

SECURITY & CMM CONTRACT REQUIREMENTS

SECURITY

As a condition for access to government-owned systems and data, all Contractor personnel must pass background investigations in accordance with OMB Circular A-130 which requires screening of all individuals involved with sensitive applications or data in Federal automated information systems. All SBA data and automated systems are considered sensitive. Investigations will be initiated by the OCIO's Office of Computer Security immediately upon assignment. The designated computer security staff will provide the appropriate forms to contractor personnel to begin the investigation. The Director, Office of Computer Security, will determine the type of background investigation required for each contractor assigned to this contract, based on the level of risk of the labor category. The Director or other designated computer security staff will review the results of the investigation and notify the Contractor if additional information, resulting from the investigation, is required. Unfavorable investigations can lead to immediate dismissal as directed by the Director, Office of Computer Security according to Security Policy Board Guidelines.

Contract personnel located at any government facility, in conjunction with this contract, shall be subject to the Standards of Conduct applicable to government employees. Contractor shall follow site specific regulations regarding access to classified or sensitive materials, access to computer facilities, and issuance of building access cards and badges. Data contained within all SBA computer systems are governed by Agency security regulations as well as the Federal Privacy Act of 1974. Contractor personnel assigned to this project will be held accountable for adherence to these regulations.

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201)' entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors."

All Offerors are advised that Homeland Security Presidential Directive-12 (HSPD-12) "Policy for a Common Identification Standard for Federal Employees and Contractors," and Federal

Information Processing Standard Publication 201 (FIPS 201), entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," establish the requirement for a Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. This is a mandatory requirement of all federal agencies.

The requirement is to be implemented in two phases. Phase I establishes a minimum standard for identity proofing, registration and card issuance/maintenance processes, effective October 27, 2005. Phase II implements a standard, interoperable ID card that contains identification data, biometrics, and PKI credentials for authentication purposes.

The Small Business Administration is currently developing its implementation guidance for both Phase I and Phase II of HSPD 12. That guidance will be disseminated when it is finalized. In the interim, offerors must anticipate Agency HSPD 12 requirements analogous to those in other federal agencies. This includes:

- Identification of risk and sensitivity levels for contractor positions and the duration of contractor staff appointments;
- Completion and favorable review of a security questionnaire form;
- Favorable review of fingerprint results;
- Favorable review of credit report, and
- Initiation and Completion of a Minimum Background Investigation (MBI).

Currently SBA designates all contractor positions as Moderate Risk and requires an MBI for all contractor employees. A pre-appointment procedure is required for all contractor personnel who cannot show positive results of a recent MBI or higher level investigation, such as a *Limited Background Investigation* or *Background Investigation*. A recent MBI is one that was successfully adjudicated within the last five years. The person in question must also have had no break of over two years in Federal employment as a contractor. This pre-appointment procedure must be completed with positive results before the contractor personnel can begin working under a contract for the Small Business Administration.

The pre-appointment procedure requires each employee of a contractor who will work under an SBA contract to complete OPM Form SF-85P (Questionnaire for Public Trust Positions) and SBA Form 2044 (Credit Report Release), as well as provide fingerprint impressions. Copies of the SF 85P and 2044 forms are available at www.opm.gov/forms/pdf_fill/SF85P.pdf and www.sba.gov/sops/3300/sop33002.pdf on page 297 of SOP 33 00 2 in Appendix 43, respectively.

In addition, the contractor personnel shall appear in person and provide two forms of identity source documents in original form to the SBA. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification.

Please note that it may take up to 60 days for the SBA to conduct and complete this pre-appointment procedure for each contractor employee. Also, with the passage of the [Federal Information Security Management Act \(FISMA\) of 2002](#), there is no longer a statutory provision to allow for agencies to waive mandatory FIPS.

Information on FIPS 201 is available at:
<http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf>.

SBA MANAGEMENT OFFICIALS

The contractor's Project Manager (PM) will be responsible for removing any employee whose work product or conduct does not meet SBA's standards. If within one day of official notification by SBA, the PM fails to take remedial action with the employee or within ten business days the employee's work products continue to not meet SBA standards for quality, timeliness and quantity SBA's Contracting Officer will issue a letter informing the Contractor that the contractor's performance is endangered and that unless the condition is cured the contractor shall be removed from the contract.

CONTRACTORS CMM LEVEL OF PERFORMANCE

CMMI Background: Capability Maturity Model[®] Integration (CMMI) is a process improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. The effort to define and develop the CMMI is being sponsored by the Office of the Secretary of Defense/Acquisition, Technology and Logistics (OSD AT&L). The Industry sponsor is the Systems Engineering Committee of the National Defense Industrial Association (NDIA). The effort includes the design, implementation, transition and sustainment efforts. The CMMI project is a collaborative effort with participation by OSD, the Services, other government agencies, industry through the National Defense Industrial Association (NDIA) Systems Engineering Committee, and the Software Engineering Institute (SEI) of Carnegie Mellon University.

Bodies of knowledge available in CMMI Models include:

- Systems Engineering (SE);
- Software Engineering (SW);
- Integrated Product and Process Development (IPPD);
- Supplier Sourcing (SS).

The Legacy CMMs:

- Capability Maturity Model for Software (SW-CMM);
- Systems Engineering Capability Maturity Model (SE-CMM);
- Integrated Product Development Capability Maturity Model (IPD-CMM) are incorporated into CMMI.

Information on CMMI is available at: <http://www.sei.cmu.edu/cmmi/>

Requirements: SBA recognizes that CMMI offers a common integrated vision of improvement for all elements of organization and increased focus and consistency in:

- requirements development and management;
- systems design and development;
- systems integration;

- risk management; and
- performance measurement and analysis.

SBA deems it essential that their contractor workforces are able to achieve, sustain and improve their CMMI level of performance. This continuous sustaining and improving characteristic emanates from top management's commitment to improvement and the ongoing education and training of all employees in the workforce.

The contractors must be Carnegie Mellon University Software Engineering Institute (CMU/SEI) CMMI-Level 2 or better for software development and/or systems engineering (SW/SE). The contractors must provide proof of company assessments/appraisals conducted by a CMU/SEI-authorized SCAMPI (the Standard CMMI Appraisal Method for Process Improvement) Lead Appraiser resulted in Maturity Level 2 or better for CMMI-SW/SE. Optionally, contractors are encouraged to identify and provide information on two (2) recent projects using CMMI level 2 standards. In case of an offeror without a relevant past performance, the offeror may not be evaluated favorably or unfavorably on this optional criterion and will receive a neutral rating.

The SEI Appraisal Program oversees the quality and consistency of the SEI's process appraisal technology and encourages its effective use. The SCAMPI is designed to provide benchmark quality ratings relative to CMMI model. Further information on how to get your projects appraised by an SEI-authorized SCAMPI Lead Appraiser is available at: <http://www.sei.cmu.edu/cmml/appraisals/appraisals.html>, including the SCAMPI Lead Appraiser Directory. The intent of the acquisition of a CMMI-SE/SW Level 2 or better contractor is to ensure that the Contractor recognizes its responsibility and accountability for the performance of the contractor staff.

The Contractor must identify their documented policies and procedures relevant to the Statement of Need and Performance Required Objectives contained in the PWS.