NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

CYBERSECURITY
CAPABILITIES

Commercial Solutions for Classified

harnessing the power of commercial industry

Criteria for 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

Version 2.3
February 2023

Criteria for CSfC Integrators

Contents

Criteria for CSfC Integrators

Introduction

NSA's Commercial Solutions for Classified Program Management Office (CSfC PMO) provides criteria to establish a baseline for CSfC Trusted 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 Trusted Integrators on www.nsa.gov.

A CSfC Trusted 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 Trusted Integrators

The criteria to qualify as a CSfC Trusted Integrator covers two areas: organizational and personnel criteria. The integrator must 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 define applicable standards that 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

1.1.1. Standard Requirements

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 Trusted Integrators. NSA may periodically have the integrators' processes and facilities inspected to ensure the criteria continue to be met.

Criteria for CSfC Integrators

1.1.2. Additional Management Requirements

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

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

c) The organization shall maintain a record-keeping system that tracks each effort, and records shall include 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)/Cybersecurity Directorate (CSD) approved CP or have authorization from NSA/CSD for a particular case to work in accordance with a pre- release CP. (Solution registration will be accepted only against a published CP.)

1.1.3. 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 to 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.

1.1.4. Required Information

a) Organizations seeking recognition as a CSfC Trusted Integrator shall provide documented evidence of compliance to the criteria by submitting the application in Section 2 to CSfC_integrators@nsa.gov.

b) Organizations who submit an application will be required to participate in a meeting with NSA to review and answer questions regarding the application. If an organization's application is denied as a CSfC Trusted Integrator, they can re-apply in six months.

c) Once the criteria is successfully met, organizations shall submit documentation to NSA/CSD when requested to confirm continued compliance to the criteria.

1.1.5. Test Methodology

CSfC Capability Packages provide guidelines for development of a Test & Evaluation (T&E) Plan and Procedures. CSfC Trusted 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 CP 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 Trusted Integrator and the customer.

1.1.6. Memorandum of Agreement

After NSA reviews the organization's application and conducts a meeting (as described in Section 1.1.4) with the applicant to confirm that the criteria has been met, NSA and the integrator will enter into a MoA.

1.2. Personnel

The organization shall employ managerial and technical personnel to fulfill a number of roles. Specific to the focus of this work, personnel performing, supervising, auditing, or providing quality control 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 8570 Baseline Certifications (modified)
Here is the full list of IAT Certifications: https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/

1.2.1. Capability Assembly and Configuration

The capability assembly and configuration personnel select and procure CSfC components.

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

Criteria for CSfC Integrators

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 https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/

1.2.2. Capability Testing

The developer of test plans and reports shall be IAT Level III and 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 shall include, but is not limited to:

a) Solution components and configuration baseline

b) Certificate Policy/Certification Practice Statement (CPS)

c) Test Plans 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

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.

Criteria for CSfC Integrators

2. CSfC Trusted 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 organization:
2. If your organization has foreign ownership, 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. Cite your organization's relevant prior experience, to include technologies, capability packages, component and system testing. Cite your organization's prior experience with CSfC.
8. Cite previous customers who have employed your integrator expertise, particularly with CSfC solutions: