INFORMATION
ASSURANCE
CAPABILITIES

Commercial Solutions for Classified

harnessing the power of commercial industry

Last Updated: September 2018

Frequently Asked Questions (FAQs)

INDEX

General FAQs

1. ***What is CSfC?***
   Commercial Solutions for Classified (CSfC) is the NSA's commercial strategy for leveraging industry innovation to deliver Information Assurance (IA) solutions efficiently and securely. The program is founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications. NSA/CSS policy mandates CSfC as the first option to be considered to satisfy an IA requirement.

2. ***Who oversees/manages CSfC?***
   The National Security Agency (NSA) oversees/manages the Commercial Solutions for Classified (CSfC) program.

3. ***Where can additional information be found for CSfC?***
   Additional information about the CSfC program can be found online at:

Unclass:	https://www.nsa.gov/resources/everyone/csfc/
SIRPNet:	https://www.iad.nsa.smil.mil/iaservices/csfc
JWICS:	https://www.iad.nsa.ic.gov/iaservices/csfc

4. ***Who are the typical CSfC clients?***
   Typical CSfC clients are National Security Systems (NSS) stakeholders, to include the Department of Defense (DoD), the Intelligence Community (IC), Military Services, and other Federal Agencies. These clients utilize commercial solutions based on CSfC Capability Packages (CPs) to quickly implement Information Assurance (IA) solutions to satisfy their mission objectives.

5. ***Is there Committee on National Security Systems (CNSS) Policy on CSfC?***
   Yes. CNSS Policy 7, dated 9 December 2015, applies to all USG Departments/Agencies (D/As) that use, or plan to use, implement, or test CSfC solutions to protect NSS. It provides a minimum set of security measures required and directs D/As on how to safeguard NSS, and the information contained therein.

   Additionally, CNSS Policy 11, dated 10 June 2013, establishes the preferential use of layered COTS product solutions to protect information on NSS and establishes processes and procedures for the evaluation and acquisition of COTS and GOTS IA or IA-enabled IT products to be used on US NSS.

6. ***Why does NSA have a commercial IA strategy?***
   US Government customers increasingly require immediate use of the market's most modern commercial hardware and software technologies within National Security Systems in order to achieve mission objectives. Consequently, NSA is developing new ways to leverage emerging technologies to deliver more timely Information Assurance solutions for rapidly evolving customer requirements.

7. ***Why would a client want to use CSfC?***

The Commercial Solutions for Classified (CSfC) Program harnesses the power of commercial industry, providing a secure alternative for government-off-the-shelf IA solutions. It has transformed the delivery of IA solutions to Combatant Commands, Military Services, and Agencies by enabling NSS customers to securely communicate using an increasingly diverse set of commercial products. Customers can efficiently meet their needs for protecting classified information due to NSA investment in the research and application of commercial technologies. Benefits include:

- *End-to-End Solutions* – Provides NSA designed and approved solutions, leveraging a cadre of vetted, trusted system integrators
- *Flexibility and Transparency* – Leverages NIAP-validated components, satisfying US and Collaborative Protection Profile requirements, validated against international Common Criteria
- *Cost Effectiveness and Efficiency* – Allows clients to keep pace with technological progress and employs the latest capabilities in their systems and networks, while reducing the time it takes to build, evaluate, and deploy IA solutions by utilizing mature technologies already available to the commercial sector. Potential cost savings may be realized through marketplace competition and rapidly deployable, scalable commercial products
- *Standards based* – Solutions leverage open, non-proprietary interoperability and security standards
- *Monitoring and Response* – Provides situational awareness about components use and location, as well as documented incident handling procedures
- *Technical Expertise* – Driven by NSA's world-class team of system engineers, threat analysts, and cyber experts

8. ***What is the client's role in CSfC? What responsibilities will the client have in stating their requirements and managing their security solutions?***

CSfC allows clients to use COTS products and to tailor their CSfC solution to meet their specific performance and environmental needs, resulting in an optimal IA solution for the client. To support this effort, NSA has developed, approved and published Capability Packages (CPs). For information or assistance in determining whether an approved CP meets their needs, clients may engage NSA through their designated NSA client advocates and the NSA Client Contact Center.

Clients must register all CSfC solutions operating on NSS or protecting NSS information, to include submitting the appropriate compliance checklist, registration form and network diagrams. Although not mandatory, CSfC strongly encourages working with a Trusted Integrator while designing building and testing a CSfC-compliant solution based upon one or more of the published CPs. Clients are responsible for obtaining, under their organization's established accreditation and approval processes, certification and accreditation of the client implementation of a CP. A client is strongly encouraged to email the CSfC registrar early in the process to advise NSA that you plan to register a solution for approval before finalizing your design.

