

# Commercial Solutions for Classified (CSfC) Customer Handbook Version 1.1

---

**This page is intentionally left blank.**

**Table of Contents**

- I. Introduction ..... 1
- II. Purpose ..... 1
- III. Audience ..... 1
- IV. CSfC Artifacts and Location ..... 2
- V. CSfC Process ..... 3
  - A. Customer Has an IA Requirement..... 3
  - B. Download Capability Package and Request Risk Assessment ..... 3
    - 1. Applicable Capability Package Available ..... 3
    - 2. No Applicable Capability Package Available ..... 3
    - 3. Request Risk Assessment ..... 4
  - C. Comply with CSfC Capability Package ..... 4
  - D. Register Solution ..... 4
  - E. Perform System Certification & Accreditation ..... 5
  - F. Maintenance ..... 5
  - G. Annual Re-assessment and De-registration..... 5
- VI. Contact Information..... 6

## **I. Introduction**

The Commercial Solutions for Classified (CSfC) process enables commercial components to be used in layered solutions to protect classified National Security Systems (NSS) information. The NSA provides architectures, component criteria, and configuration of the solution to meet an Information Assurance (IA) requirement. The CSfC process also includes the means for vendors to get their components on the CSfC Components List, making them eligible for use in a CSfC solution.

## **II. Purpose**

This document serves as a guide for customers of CSfC artifacts to include Capability Packages, CSfC Components List, Registration and Life Cycle Support resources. Once a Capability Package is published to the public Internet, customers are able to “download and go.” But what does this actually mean? This document will explain the customer process from the time the customer believes it has a CSfC requirement to fielding and life cycle support.

This document is intended to provide the process for customers to follow, identify the location and use of each CSfC artifact, and explain expectations for successful navigation through the road to approved composed solutions that protect classified information and systems.

## **III. Audience**

Customers of the Capability Package are typically the U.S. Government Client who will be implementing and managing the solution. However the contents of a Capability Package may be useful to the accreditor, system integrator, and vendor/component developer.

Accreditor - The Authorizing Official/Designated Approving Official (AO/DAO) uses the Capability Package to understand and facilitate the collaboration between the owners and developers and ultimately determine whether the solution provides an acceptable level of risk.

System Integrator - System integrators integrate a CSfC solution per the Capability Package and customer requirements. Integration of the CSfC solution includes selection of the components of the CSfC solution from the CSfC Components List, in accordance with the restrictions in the Capability Package, and testing of the CSfC solution per the Capability Package. Integrators should ensure that the component selection and configurations provide acceptable functionality, security, and risk levels.

Vendor/Component Developer - Vendors may review the Capability Package to understand how the component could be used in the architecture provided in the Capability Package. However, in order to be used within a CSfC solution a component vendor will undergo the CSfC process for use in a composed solution rather than one component vendor developing an entire CSfC solution. This follows the general tenets of independence that serves as one of the foundational components of the CSfC process.

Vendors who wish to have their components eligible as CSfC components of a composed, layered IA solution must have their component evaluated per the National Information Assurance Partnership

(NIAP) process in accordance with the applicable U.S. Government Protection Profile(s), undergo the Federal Information Processing Standards validation process, and undergo interoperability testing when it is established. Additionally, the CSfC program requires a vendor to enter into a Memorandum of Agreement (MOA) with NSA. The MOA obligates the company to provide sufficient information for NSA to make a risk decision, and to cooperate with NSA to mitigate any discovered vulnerabilities that would impact the risk management posture of the CSfC solution, both initially and throughout the component's life cycle.

Once a component has met the requirements, NSA will add it to the CSfC Components List so the component is eligible for use in an approved CSfC solution. These components become the building blocks for CSfC solution providers to create solutions.

#### **IV. CSfC Artifacts and Location**

This section provides the definition and location of unclassified CSfC artifacts.

