO has recognized the need to be FISMA compliant due to the services the Agency provides, including services to executive branch agencies. The OIG contracted with a consulting firm to perform a baseline assessment of GPO’s FISMA compliance and to evaluate the design and effectiveness of the controls over GPO’s information security program, policies, and practices. The assessment was performed using the most recent applicable FISMA requirements and guidelines published by the Office of Management and Budget and the National Institute of Standards and Technology. Significant emphasis was placed on evaluating the GPO systems used for providing services to client agencies.

The OIG issued a sensitive report concluding that although the Agency has taken steps to comply with FISMA, additional progress is needed to fully comply. The report contains recommendations which, if implemented, will help move GPO toward FISMA compliance.