9. ***Who can approve the mechanisms that are in place to safeguard National Security Systems (NSS) data?***
All CSfC solutions operating on National Security Systems (NSS) or protecting NSS information need to be registered with NSA and several approvals are necessary to implement a CSfC registered solution. Component requirements are validated at the NIAP system level, design requirements are approved by the National Manager, and connection approval is provided by the local Authorizing Official. Approvals require several steps and are further detailed at:
https://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml

10. ***How often is the CSfC website updated?***
CSfC maintains a web presence on multiple security domains and they are updated frequently to reflect changes and enhancement to the Capability Packages, Components List, and Trusted Integrator List. At a minimum, the CPs available on the websites are reviewed/updated biannually.

11. ***Can commercial industry participate to help develop requirements for commercial components?***
Yes. NSA encourages technical innovation, and works with technical communities from across industry, government, and academia to develop product-level requirements called USG Protection Profiles (PPs). Additionally, commercial industry can participate by taking part in Technical Communities (TCs) that help with the development of PPs. More information on NIAP TCs can be viewed at:
https://www.niap-ccevs.org/NIAP_Evolution/tech_communities.cfm

12. ***Does CSfC specify any physical security requirements?***
Yes. Required physical security requirements are specified in the corresponding CSfC CP or documented in the relevant Protection Profile (PP). These requirements may include, but are not limited to, anti-tamper, tempest, authentication, and display the far-end identity.

13. ***What assurance features are incorporated into the CSfC solution designs?***
Multiple levels of assurance are incorporated into every CSfC solution, at the design phase and continuing through the solution lifecycle with periodic assessments. Assurance features are customized with individual implementations, however, typically included are:

- Product diversity using layered solutions for commercial components
- Component selection from the approved CSfC Components List, ensuring components have satisfied specific requirements to include successful evaluation by a Common Criteria Testing Lab and compliance with the applicable public standards and protocols as specified in the PPs and CSfC CPs
- Risk models and risk assessments for CSfC prototypes and CPs
- Analysis of standards, protocols, and algorithms used in a particular solution or prototype
- Vulnerability analysis of appropriate products and solutions, as well as follow-on National Manager Risk Notifications and mitigation guidance, if needed
- Established security incident response process
- Security testing of CPs that will provide sufficient guidance for accreditors to make informed decisions as well as an independent senior review of CPs to provide high-level security and configuration guidance

14. ***Can a CSfC solution be used on coalition networks?***
CSfC is an appropriate solution for networks where foreign nationals are involved and in which the client may be utilizing CCI devices for protection of information in transit to foreign nationals.

15. ***Does CSfC support Mobile Device Management?***
    Yes. Mobile Device Management (MDM) is a critical aspect for implementing a secure architecture. The list of approved MDM Components can be viewed at:
    https://www.nsa.gov/resources/everyone/csfc/components-list/#mdm

16. ***Can a CSfC solution be deployed to replace a Protected Distribution System (PDS)?***
    There is a strong business case for deploying a CSfC solution as a replacement for a PDS. Protected Distribution Systems with COMSEC Controlled Cryptographic Items may be costlier and more logistically intensive as compared to modern technologies and architectures. However, as individual requirements and solutions may vary, local policy justification and cost analysis would need to be conducted.

17. ***Does CSfC replace NSA's Government-of-the-Shelf (GOTS) IA strategy?***
    No, CSfC is a secure alternative to GOTS. NSA will examine the client's needs to ensure the right tool is used at the right place and in the right environment.

18. ***Does CSfC still support GOTS, and is it as secure as COTS information assurance solutions?***
    NSA's strategy for protecting classified information continues to employ both commercially-based and traditional Government off the shelf (GOTS) solutions, however, NSA will look first to commercial technology and commercial solutions in helping clients meet their needs for protecting classified information.

    While the greater NSA continues to support clients with existing GOTS solutions or with needs that can only be met via GOTS, CSfC is focused on commercial off the shelf (COTS) IA solutions, leveraging commercial products in properly configured, layered solutions to provide adequate protection of classified data.

Back to Index

Capability Package FAQs:

19. ***What is a CP and what approved CPs are listed on the CSfC website?***

    Capability Packages (CPs) are NSA-developed, approved and published solution-level specifications and are the foundation of the Commercial Solutions for Classified Program. They are vendor-agnostic and provide high-level security and configuration guidance.

    NSA uses a defense-in-depth approach using properly configured, layered solutions to provide adequate protection of classified data for a variety of different capabilities. CPs support this by providing high-level reference designs and corresponding configuration information that allows the client to select Commercial off-the-shelf (COTS) products from the CSfC components list for its solution and properly configure those products resulting in a level of assurance sufficient for protecting classified National Security Systems (NSS) data.

