Commercial Solutions for Classified Handbook

Version 3.0

Last updated November 2017

Table of Contents

Last updated November 2017

1. Introduction

What is Commercial Solutions for Classified (CSfC)?

The National Security Agency (NSA) Commercial Solutions for Classified (CSfC) Program has been established to enable 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, governments, 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 now published on the CSfC website at: https://www.nsa.gov/resources/everyone/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 IA 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 CSfC solution integrators, enabling NSA, 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 CSfC TIs can be located under the TI list on the CSfC Webpage here: https://www.nsa.gov/resources/everyone/csfc/trusted-integrator-list.shtml

Commercial Component Developer

Commercial component developers (i.e., vendors) who wish to have their products listed as eligible CSfC components must build their products in accordance with the applicable U.S. Government/collaborative PPs and submit the product for evaluation using the Common Criteria

Process. The CSfC components list can be viewed at: https://www.nsa.gov/resources/everyone/csfc/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. CPs can be customized to the client's needs in order to help them achieve their mission objectives. These provide designs that allow the client to independently implement secure solutions using approved layered Commercial Off-the-Shelf (COTS) products. CPs are vendor-agnostic and provide high-level security and configuration guidance for the client and/or TIs.

CPs are updated biannually or as warranted. Current CPs are listed on the CSfC webpage at: 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.

This CP describes a general MA solution that 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.

The 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. The MA 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.

- MA CP can be viewed at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/mobile-access-cp-next-version.pdf

- MA Compliance Checklist can be viewed at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/compliance-checklist-mobile-access.pdf

- MA Solution Registration Form can be downloaded at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/registration-form-mobile-access.pdf

4.2 Campus Wireless Local Area Networks CP

This CP enables the client to meet the demand for commercial EUDs (e.g., tablets, smartphones, and laptop computers) to access secure enterprise services over a campus wireless network. Commercial National Security Algorithm (CNSA) Suite use layers of COTS products to protect classified data. The Campus WLAN CP enables the client to implement layered encryption between a secure network and EUD.

The purpose of this CP is to provide a reference architecture and corresponding configuration information that allows the client to select COTS products from the CSfC Components List. COTS will be used for the client's Campus WLAN solution which will properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit.

- Campus WLAN CP can be viewed at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/campus-wlan-cp.pdf

- Campus WLAN Compliance Checklist can be viewed at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/compliance-checklist-wlan.pdf

- Campus WLAN Solution Registration Form can be downloaded at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/registration-form-wlan.pdf

4.3 Multi-Site Connectivity CP (MSC)

This 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 at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/msc-cp.pdf

- The MSC Compliance Checklist can be viewed at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/compliance-checklist-msc.pdf

- The MSC Solution Registration Form can be downloaded at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/registration-form-msc.pdf

4.4 Data at Rest Solution CP

The CSfC Data-at-Rest (DAR) CP meets the demand for DAR solutions using the CNSA suite. These algorithms are used to protect classified data using layers of COTS products. The DAR CP enables the client to implement two independent layers of encryption for the purpose of providing protection for stored information while the EUD is powered off or in an unauthenticated state.

The purpose of the DAR CP is to provide high-level reference designs and corresponding configuration requirements that allow the client to select COTS products from the CSfC components list for their DAR solution. The next step is to properly configure those products to achieve a level of assurance sufficient for protecting classified data while at rest.

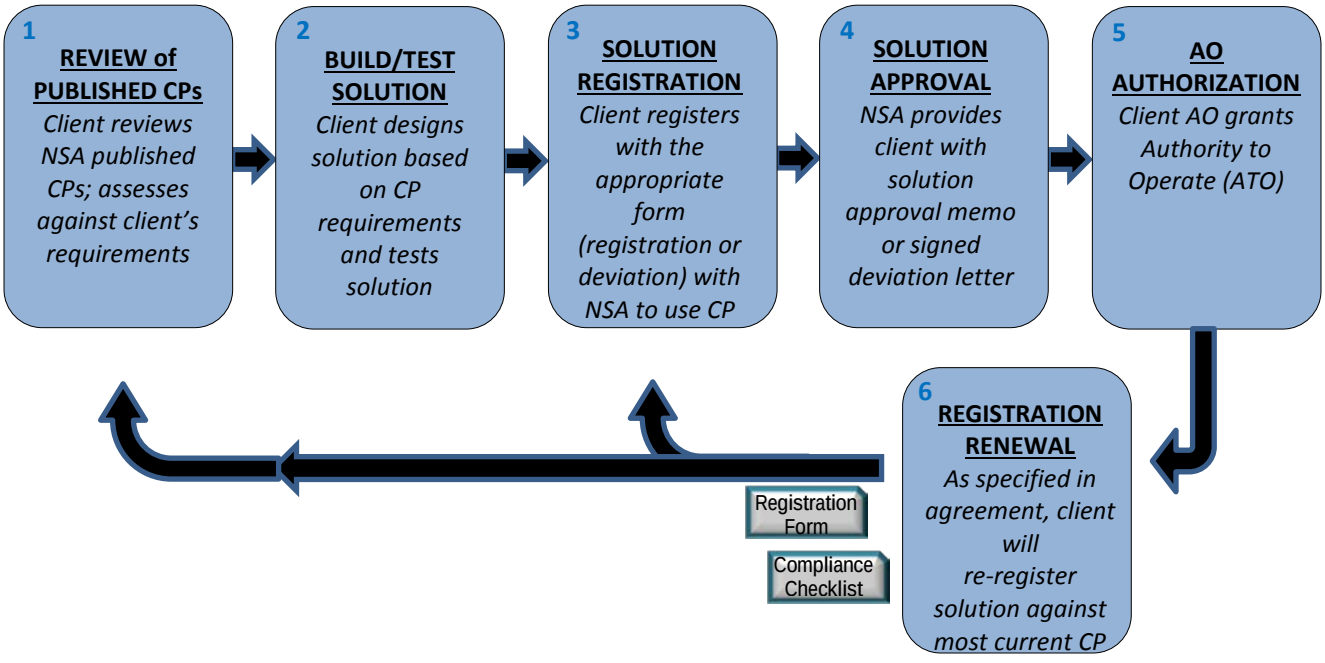
- DAR CP can be viewed at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/dar-cp.pdf