##### CSfC Solution

- Integration of multiple components from the CSfC Components List, each providing/supporting a layer of protection
- Compliant with applicable CSfC Capability Package
- Approved by NSA for the protection of classified data/systems if compliant with the CSfC Capability Package

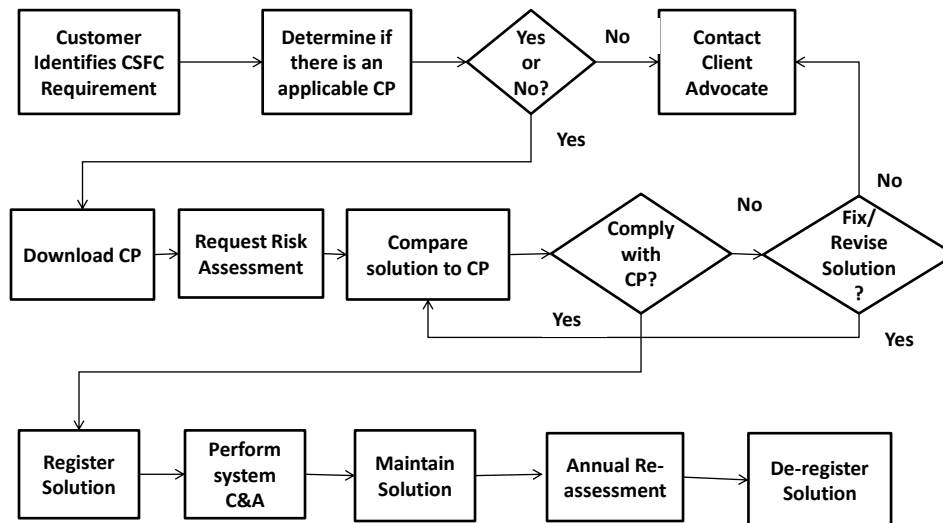
CSfC Components List – List of products eligible for use as components in a CSfC solution. Available CSfC components will be located at [http://www.nsa.gov/ia/programs/csfc\\_program](http://www.nsa.gov/ia/programs/csfc_program). To request that a component be considered for the “CSfC Components” list a vendor can download and complete a questionnaire located at [http://www.nsa.gov/ia/files/bao/csfc\\_questionnaire.pdf](http://www.nsa.gov/ia/files/bao/csfc_questionnaire.pdf).

CSfC Prototype Solution – This is a CSfC solution developed by National Security Agency (NSA), with a partner, to acquire knowledge for incorporation into a CSfC Capability Package. CSfC prototype solutions can be approved by NSA for use by the partner for a specified period of time. The prototypes will not be located on the public website.

##### CSfC Capability Package contains:

- Architecture and description of a CSfC solution
- Requirements for component selection, configuration, keying and testing
- Rules on use of CSfC solution and its life cycle support
- Risk assessment stating the residual risk (classified)

## V. CSfC Process



### A. Customer Has an IA Requirement

The unclassified portion of the NSA approved Capability Packages are published on NSA's Internet site. Customers who have an IA requirement that can be met using a CSfC solution will need to visit the CSfC Program website ([http://www.nsa.gov/ia/programs/csfc\\_program](http://www.nsa.gov/ia/programs/csfc_program)) to determine if there is an approved Capability Package that meets the requirement. The sections below address how the various customer types would use data within the Capability Package.

### B. Download Capability Package and Request Risk Assessment

#### 1. Applicable Capability Package Available

Customers should select the Capability Package that will best meet their needs. Customers can use the Capability Package to understand the capability that could be provided and restrictions on how it can be used. When choosing a Capability Package, keep in mind that a Capability Package is developed for a specific type of capability.

#### 2. No Applicable Capability Package Available

If there is no available Capability Package, the current Capability Package is not applicable to the solution, or the Capability Package cannot be applied in a manner that would produce a compliant solution, the client must contact the NSA Client Advocate (CA) requesting NSA support to the CSfC requirement. The customer will submit an IA requirement for development of a solution by documenting the requirement in a Requirements Scoping Questionnaire. In addition to sufficient detail in the questionnaire, the customer/client/agency must submit all relevant supporting documentation to

the Client Advocate. The CA will coordinate internally to determine if the requirement should be handled through the CSfC process or another better suited process.