    The current National Manager approved capabilities are:

    - Mobile Access
    - Campus WLAN
    - Multi-Site Connectivity (replaced Virtual Private Network)
    - Data at Rest (replaced Virtual Private Network)

20. ***How often will Capabilities Packages be changed and how are the changes managed?***

    Capability Packages (CPs) are reviewed by NSA semi-annually and revised as appropriate. CPs are living documents and are updated to keep pace with changing technology and policies, as additional security products and services are developed, and to incorporate the lessons learned from early adopters as they apply this architecture. Updates will often be driven by changes in client needs, technology advances, policies, and problems encountered with the use of existing documents.

    NSA retains responsibility for reviewing requests for changes to CSfC-related documents, identifying the need for the changes, and determining which changes will be implemented.

21. ***Who designs and approves the solution-level specifications for Capability Packages (CPs)?***

    NSA designs, develops, approves and publishes solution-level specifications as Capability Packages. These CPs provide the client with ready-access to the information needed to satisfy operational requirements.

    In accordance with the Committee on National Security Systems (CNSS) Policy 7, "*Use of Commercial Solutions to Protect National Security Systems,*" the Deputy National Manager (DNM) must approve CSfC capability packages developed under the CSfC process and all CSfC solutions operating on, or protecting, NSS information must be registered with NSA.

    Additionally, Trusted Integrators (TIs) specialize in architecting together CSfC components in accordance with the CPs to ensure secure and proper solution functionality. They support NSS clients with the implementation of solution-level specifications outlined in the CPs, but do not approve them.

22. ***Who are the POCs for the published CPs?***

    Capability questions can be emailed to the specific Capability Maintenance Teams at the following:

    - Mobile Access Capability Team: mobile_access@nsa.gov
    - Campus WLAN Capability Maintenance Team: wi-fi@nsa.gov
    - Multi-Site Capability Maintenance Team: msc_cp@nsa.gov
    - Data at Rest Capability Team: CSFC_DAR_Team@nsa.gov
    -

23. ***Where are the Deputy National Manager approved CPs located?***
Current approved CPs are listed on the CSfC webpage at:
https://www.nsa.gov/resources/everyone/csfc/capability-packages

Additional information about CPs and CSfC can be found online at:

Unclass:	https://www.nsa.gov/resources/everyone/csfc/
SIPRNet:	https://www.iad.nsa.smil.mil/iaservices/csfc
JWICS:	https://www.iad.nsa.ic.gov/iaservices/csfc

24. ***What is the difference between a ".8" and an "approved" version of a Capability Package? Can a client register a solution against .8 versions of CPs?***
All solutions must be registered based upon the Deputy National Manager approved versions, which are clearly identified on the websites. Clients cannot register solutions based on .8 versions.

The .8 versions of the CPs are provided to initiate discussions and solicit feedback regarding possible additions to approved versions of the CP. NSA welcomes input and feedback. To contribute to a CP version in development, please contact the CSfC PMO at csfc@nsa.gov.

25. ***What are the current approved CPs and how do they work?***
A brief description of each of the current Capability Packages (CPs) follows:

- **Mobile Access (MA CP)**

  The MA CP describes a general mobile access solution that protects classified information as it travels across either an untrusted network or a network consisting of multiple classification levels. This includes protecting classified data transiting wired networks, domestic cellular networks, and trusted wireless networks to include government private cellular networks and government private Wi-Fi networks.

  This solution supports connecting End User Devices (EUDs) to a classified network via two layers of encryption terminated on the EUD, if 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 IPsec as the outer tunnel and, depending on the solution design, IPsec or Transport Layer Security (TLS) as the inner layer of protection.

- **Campus WLAN (WLAN CP)**

  The WLAN CP enables the client to meet the demand for commercial End User Devices (EUDs) -- such as tablets, smartphones, and laptop computers -- to access secure enterprise services over a campus wireless network. The Campus WLAN CP enables the client to implement layered encryption between a secure network and an EUD.

  The WLAN CP provides a reference architecture and corresponding configuration information leveraging the list of COTS products from the CSfC Components List. Approved COTS devices will be used for the client's Campus A wireless local area network (WLAN) solution which, when properly configured, will achieve a level of assurance sufficient for protecting classified data while in transit. Suite B algorithms use layers of COTS products to protect classified data.

- **Multi-Site Connectivity (MSC CP)**

  The MSC CP (sometimes referred to as “VPN 3.2 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 Internet Protocol Security (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.