- DAR Compliance Checklist can be viewed at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/compliance-checklist-dar.pdf

- DAR Solution Registration Form can be downloaded at: https://www.nsa.gov/resources/everyone/csfc/assets/files/solution-registration/registration-form-dar.pdf

5. CSfC Solution Registration 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.



5.1 Review of Published CPs

The Client is strongly encouraged to email csfc_register@nsa.gov early on to advise NSA that you plan to register a solution for approval before finalizing your design.

NSA has developed CPs for our client with ready access to the information needed to satisfy their operational requirements, and publishes them on the unclassified NSA website . The client will check the CSfC CPs on the site to see if there is an existing CP that meets the client's needs.

For information or assistance in determining whether an approved CP satisfies their requirements, client (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 at: 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/csfc or JWICS: https://www.iad.nsa.ic.gov/iaservices/csfc accounts. 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/Test Solution

Although not mandatory, CSfC strongly encourages working with a TI while designing, building, and testing a CSfC-compliant solution based upon one or more of the published CPs. Users of the CP are responsible for obtaining, under their organization's established accreditation and approval processes, certification and accreditation of the client implementation of this CP. For the latest CPs please visit: https://www.nsa.gov/resources/everyone/csfc/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 clients 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. Client, commercial component developers, and TIs can download the specific registration form at: https://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml.

5.4/5.5 Solution Approval/AO Authorization

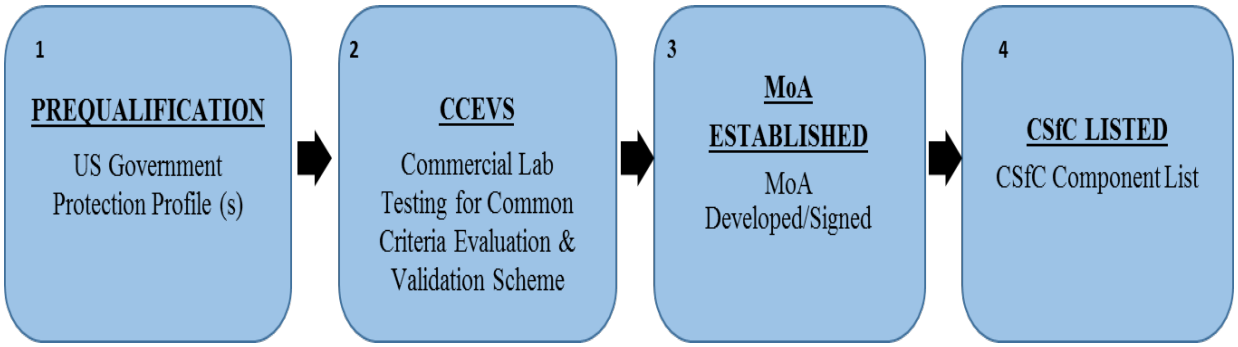
The AO/DAA will confirm after client testing that the checklist is accurate and will then sign the CSfC registration form. The AO/DAA submits the signed form, compliance checklist, deviation form (if applicable), and network diagrams to NSA. Upon verifying compliance, NSA will provide a letter acknowledging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

6.0 The Registration Renewal Process

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

6. Commercial Component Developer Engagement

Commercial Component Developers who wish to have their products eligible as CSfC components of a composed, layered IA solution must build their products in accordance with the applicable U.S. Government approved PP(s) and submit their product using the Common Criteria Process. The process is show in the diagram below:



1. Prequalification

Commercial Component Developers who wish to have their products eligible to become CSfC components of a composed, layered IA 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.

2. Common Criteria Evaluation and Validation Scheme (CCEVS)

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

3. MoA Established

Interested commercial component developers must complete and submit a CSfC questionnaire for each product. Please submit completed questionnaires to csfc_components@nsa.gov. The CSfC PMO will notify the company and initiate the MoA. The MoA agreement 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 at: https://www.nsa.gov/resources/everyone/csfc/assets/files/questionnaire.pdf

4. CSfC Listed

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

7. Trusted Integrator 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/everyone/csfc/assets/files/criteria-for-integrators.pdf. Once completed, the TI should email the completed form to CSfC_integrators@nsa.gov. Applications will be reviewed for completeness. If the criteria are met, the CSfC PMO will schedule a meeting with the company 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 at: https://www.nsa.gov/resources/everyone/csfc/

Back to Table of Contents

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. Below is a list of contacts for your convenience:

Industry Inquiries:

- Email: bao@nsa.gov
- Phone: 410-854-6091

U.S. Government/IC client Inquiries:

- Phone: 410-854-4790

DoD/U.S. Government client Inquiries:

- Phone: 410-854-4200

CSfC PMO General Inquiries:

- Email: csfc@nsa.gov

NIAP Inquiries:

- Email: csfc@nsa.gov
- Phone: 410-854-4458

Back to Table of Contents