GENERAL SERVICES ADMINISTRATION
Washington, DC 20417

CIO IL-12-02
November 1, 2012

GSA Instructional Letter

SUBJECT: Continuous Monitoring and Ongoing Authorizations

1. Purpose. This instructional letter (IL) provides direction and guidance for information systems with new, existing and expiring authorizations (Authority-to-Operate (ATO)) to transition to a Continuous Monitoring Program and ongoing authorizations.

2. Background. The Office of Management and Budget (OMB) memorandum M-11-33, *FY2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, issued on September 14, 2011 and Federal Information Security Memorandum FISM-12-02, issued on February 15, 2012 signaled a clear shift away from static point in time security authorization processes to more dynamic, outcome-focused approaches based on continuous monitoring that facilitates ongoing authorizations. To facilitate the new direction favored by OMB and supported in National Institute of Standards and Technology (NIST) guidelines, the Office of the Senior Agency Information Security Officer (OSAISO) has developed a GSA Continuous Monitoring Program.

3. Clearance due date. This IL takes effect immediately; comments are due 10 working days from the signature date.

4. Applicability. The provisions of this IL apply to all GSA Service and Staff Offices (SSOs) and all their employees and contractors, including IT security personnel supporting the security authorization of GSA information systems.

5. Policy.

a. In accordance with GSA IT Security Procedural Guide 06-30, *Managing Enterprise Risk*, all new GSA information systems must be assessed and authorized initially before being placed into production or when significant changes are made to the system.

b. Upon request by a SSO, the OSAISO may accept a GSA information system into the Continuous Monitoring Program provided that the system has a current or expired authorization to operate and meets the qualifying requirements outlined in Section 4.0 of the IT Security Procedural Guide 12-66, *Continuous Monitoring Program*. Upon acceptance into the Continuous Monitoring Program, the SSO will not need to request

re-authorization every three years, but will continue to need a re-authorization if the system undergoes a significant change or if there is a major security breach that impacts the security posture of the system.

c. GSA information systems that do not meet the qualifying requirements for transitioning to the Continuous Monitoring Program must continue to follow the traditional process, including re-authorization every three years or when the system undergoes a significant change or when there is a major security breach impacting the security posture of the system.

d. This IL does not relieve authorizing officials, system owners (aka. System Program Managers/Project Managers), and operators from exercising due diligence and care in ensuring that information systems under their authority have adequate security controls in place and being appropriately monitored per requirements in GSA Order CIO P 2100.1H – *GSA Information Technology (IT) Security policy*.

CASEY COLEMAN
Chief Information Officer
Office of the Chief Information Officer