- **Data at Rest Capability Package (DAR CP)**

  The DAR CP enables customers to implement two independent layers of encryption for providing protection for stored information using NSA approved cryptography while the End User Device (EUD) is powered off or in an unauthenticated state (defined as prior to a user presenting credentials and being validated by both layers of the DAR solution). Specific data to be protected must be determined by the data owner.

  Although the DAR solution designs can protect the confidentiality of data and render the EUD unclassified, it does not protect the integrity of an EUD outside of the control of an approved user. Therefore, implementing organizations, as part of their solution, must define the circumstances in which an EUD is to be considered outside of the Positive Control of authorized users (i.e., "lost"). Authorizing Officials (AOs) will define the circumstances for considering a device outside of the Positive Control of an authorized user that aligns with the intended mission and threat environment for which the solution will be deployed.

26. ***Where can information about future direction and requirements for new/revised CPs be located?***
    Updates will be posted to the CSfC website as new information becomes available. Also, any client wishing to receive email notifications about updates to this website may email the CSfC PMO at csfc@nsa.gov with any questions. CSfC information is available at:

    Unclass: https://www.nsa.gov/resources/everyone/csfc/
    SIPRNet: https://www.iad.nsa.smil.mil/iaservices/csfc
    JWICS: https://www.iad.nsa.ic.gov/iaservices/csfc

27. ***How can clients be more successful implementing solutions in compliance with CP requirements?***
    Clients can improve the likelihood of successful implementations by utilizing the services of an experienced solution integrator. A list of approved Trusted Integrators is available at: https://www.nsa.gov/resources/everyone/csfc/trusted-integrator-list.shtml

28. ***Does the client need to notify NSA if any changes are made to the solution implementation of the Capability Package?***
    Yes. If a Trusted Integrator or the client decide to make changes to a solution implementation that results in the solution no longer conforming to a current CP, the client must notify NSA.

29. ***What are Retransmission Devices (RDs)?***

A government-owned Retransmission Device (RD) is a category which includes WI-FI Hotspots and Mobile Routers. RDs provide a connection to the Mobile Access (MA) solution infrastructure via any Black network and interfaces to the End User Device (EUD) using WI-FI or an Ethernet Cable.

On the external side, the RD can be connected to any type of medium (e.g. cellular, Wi-Fi, SATCOM, Ethernet) to gain access to a Wide Area Network. On the internal side, the RD is connected to End User Devices (EUDs) either through an Ethernet cable or Wi-Fi. More information on RD specifications and requirements can be found by accessing the Mobile Access Capability Package (MA CP), located at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/mobile-access-cp.pdf

30. ***Since biometrics are optional, are there any plans for specific supplemental CSfC selections in this area?***

While there are biometric details written into NIAP's MDF PP, there are currently no biometric selections for CSfC.

31. ***Will biometrics, if allowed, be limited to only the fingerprint template?***

As specified in the Mobile Access Capability Package (MA CP 2.0, Section 4.4, Authentication): "The second factor will be a "something-you-have" factor manifesting as a physically separate token from the VPN EUD supplying a one-time password for the user to enter. For future versions of the MA CP, transferring this one-time password via a short-range RF communication will be explored. Allowing "something-you-are" (e.g. biometric) as a second factor is also being explored for future versions."

32. ***Why is CSfC requiring virtual machines within a tablet/laptop solution, but not in a Smartphone Secure VoIP solution?***

There is currently a Tablet/Laptop (Mobility Wi-Fi) pilot solution, providing wireless data capabilities to a TS//SCI enterprise. This pilot activity is providing a test foundation to develop the Wi-Fi Capability Package, but the final requirements may be very different than the test deployment.

If virtualization technology was commonly available in smartphones, it could be leveraged for some solutions, however, to-date the devices that have been under CSfC consideration for addition to the Components List have not employed that technology. The Secure VoIP solution currently available provides VoIP services to a constrained classified collateral environment, not to a TS//SCI environment.

Each CSfC solution requires a separate risk decision to be made, depending on the client’s mission. The intent is always to deploy the best security solutions that are currently available while documenting the design risk accepted by the National Manager. Solutions that do not offer virtualization are not prohibited, but they may be more restricted or present a higher risk than solutions with virtualization.

33. ***Who assumes responsibility for the inherent risk in Capability Package designs?***

The Deputy National Manager (DNM) for National Security Systems (NSS) assumes the inherent risk in the solution designs as specified in the published CPs. However, the overall risk of the solution is shared, as the Client's Authorizing Official (AO) is responsible for ensuring the fielded solution complies with the CP specifications and remains in compliance.

