National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

CRITERIA FOR COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSFC) SOLUTION INTEGRATORS

These criteria and processes are defined to provide a common baseline for CSfC solution integrators, enabling NSA, Authorizing Officials (AOs), and Designated Approving Authorities (DAAs) to assess the capabilities of solution integrators and accept their results.

Commercial Solutions for Classified Program Management Office (CSfC PMO)
V 2.1 13 August 2014

Criteria For CSfC Integrators

Contents

Introduction 3

1. Criteria for CSfC Integrators 3

1.1. Organization 3

1.1.1. Additional Management Requirements 4

1.1.2. Access to Secure Facility 4

1.1.3. Required Information 4

1.1.4. Test Methodology 4

1.1.5 Memorandum of Agreement 5

1.2. Personnel 5

1.2.1. Capability Assembly and Configuration 5

1.2.2. Capability Testing 6

1.2.3. Capability Documentation 6

1.2.4. Personnel Clearances 6

2. CSfC Integrator Application: Required Information 7

Table 1: Department of Defense (DoD) Approved Baseline Certifications 5

Criteria For CSfC Integrators

Introduction

NSA's Commercial Solutions for Classified Program Management Office (CSfC PMO) provides the following criteria to establish a baseline for CSfC integrators. Integrators who demonstrate compliance to these criteria and sign a Memorandum of Agreement (MoA) with NSA have the option to be listed as CSfC Integrators on www.nsa.gov.

A CSfC Integrator is defined as an organization that meets the following criteria and is qualified to assemble and integrate components according to a CSfC Capability Package (CP), test the resulting solution, provide a body of evidence to the solution Authorizing Official (AO)/Designated Approving Authority (DAA), maintain the solution, and be the first line of response in troubleshooting or responding to security incidents.

To perform these tasks, the organization shall have demonstrated experience in system integration, with the technologies to be integrated, in formal testing processes, and in evidence generation for system authorization.

1. Criteria for CSfC Integrators

These criteria cover two areas, organizational criteria and personnel criteria. In general, the integrator must be prepared to demonstrate that they have the staff and processes in place to architect, design, integrate, test, document, field, and support systems that meet the requirements of the CSfC program. The sections below highlight applicable standards that can be used to demonstrate compliance. Evidence of compliance must be provided upon request. Alternatively, a potential CSfC integrator may proffer other or additional standards in their place to demonstrate the quality of their processes and staff.

1.1. Organization

The organization shall comply with one or more of the following standards:

- The management and technical (minus calibration) requirements of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17025:2005, "General requirements for the competence of testing and calibration laboratories,"
- National Voluntary Lab Accreditation Program according to NIST Handbook 150
- ISO9000, Quality Management Systems
- Capability Model Maturity Integration (CMMI)

NSA will assess, based on Integrator input, whether organizations meet the criteria for CSfC Integrators. NSA may periodically have the integrators' processes and facilities inspected to ensure the criteria continue to be met.

1.1.1. Additional Management Requirements

a) The organization shall ensure that objective personnel are used to test the integrated system – separate from the personnel who assemble and configure the system.

b) The management system shall include policies and procedures to ensure the protection of information. Only persons authorized to work on a particular integration activity shall have access to related information.

c) The integrator shall maintain a record-keeping system that is used to track each effort. Records shall be complete with enough data to allow an independent body to review and concur with the work performed.

d) All solution integration efforts shall follow a current National Security Agency (NSA)/Information Assurance Directorate (IAD) approved Capability Package (CP) or have pre-authorization from NSA/IAD for a particular case to work in accordance with a pre-release CP. (Solution registration will be accepted only against a final CP.)

1.1.2. Access to Secure Facility

It is not required that the integrator have a secure facility. However, the integrator must have access to a secure facility where they can receive classified risk assessments and test for classified vulnerabilities if needed. The facility clearance shall be equivalent to the level of data to be processed by the solution.

1.1.3. Required Information

a) Organizations seeking recognition as a CSfC Integrator shall provide documented evidence of compliance to these criteria by submitting the attached application to CSfC_integrators@nsa.gov.

b) Organizations who submit an application will be required to participate in a meeting at NSA to review and answer questions regarding the application.

c) Organizations shall submit documentation to NSA/IAD at least annually to confirm continued compliance to these criteria.

