# ePM Access Requirements

## Who Will Use This?

- √ General Contractor
- √ Construction Manager
- √ Architect/Engineer
- √ Project Manager
- √ Project Team Members
- √ Customer

Licensed ePM users are required to have at a minimum a fully adjudicated Access National Agency Check and Inquiries (ANACI) in place. Under limited circumstances, a user may be granted access to ePM via a waiver process if the user has a favorable fingerprint check and has successfully submitted the appropriate paperwork to initiate at a minimum a NACI background investigation.

These requirements are governed by the following policies:

- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors,"
- GSA Order CIO P 2100.1F April 1, 2010
- CIO P2181.1 – GSA HSPD-12 Personal Identity Verification and Credentialing Handbook

Following are relevant excerpts from these policies explaining who the policies apply to and what type of background investigation is required for access to GSA IT systems. The full versions of the policies are also attached at the bottom of this document.

The **HSPD-12 Policy** "require(s) the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems".

# GSA Order CIO 2100.1F

**GSA Order CIO 2100.1F** additionally states, "This IT Security Policy applies to: all GSA employees, contractors, subcontractors, anyone specified in Memoranda of Understanding (MOUs) or other agreement vehicles, government agencies, individual corporations, other organizations that process or handle GSA-owned information, data, all GSA IT systems, or any GSA data processed on IT systems owned and operated by any of the Services, Staff Offices, and Regions (S/SO/R)." Additionally the policy states, "This IT Security Policy applies to: a. All GSA employees and contractor personnel (and) b. Contractors, subcontractors, and as specified in Memoranda of Understanding (MOUs) or other agreement vehicles, government agencies, individuals, corporations, or other organizations that process or handle any GSA-owned information, data, or IT system equipment.

With regard to investigations requirements, 2100.1 F states, under Personnel Security, "Background investigation requirements for access to GSA information systems (including contractor operations containing GSA information) shall comply with GSA Order CIO P 2181.1, "GSA HSPD-12 Personal Identity Verification and Credentialing Handbook" and GSA Handbook ADM 9732.1C, "Suitability and Personnel Security."

# GSA HSPD-12 Handbook

**The GSA HSPD-12 Personal Identity Verification and Credentialing Handbook**, which provides the policies and procedures for issuing and maintaining GSA credentials, further clarifies who the policy applies to and what type of investigation is required for GSA IT Systems access. The policy states, "GSA employees and contractors requiring access to GSA IT systems and networks must have personnel investigations and other checks appropriate to the level of sensitivity and risk of those IT systems and their contents." The order also states, "Initial or full access to GSA Information Technology (IT) systems may be granted by the authorizing official for IT systems (known as the Designated Approving Authority (DAA). Authorizing officials may grant initial or full access to GSA IT systems after verifying through the GSA OCHCO/CPR that an employee or contractor has an Access National Agency Check and Inquiries (ANACI), National Agency Check with Law and Credit (NACLC), Single Scope Background Investigation (SSBI), or other acceptable level of investigation or clearance.

Any questions regarding the ePM access requirements or how to initiate a NACI background investigation, please contact the ePM Project Team at epmsupport@gsa.gov.

Please also take a moment to review the attached GSA Order PBS 3490.1A Document Security for Sensitive But Unclassified Building Information. This document outlines how Sensitive But Unclassified Information (SBU) is to be handled. Aggreement to GSA's Rules Of Behavior occurs when filling out an ePM External User Account Request form. The Rules of Behavior state that the user will follow the guidelines set forth in PBS 3490.1A.