34. ***How does the alternative authentication mechanism apply with the DAR Solution? Is a primary authentication mechanism still needed?***

Many products offer alternative authentication mechanisms. When implementing the DAR solution, these alternate mechanisms may be used only as a secondary authentication factor and must be paired with a primary authentication factor. Secondary authentication factors may act as an additional access control or may contribute to the product's key chain. The product's PP evaluation guarantees no loss in strength when combining keys with potentially weaker sources.

35. ***What does Data at Rest have to do with Diversity and Supply Chain?***

Supply Chain and Diversity co-exist with DAR. Supply chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Diversity is applied by using multiple layers, implemented with components that meet the CSfC vendor diversity requirements, which then reduce the likelihood that a single vulnerability can be exploited to reveal protected information. Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process.

36. **How long does a client (Government Agency) have to comply with a newly released Capability Package?**

Once a new version of a CP is published, the client may continue to operate, however, in accordance with CSfC registration policies, the client must comply with the new version upon re-registration. CSfC PMO will send out 120-day, 60-day and 30-day notifications of registration expirations to the client via email.

37. ***How can the Campus WLAN CP Version 2.0 be applied?***

The Campus WLAN CP enables the client to meet 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.

38. ***How can the Mobile Access CP Version 1.1 be applied?***

The MA CP Version 1.1 provides the client with requirements for domestic and international voice, video, and data capabilities from a mobile End User Device. VPN Remote and Local EUD Designs which complied with previous versions of the VPN CP are expected to need only minor changes to comply with the VPN EUD Design of this CP.

39. ***Who dictates the installation of patches for solution components for Capability Packages (CPs)?***

Local policy dictates how the Security Administrator installs patches to Solution Components. Ensuring that the latest patches and updates are applied to each product in a timely fashion. Critical patches shall be tested and subsequently applied to all components in the solution in accordance with local policy and the CP.

Back to Index

Component List FAQs:

40. ***What is the CSfC Component List?***

    The CSfC Components List is a list of commercial product selections that can be used to create an architecture configured in a particular manner. These products are NSA approved and can be used in National Manager approved commercial IA solutions. The client can select products from the Components List which satisfies the reference architectures and configuration information contained in published Capability Packages (CPs). The client must ensure that the components selected will permit the necessary functionality for the selected architecture.

41. ***Who maintains the Commercial Solutions for the Classified (CSfC) Component List?***

    The CSfC PMO maintains the Components List. Additional information, to include the list of components, can be found online at:

Unclass:	https://www.nsa.gov/resources/everyone/csfc/
SIPRNet:	https://www.iad.nsa.smil.mil/iaservices/csfc
JWICS:	https://www.iad.nsa.ic.gov/iaservices/csfc

42. ***What is the process for commercial component developers to have their products become eligible as CSfC components?***

    Commercial component developers who wish to have their products declared eligible as CSfC components must build their products in accordance with the current applicable US Government approved or collaborative Protection Profiles and submit their product for evaluation in accordance with the established Common Criteria process.

    The commercial component developer will enter into a MOA with NSA. Interested commercial component developers must complete and submit the CSfC Questionnaire for each product. Submit completed Questionnaires to: csfc_components@nsa.gov

43. ***What are the benefits of being included on the CSfC Components List?***

    In accordance with CNSS Policy 7, only approved products on the CSfC Component List can be used in commercial IA Solutions protecting classified NSS data.

44. ***Where can I see the technology categories for the CSfC Component List?***

    The technology categories are listed on the CSfC Component List. Additional information can be found online at:

Unclass:	https://www.nsa.gov/resources/everyone/csfc/
SIPRNet:	https://www.iad.nsa.smil.mil/iaservices/csfc
JWICS:	https://www.iad.nsa.ic.gov/iaservices/csfc

45. ***Where can current listings of the approved Protection Profiles (PPs) be accessed?***

    Currently approved and in-development listings of NIAP approved, US Government PPs are provided online on the NIAP site.

46. ***Why is there an Archived Component List?***

    The Archived Component List outlines products that are no longer approved for use in CSfC solutions. Any client using products from the Archived Components List must transition to currently approved products when renewing a registered solution, when making other changes to the registered solution, or when security risks mandate a change.

47. ***How frequently is the Component List updated?***
The Component List is updated every two to three weeks or when necessitated by a significant change.

48. ***Where can information on CSfC manufacturer diversity requirements be found?***
The CSfC program contains details on how a manufacturer can submit diversity evidence to NSA and what documentation must be provided. This information can be accessed at the CSfC web page at https://www.nsa.gov/ia/programs/

49. ***Can open-source components be used in CSfC?***
An open-source component may be used, provided it has a responsible sponsor and an NSA-approved plan for taking the component through the Common Criteria Evaluation as well as a plan for the sustainment of the component that includes version updates and software patch installation, as required. A client who wishes to use open-source components should contact csfc_components@nsa.gov and provide the evaluation, sustainment plan and the responsible parties for each such open-source component.