1.1.4. Test Methodology

CSfC Capability Packages provide guidelines for the development of a Test & Evaluation (T&E) Plan and Procedures. Integrator testing shall include the following:

a) Integration Testing – Integration testing shall focus on the flow of data between CSfC solution components.

b) System Testing – System testing shall test all requirements in the Capability Package on a documented end to end commercial solution.

c) Security Testing – Security testing shall verify all security requirements.

d) Penetration Testing – Penetration testing shall validate how the system functions when presented with unexpected input. The sufficiency of penetration testing should be agreed to by the integrator and the customer.

1.1.5 Memorandum of Agreement

After NSA reviews the integrator's application and conducts a face to face meeting (as described in Section 1.1.3) with the integrator to confirm the integrator meets the criteria, NSA and the integrator will enter into a Memorandum of Agreement (MoA).

1.2. Personnel

The integrator shall employ managerial and technical personnel to fulfill a number of roles per these criteria. Specific to the focus of this work, personnel performing, supervising, auditing, or providing quality control of these efforts shall hold at least one of the following certifications in the appropriate column as specified in Sections 1.2.1 and 1.2.2.

IAT Level I	IAT Level II	IAT Level III
A+ CE	GIAC Security Essentials (GSEC)	CISA (with hands-on experience)
Network+ CE	Security+ CE	CISSP (with hands-on experience)
SSCP (with hands-on experience)	SSCP (with hands-on experience)	CASP
		GIAC Certified Incident Handler (GCIH) (with IAT Level II)
		GIAC Certified Enterprise Defender (GCED)

Table 1: Department of Defense (DoD) Approved Baseline Certifications (modified)

1.2.1. Capability Assembly and Configuration

The role of the capability assembly and configuration personnel is to select and procure CSfC components.

All personnel assigned to assemble and configure the solutions shall be knowledgeable in computing and network environments. They shall comply with the Information Assurance

Technical (IAT) Level II criteria which require at least one of the certifications indicated in Table 1. Additionally, the individuals assembling and configuring the solutions should have certifications in the components being integrated. Updated certification requirements can be found at http://iase.disa.mil.

1.2.2. Capability Testing

The developer of test plans and reports shall be IAT Level III and shall have additional experience/training in the devices being integrated. The personnel conducting the testing shall be at least IAT level I.

Personnel shall have experience in the required component and system testing.

1.2.3. Capability Documentation

Technical writers and editors shall be employed to produce complete documentation of the effort.

Documentation to be prepared shall include, but is not limited to:

a) Solution components and configuration baseline

b) Certificate Policy (CP)/Certification Practice Statement (CPS)

c) Test Plan and Test Procedures, per guidance provided in the Capability Package

d) Final Test Report to include security and non-security discrepancies

e) Other documentation as required by the AO/DAA

1.2.4. Personnel Clearances

Integrator personnel responsible for integrating, testing, maintaining, and responding to security incidents shall hold clearances that enable them to receive risk assessments and adequately address vulnerabilities: Clearances for at least one team member shall be equivalent to the level of data to be processed by the solution.

2. CSfC Integrator Application: Required Information

Please email the following application to CSfC_integrators@nsa.gov to demonstrate and document compliance with these requirements:

1. Legal name and full address of the integrator:
2. If your organization has foreign ownership, please cite your proxy or SSA (Special Security Agreement) number from the Defense Security Service (DSS):
3. Authorized representative's name and contact information:
4. Does your organization meet ISO/IEC 17025:2005, ISO9000, the National Voluntary Lab Accreditation Program, or CMMI? Y/N
5. Facility clearance level for your organization:
6. Titles, certification, and clearance information for personnel filling key roles identified in the criteria (integration, testing, documentation, incident response):

Title	Certifications	Clearance

7. Please cite your organization's relevant prior experience, to include technologies, capability packages, component and system testing. Please cite your organization's prior experience with CSfC.
8. Please cite previous customers who have employed your integrator expertise, particularly with CSfC solutions: