National Security Agency/
Central Security Service

CYBERSECURITY
SOLUTIONS

COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC) CUSTOMER HANDBOOK

Last Updated 07/22/2021

Table of Contents

1 INTRODUCTION

What is Commercial Solutions for Classified (CSfC)?

The National Security Agency (NSA) Commercial Solutions for Classified (CSfC) Program enables commercial products to be used in layered solutions leveraging industry innovation in order to protect classified National Security Systems (NSS) data. This provides the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.

NSA has developed, approved and published solution-level specifications called Capability Packages (CPs), and works with technical communities from across the industry, government, and academia to develop and publish product-level requirements in US Government Protection Profiles (PPs). CPs for Mobile Access (MA), Campus Wireless LAN, Multi-Site Connectivity (MSC) and Data at Rest (DAR) solutions are listed on the CSfC website here:

https://www.nsa.gov/CSfC/

2 PURPOSE

The CSfC handbook serves as a quick reference guide for clients, Commercial Component Developers, and Trusted Integrators (TI). The information contained herein will help explain the processes for these stakeholders.

3 AUDIENCE

U.S. Government Client

Typical CSfC clients include Department of Defense, Intelligence Community, Military Services, and other Federal Agencies. These NSS stakeholders utilize CSfC's CPs to rapidly implement commercial cybersecurity solutions to achieve their mission objectives.

Trusted Integrator

TIs support NSS clients with the implementation of CSfC CPs. TIs specialize in architecting together CSfC components in accordance with the CSfC CPs to ensure secure and proper solution functionality. The NSA CSfC Program Management Office (CSfC PMO) provides criteria and processes to establish a common baseline for TIs. This enables the NSA and AOs/Designated Approving Authorities (DAAs) to assess the capabilities of solution integrators and accept their results. TIs that demonstrate compliance with these criteria and sign a Memorandum of Agreement (MoA) with NSA have the option to be listed as a CSfC TI. Criteria for TIs can be located under the TI list on the CSfC Webpage here:

https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Trusted-Integrator-List/

Commercial Component Developer

Commercial component developers (i.e., vendors) who wish to have their products listed as CSfC approved components must build their products in accordance with the applicable U.S. Government/collaborative PPs and submit their products for evaluation using the Common Criteria Process. The CSfC components list can be viewed here:

https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/

Authorizing Official/Designated Approving Authority (AO/DAA)

The AO/DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

4 CSFC CAPABILITY PACKAGES

CPs are the foundation of the CSfC Program. These can be customized to the client's needs in order to help them achieve their mission objectives. CPs provide designs that allow the client to independently implement secure solutions using approved layered Commercial Off-the-Shelf (COTS) products. These are vendor-agnostic and provide high-level security and configuration guidance for the client and/or TIs. CPs are updated biannually or as warranted. Currently these are listed on the CSfC webpage here:

https://www.nsa.gov/resources/everyone/csfc/capability-packages

Described below in sections 4.1 – 4.4 are the National Manager approved CPs.

4.1 Mobile Access (MA) CP

The MA CP describes how to protect classified data in MA solutions transiting wired networks, domestic cellular networks, and trusted wireless networks to include government private cellular networks and government private Wi-Fi networks.

An MA solution protects classified information as it travels across either an untrusted network or a network consisting of multiple classification levels. This solution supports connecting end-user devices (EUDs) to a classified network via two layers of encryption terminated on the EUD provided that the EUD and the network operate at the same security level.

An MA solution uses two nested, independent tunnels to protect the confidentiality and integrity of data (including voice and video) as it transits the untrusted network. This solution utilizes Internet Protocol Security (IPSec) as the outer tunnel and, depending on the solution design, IPsec or Transport Layer Security (TLS) as the inner layer of protection.

- The MA CP can be viewed here:

https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/capability-packages/#mobile-access

• MA Compliance Checklist can be viewed here:

https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

• MA Solution Registration Form can be downloaded here:

https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

4.2 Campus Wireless Local Area Network (WLAN) CP

The Campus WLAN CP meets the demand for commercial End User Devices (EUDs) (i.e., tablets, smartphones, and laptop computers) to access secure enterprise services over a campus wireless network. Cryptographic algorithms, known as Commercial National Security Algorithm (CNSA) Suite, are used to protect data using layers of Commercial off the Shelf (COTS) products. This solution enables the client to implement layered encryption between a secure network and EUDs.

This CP provides a reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List for their Campus WLAN solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit.

- Campus WLAN CP can be viewed here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/capability-packages/#wlan

- Campus WLAN Compliance Checklist can be viewed here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

- Campus WLAN Solution Registration Form can be downloaded here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

4.3 Multi-Site Connectivity CP (MSC)

The MSC CP describes a general MSC Solution to protect classified information as it travels across either an untrusted network or a network of a different security level. The solution supports interconnecting two or more networks operating at the same security level via encryption tunnels, where the security level encompasses the classification level, list of compartments, dissemination controls, and other such controls over information. The solution provides sufficient flexibility to be applicable to many use cases of MSC implementations.

The MSC solution uses two nested, independent encryption tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two encryption tunnels protecting a data flow can use either IPsec generated by a Virtual Private Network (VPN) Gateway or Media Access Control Security (MACsec) generated by a MACsec Device. VPN Gateways and MACsec Devices are implemented as part of the network infrastructure.

- The MSC CP can be viewed here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/capability-packages/#multi-site

- The MSC Compliance Checklist can be viewed here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

- The MSC Solution Registration Form can be downloaded here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

4.4 Data at Rest (DAR) Solution CP

The DAR CP meets the demand for DAR solutions using the Commercial National Security Algorithm (CNSA) Suite. These algorithms are used to protect up to top secret data using layers of COTS products. The DAR CP enables the customers to implement two independent layers of encryption for the purpose of providing protection for stored information on the End User Device (EUD) or DAR protected system, while in a powered off or unauthenticated state.

This CP provides high-level reference designs and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List for their DAR solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while at rest.

- DAR CP can be viewed here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/capability-packages/#data-at-rest

- DAR Compliance Checklist can be viewed here:

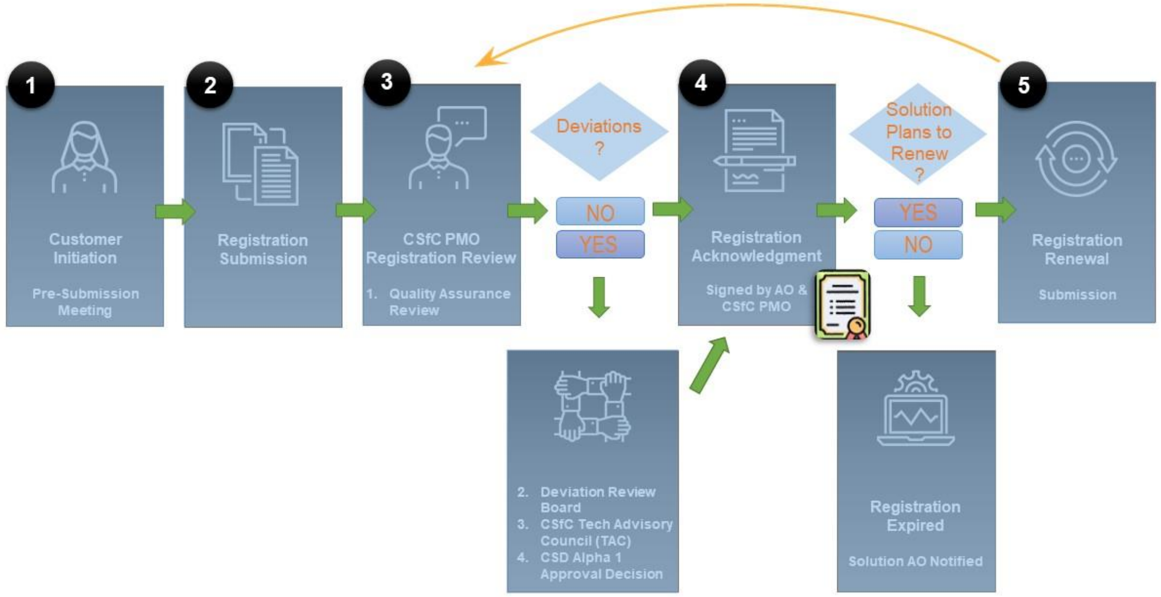
  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

- DAR Solution Registration Form can be downloaded here:

  https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

5 CSFC SOLUTION REGISTRATOIN AND APPROVAL PROCESS

The flowchart below captures the overall CSfC approval process from the initial development/publication of the CP to the final connection approval decision by the relevant AO/DAA.


1
Customer Initiation
Pre-Submission Meeting
2
Registration Submission
3
CSfC PMO Registration Review
1. Quality Assurance Review
Deviations ?
NO
YES
2. Deviation Review Board
3. CSfC Tech Advisory Council (TAC)
4. CSD Alpha 1 Approval Decision
4
Registration Acknowledgment
Signed by AO & CSfC PMO
Solution Plans to Renew ?
YES
NO
Registration Expired
Solution AO Notified
5
Registration Renewal
Submission

5.1 Review of Published CPs

Customers are strongly encouraged to email csfc_register@nsa.gov early on to advise NSA that they plan to register a solution for approval before finalizing their design. NSA has developed CPs for our customers with ready access to the information needed to satisfy their operational requirements, and publishes them on the unclassified NSA website. Customers should check the CSfC CPs on the site to see if there is an existing CP that meets their needs.

For information or assistance in determining whether an approved CP satisfies their requirements, customers (e.g., Department of Defense Components, Intelligence Community Organizations, and Federal Agencies) may engage NSA through their designated NSA client advocates and the NSA client contact center which can be viewed here:

https://www.nsa.gov/about/contact-us/#subject:iad

Appropriately cleared personnel can request a classified risk assessment on SIPRNet: https://www.iad.nsa.smil/iaservices/commercial-solutions-for-classified-program or JWICS: https://www.iad.nsa.ic.gov/iaservices/commercial-solutions-for-classified-program. Please be advised that these links only work on either the SIPRNET or JWICS classified networks, and requires users to have authorized access to those respective systems.

5.2 Client Builds/Tests Solution

CSfC strongly encourages, but does not mandate, customers to work with a Trusted Integrator (TI) while designing, building, and testing a CSfC-compliant solution based upon one or more of the published CPs. Customers of the solution are responsible for obtaining, under their organization's established accreditation and approval processes, certification and accreditation of the customer's implementation of the CP.

For the latest CPs please visit: https://www.nsa.gov/Resources/Commercial -Solutions-for-Classified-Program/Capability-Packages/

5.3 Solution Registration

Per CNSSP No. 7, all CSfC solutions operating on, or protecting, NSS information must be registered with NSA. To complete the solution registration form, an assigned Solution Registration Identification Number must be obtained from the CSfC PMO. Registrations will be processed only after all required forms are submitted and validated. All NSS customers are required to submit the appropriate CP-specific Compliance Checklist with their AO signed registration form, deviation forms (if applicable), and network diagrams. Please provide brief, specific responses in the compliance checklist to explain how your solution is compliant with the requirements.

By signing the registration form the AO is either: asserting compliance with the published CP and acknowledging/accepting the risk of fielding a CSfC solution; or acknowledging inclusion of the appropriate CP deviation approval signed by NSA and acknowledging/accepting the risk of fielding a CSfC solution.

For verification of the following items listed below, please email the CSfC PMO at csfc_register@nsa.gov. Customers, Commercial Component Deveopers, and TIs can download the specific registration form here: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/

5.4 Solution Approval

The AO/DAA will confirm after customer testing that the checklist is accurate and will then sign the CSfC registration form. The AO/DAA submits the signed form, compliance checklist, deviation form (if applicable), and network diagrams to NSA. Upon verifying compliance, NSA will provide a letter acknowledging the registration for a specific time period (typically for 1 year).