Back to Index

Key Management-Enterprise Gray FAQs:

50. ***Who issues certificates?***
    Certificates may either be issued by a US PKI Certificate Authority (CA) or include a cross certification between US CAs and foreign partner CAs.

51. ***What is the difference between Enterprise Gray and Global Gray networks?***
    The Enterprise Gray network is a single Authorizing Official (AO) with robust deployments for supporting a National Security System (NSS) enterprise environment. This may include remote management, redundant or distributed infrastructure for higher availability, and overlap of more than one CSfC Capability Package (CP).

    The Global Gray network is primarily envisioned as the sharing of a distributed CSfC ecosystem to support Data-In-Transit for large scale networks (e.g. SIPRNet) with multiple AOs assuming various responsibilities. Conceptually, a primary entity (e.g. DISA) would own/operate and provide access to this gray network as a service. Features may include those already identified for the Enterprise Gray network along with the clear benefit of interagency interoperability.

    Neither the Enterprise Gray network nor the Global network currently exist operationally, only as a proof of concept.

52. ***Will Commercial Solutions for Classified (CSfC) Gray Networks expand in the near future?***
    NSA is focused on expanding the Enterprise Gray network and Global Gray network beyond the concept phase, however, there is not yet a date for its availability.

53. ***Is there any CP that provides support for multi-level classifications?***
    Mobile Access CP version 2.0 is currently near completion and will provide support for multi-level classifications which could include a classified coalition network. More information regarding Mobile Access CP classifications will be available on the website as it becomes available.

54. ***Can CSfC be utilized to protect classified data exchanges with foreign partners when the US owns/operates all components of a solution?***
    Yes. If the US owns/operates all components of a solution, CSfC can be used to protect classified data exchanges involving foreign partners.

55. ***Can CSfC be utilized to protect classified data exchanges with multiple foreign partners connected to a bilateral network when the US owns/operates one side and foreign partner owns/operates the distant side?***
    Yes. CSfC can be used to protect classified data exchanges involving multiple foreign partners where the US owns/operates one side and the foreign partner owns/operates the distant side.

56. ***How does CSfC mitigate supply chain concerns?***
    Each CSfC CP addresses the supply chain with the CP requirements to ensure a device has been validated to function as required. Diversity is applied by having two layers of Suite CSNA encryption. Even after selecting components from the CSfC components list and utilizing a rigorous acquisition process, each component shall then undergo a product supply chain threat assessment to determine the appropriate mitigations for the intended application of the component per the organization’s AO-approved product supply chain threat assessment process. An AO must perform due diligence when integrating commercial components for mission operations.

57. ***What are the approved security "layers" (protocols and or clarification to Commercial Off-the-Shelf (COTS) protocol options?***

The foundation of Cryptographic Interoperability Strategy is CNSA cryptography. CNSA algorithms are approved by the NIST. The CNSA suite includes cryptographic algorithms for confidentiality, key exchange, digital signature, and hashing. Specific protocols are in the Capability Packages (CPs).

58. ***What is CNSA?***

CNSA is a set of commercial algorithms capable of protecting data through the Top-Secret level (previously known as Suite B).

59. ***What happened to Suite B? Why is it being replaced with the CNSA suite?***

NSA issued a CNSS Advisory Memorandum 02-15 listing cryptographic algorithms that can be used in NSS. More information concerning this memorandum can be viewed at:

https://www.cnss.gov/CNSS/issuances/Memoranda.cfm

The Commercial National Security Algorithm Suite (CNSA Suite) replaces the current Suite B Algorithms and provides new algorithms for the client who is looking for mitigations to perform. The transition from Suite B to CNSA is a result of NSS using more complex approved cryptographic algorithms. This list/changes can be viewed at:

https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

For questions about Suite B and Cryptography, contact the National Cryptographic Solutions Management Office (NCSMO) at (410) 854-8577.

60. ***What algorithms are used in CSfC solutions?***

The algorithms that are used in CSfC solutions are the CNSS Advisory Memorandum (AM) Information Assurance (IA) 02-15. CNSS AM IA 02-15 expands on the guidance contained in CNSS Policy No. 15 and identifies additional public algorithms to protect information within NSS. Specifically, the following algorithms will be required to protect all NSS up to the Top-Secret level: AES 256 (confidentiality) (*Note that AES 256 is an objective requirement for WPA2 Enterprise). Other algorithms include RSA 3072 or ECDSA P-384 (digital signature and authentication), RSA 3072, DH 3072 or ECDH P-384 (key exchange), and SHA-384 (hashing and integrity).