If the requirement is a CSfC solution, then the client will go through the CSfC prototyping phase. An acceptable prototype should present a capability with sufficient deltas from the current Capability Packages and previously approved prototypes. An approved prototype must become compliant with the Capability Package within two years, unless stated otherwise in the prototype approval letter.

### **3. Request Risk Assessment**

After downloading a Capability Package, the customer must also request a copy of the risk assessment for that Capability Package by contacting the NSA IAD Client Advocate. The Risk Assessment is a separate document that supplements the Capability Package.

The risk assessment documents the threats, mitigations, and residual risks associated with CSfC solutions based on a Capability Package. It contains classified information and therefore is not included within the unclassified portion of the Capability Package. It informs the AO/DAO and potential customers of the residual risks with implementing a solution. The additional controls recommended within the risk assessment can be implemented by a customer to further reduce residual risks.

### **C. Comply with CSfC Capability Package**

It is expected that customers will obtain the current versions of both the Capability Package and the associated Risk Assessment document as necessary and will verify that they have reviewed the current version.

To comply with a Capability Package, it is required that the AO/DAO thoroughly reviews the risk assessment and determines that the residual risks are acceptable for the system implementing the CSfC solution. It is strongly recommended that others associated with the system also review the risk assessment.

If the customer builds the solution and identifies an issue designing a technologically feasible solution in accordance with the Capability Package requirements, the customer may determine to modify the design to be compliant with the solution. If after the revision or fix to the solution the customer is not able to comply with the Capability Package, the customer should contact the NSA Client Advocate.

### **D. Register Solution**

The customer/DAO will download the registration form from [http://www.nsa.gov/ia/programs/csfc\\_program/index.shtml](http://www.nsa.gov/ia/programs/csfc_program/index.shtml). Each registration form is specific to a particular Capability Package thereby requiring different information. In order to accurately complete the form the customer should have detailed architecture and component information for each solution. The form requests the following data at a minimum:

- DAO POC
- Integrator POC
- Operational POC

- Components selected from the CSfC Components List and their purpose within the architecture

By signing and submitting the form, the AO/DAO certifies to NSA that the solution is fully compliant with the Capability Package and that AO/DAO accepts the residual risks provided with the Capability Package or has mitigated those risks to an acceptable level.

### **E. Perform System Certification & Accreditation**

The system containing the CSfC solution undergoes certification and accreditation (C&A) per the process applicable to the customer. At this point the CSfC solution is operational.

### **F. Maintenance**

Once a solution is fielded the customers must maintain the security of the solutions by implementing updates, responding to alerts, and reporting incidents.

NSA Responsibilities:

- Provide the incident reporting process to the customers
- Provide customers with CSfC alerts, including Capability Package updates, additional risk data, or direction to change the solution based on additional information
- Provide incident analysis as needed

Customer Responsibilities:

- Report security incidents to NSA
- Process CSfC alerts from NSA
- Implement component updates
- Apply patches

### **G. Annual Re-assessment and De-registration**

Prior to the expiration of the CSfC solution registration, the customer will need to determine if the CSfC solution in operational use complies with the latest version of the applicable Capability Package. Capability Packages include requirements that the customer can use to assess against to determine compliance. If the CSfC solution is compliant, the customer will re-register the CSfC solution and obtain approval for another year. If the CSfC solution is not compliant, the customer will re-register the CSfC solution, stating that it is not compliant, and will obtain approval for one year, on the condition that the customer will bring the CSfC solution into full compliance as quickly as possible, not to exceed six months.

When the customer no longer needs the CSfC solution, the customer will de-register the CSfC solution using the solution number, which was provided when the solution was registered.



## **VI. Contact Information**

Please direct all inquiries related to the CSfC process and program to [csfc@nsa.gov](mailto:csfc@nsa.gov).