5.5 AO Authorization

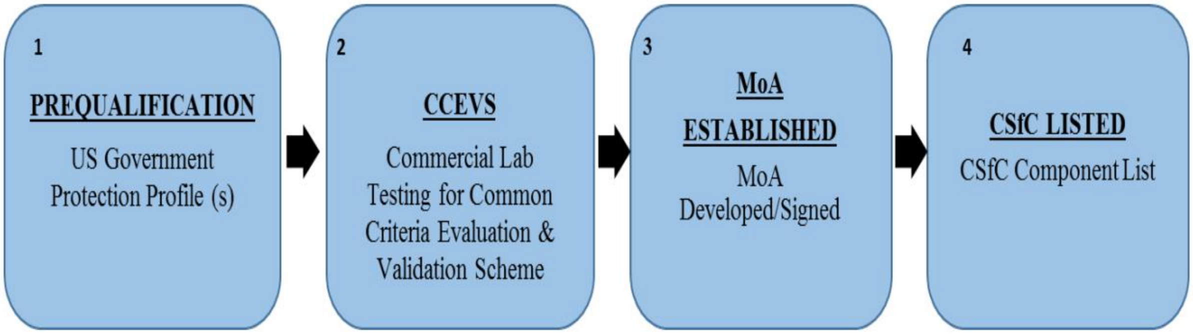
The AO/DAA will make the determination to field the solution.

5.6 Registration Renewal Process

The CSfC PMO will send out 120-day, 60-day, and 30-day notifications preceding the expiration of the CSfC solution registration. The customer will need to re-register their solution against the latest version of the applicable CP before expiration. The customer must submit updated registration and compliance checklist forms. If the forms are classified; the client will notify the CSfC PMO for suitable sending instructions. Email them to: csfc_register@nsa.gov. Failure to re-register shall result in the expiration of the customer's solution registration from NSA.

6 COMMERCIAL COMPONENT DEVELOPER ENGAGEMENT

The flowchart below captures the overall process for Commercial Component Developers who wish to have their products eligible as CSfC components of a composed, layered cybersecurity solution.


1
PREQUALIFICATION
US Government Protection Profile (s)
2
CCEVS
Commercial Lab Testing for Common Criteria Evaluation & Validation Scheme
3
MoA ESTABLISHED
MoA Developed/Signed
4
CSfC LISTED
CSfC Component List

6.1 Prequalification

Commercial Component Developers who wish to have their products eligible to become CSfC components of a composed, layered cybersecurity solution must build their products in accordance with the applicable US Government PPs. It is the Commercial Component Developer's responsibility to correctly implement the commercial standards that are referenced in the PPs to enable interoperability.

6.2 Common Criteria Evaluation and Validation Scheme (CCEVS)

The Commercial Component Developers will submit their product using the Common Criteria Process to obtain NIAP certifications. To view current and in development listings of NIAP approved U.S. Government PPs, use link provided here: https://www.niap-ccevs.org

6.3 Memorandum of Agreement (MoA) Established

Interested Commercial Component Developers must complete and submit a CSfC questionnaire for each product.

The CSfC PMO will notify the company and initiate the MoA. The MOA specifies that the Commercial Component Developer's product must be NIAP certified, FIPS certified, and that the Commercial Component Developer agrees to fix vulnerabilities in a timely fashion. It may also list other specific requirements for that specific technology. The CSfC questionnaire can be viewed here: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/. Please submit completed questionnaires to csfc_components@nsa.gov.

6.4 CSfC Component Listed

Once components meet the approved requirements set by NSA, then the Commercial Component Developer and NSA will sign the MoA. NSA will then list them on the CSfC Components List.

7 TRUSTED INTEGRATOR (TI) APPLICATION

Companies and organizations that are interested in becoming a TI should submit a completed integrator application form located here: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Trusted-Integrator-List/. Once completed, the TI should email the completed form to CSfC_integrators@nsa.gov. Applications will be reviewed & if the criteria are met, the CSfC PMO will schedule a meeting. This meeting between the CSfC PMO and the company will be an opportunity to discuss the application responses in detail.

Following the meeting, a determination will be made by the CSfC PMO as to whether the company has indeed satisfied the application criteria. The CSfC PMO will notify the company and initiate the MoA. Once the MoA has been signed by all parties, the company will be listed as a CSfC TI. If the criteria are not met, the CSfC PMO will notify the company of the unmet criteria and invite them to apply again in the future when the criteria can be satisfied.

8 FREQUENTLY ASKED QUESTIONS

For more information regarding non-technical and technical frequently asked questions please refer to CSfC homepage here:

https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/faq/

9 CONTACT INFORMATION

For all stakeholders who may have questions in regard to the CSfC process, please email the CSfC PMO at csfc@nsa.gov.

For questions related to Common Criteria Testing and NIAP Inquiries, please visit:

- https://www.niap-ccevs.org/Contact_Us/WebForm.cfm