61. ***The CSfC website states that there will be a transition from the CNSA (Commercial National Security Algorithm) suite to quantum resistance algorithms. Will this affect the use of components?***

    It is important to note that vendors may continue to implement Suite B algorithms and the client may continue to use those algorithms. Certainly, where elliptic curve protocols are to be used, the preferred Suite B standards should be used to the fullest extent possible since they have a long history of security evaluation and time-tested implementation that the newer proposals do not yet have.

    However, in order to provide more flexibility to commercial developers and clients, a transition to quantum resistance algorithms is anticipated in order to provide a quantum safe future. Additional information and guidance in transitioning to quantum resistant algorithms, can be found at: https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

62. ***Are the CSfC Capability Packages an alternative to Type 1 attended or unattended solutions?***

    CSFC CPs describe solutions that empower the client to implement secure solutions using independent, layered Commercial Off-the-Shelf products from the CSfC Components List. Depending on the client's needs, CSfC solutions can be used to protect classified data in a variety of applications. NSA CSfC has not replaced Type 1 solutions. Based on the client's needs, NSA will use the correct tool for the right job.

    Sometimes the right tool can include the layered use of the commercial products in accordance with CSfC requirements. U.S. national (CNSSP-15) policy provides the protection of NSS (National Security Systems), and shall utilize CNSA (Commercial National Security Algorithm) suite solutions for protection of information systems.

63. ***Can the CSfC solution be used to remove Taclanes from local buildings on the client's site?***

    Yes, it may be possible to replace Taclanes with a CSfC solution but it would depend on several factors (requirements, AO, etc.). In general, the MSC CP is adaptable to support capabilities for multiple sites and/or multiple security levels, depending on the needs of the client implementing the solution. For more information on the MSC CP, please go to the CSfC website at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/msc-cp.pdf

Back to Index

National Information Assurance Partnership (NIAP) FAQs:

64. ***Where can additional information about the NIAP Evaluation and Validation Process be found?***
The NIAP Evaluation and Validation Process is explained in detail at:
https://www.niap-ccevs.org/Ref/Evals.cfm.

65. ***What is the approximate length of time of a NIAP evaluation?***
An evaluation in NIAP can be completed in less than 90 days, but must not exceed 180 days (6 months). The time it takes to evaluate/validate a product depends on many factors, including; size and complexity of the product, the amount of evidence available vs. the amount that needs to be generated, and the availability of lab resources to do the evaluation. Common Criteria evaluations conducted outside of NIAP (in other CCRA nations) may take longer. Additional information can be found on the NIAP webpage at: https://www.niap-ccevs.org/Ref/FAQ.cfm.

66. ***Is it possible for an IT product to be evaluated in non-US labs and still be used in the Commercial Solutions for Classified (CSfC) program?***
Yes. NIAP can recognize evaluations handled against NIAP-approved Protection Profiles in other schemes per the Common Criteria recognition arrangement. Further information may be found at: https://www.niap-ccevs.org/Ref/CCRA.Partners.cfm.

67. ***Is it necessary to engage the National Information Assurance Partnership (NIAP) when modifying a component?***
Guidelines concerning modifications to NIAP approved components can be found on NIAPs assured continuity website, located at:
https://www.niap-ccevs.org/Ref/FAQ.cfm.

68. ***Are GOTS products evaluated by NIAP?***
No. NIAP does not evaluate Government Off the Shelf (GOTS) products.

69. ***Is Common Criteria mandatory for CSf*C?**
Yes. Common Criteria is mandatory for CSfC. Additionally, per CNSS Policy 7, all CSfC solutions operating on or protecting NSS information must be registered with NSA.

70. ***Why do some technology areas on the CSfC Components List have selectable requirements?***
For some technologies, the CSfC program requires specific, selectable requirements to be included in the Common Criteria Evaluation, validating that the product complies with the applicable NIAP-approved Protection Profiles (PPs). It is possible that some selectable requirements, which are not mandatory for the NIAP Product Compliant List, may still be mandatory for the product to be listed on the CSfC Components List.

Back to Index

Policy FAQs:

71. ***Who can approve the certificate requests for Capability Packages (CPs)*?**
Certificate requests are approved by an authorized registration authority and submitted to the Certificate Authority in accordance with the corresponding CP.

72. ***What is Committee on National Security Systems Policy (CNSSP) No. 7?***
CNSS Policy 7 provides a minimum set of security measures required for US Government Departments and Agencies use of CSfC solutions. The heads of D/As are ultimately responsible for protecting NSS (both classified and unclassified) that transmit, receive, process, or store information using CSfC solutions.

    Department/Agencies will ensure all CSfC solutions comply with NSA requirements, as delineated in this policy. Implementation of CSfC solutions does not preclude the application of additional requirements associated with the security of NSS (e.g., physical security, TEMPEST, Operations Security).

73. ***What is Committee on National Security Systems Policy (CNSSP) No. 11?***
CNSS Policy 11 is a key component of the US Government's overall Cyber Security strategy. This mandatory national policy clarifies the required evaluation processes applicable to Commercial off-the-Shelf (COTS) and Government off-the-shelf (GOTS) IA and IA-enabled IT products that are used on US National Security Systems to protect information. All users and commercial component developers of IA and IA-enabled IT products should be familiar with the policy and its associated processes to ensure full compliance with its documented requirements. Products must be on National Information Assurance Partnership (NIAP) product Compliant List for departments/agencies to purchase them for CSfC applications.

74. ***What is Committee on National Security Systems Policy (CNSSP) No. 15?***
CNSS Policy 15 describes the requirements, roles, and responsibilities associated with the use of public cryptologic protocols and algorithms to protect NSS and the information residing therein, or transmitted between NSS.

Back to Index

Protection Profiles FAQs:

75. ***Why are Protection Profiles (PPs) important?***

Protection Profiles are an implementation-independent set of security requirements and test activities for a particular technology that enables achievable, repeatable, and testable evaluations. These PPs define security measures and assurance requirements that clients, Trusted Integrators, and commercial component developers expect components to meet. Commercial component developers can apply these requirements and make judgements about the security attributes of their products.

All products evaluated must demonstrate exact compliance to the applicable technology protection profile. NIAP assesses the results of the security evaluation conducted by an appropriate lab and, if the evaluation is successful, issues a validation certificate and lists the product on the US NIAP Product Compliant List. US Customers, to include Designated Approving Authorities (DAAs), Authorizing Officials (AOs), and integrators, may treat these mutually-recognized evaluation results as complying with CNSS Policy 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*.

CSfC selections define the specific PP requirements that must be included as part of a Common Criteria Evaluation for a product to be eligible for use in a CSfC solution. Testing facilities will evaluate the products to determine if they meet these requirements. PPs are intended to help all stakeholders and end users meet the increasing demand for more security from cyber threats by making it easy for individuals to procure, deploy, and utilize certified, approved products. Commercial component developers who wish to have their products be eligible as CSfC components and approved for use as part of a composed, layered IA solution, must build their products in accordance with the applicable US Government approved PPs.

76. ***If a Protection Profile does not exist for a specific CSfC technology category, what is the next logical step?***

The National Information Assurance Partnership (NIAP) should be contacted directly to discuss a way forward for each specific situation. For more information, please visit the NIAP website at: https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/No PP_Exists.pdf

77. ***Who is responsible for interoperability among systems, and will there be interoperability Protection Profiles (PPs) or Capability Packages (CPs)?***

The client is ultimately responsible for ensuring that the solutions it procures satisfies specific interoperability needs. However, correctly utilizing the Capability Packages, Protection Profiles and leveraging the services of a Trusted Integrator will assist the Client in achieving interoperability goals.

The National Information Assurance Partnership (NIAP) develops Protection Profiles (PPs), evaluation methodologies, and policies to ensure achievable, repeatable, and testable requirements. NIAP evaluates Commercial Off-The-Shelf (COTS) Information Technology (IT) products for conformance to the international Common Criteria. CSfC defines the specific PP requirements that must be included as part of a Common Criteria evaluation in order for a product to be eligible for use in a CSfC solution.

Although the Client is responsible for overall interoperability of a solution, it is the commercial component developer's responsibility to correctly implement the commercial standards that are referenced in the PP to enable interoperability with CNSA suite products from other commercial component developers. Additionally, CSfC Capability Packages provide high-level reference designs and corresponding configuration information which facilitates, but does not guarantee, interoperability among components and systems. Clients and integrators should perform interoperability testing to ensure the components selected for their CSfC solution are interoperable.

78. ***How does a vendor obtain a current Protection Profile?***
Current versions of all PPs are available on the NIAP website at:
http://niap-ccevs.org/Profile/PP.cfm

79. ***How are updates or corrections to a Protection Profile (PP) made?***
PPs are regularly updated to account for new security capabilities, address known vulnerabilities and to align with industry standards and best practices. Approved, developing, and archived PPs, as well as other pertinent information, is located on the NIAP website.

80. ***What assurances are there that a new system/capability will be CSfC compliant?***
Technologies from the CSfC Components List shall be used, in accordance with NSA's published CSfC Capability Packages(CPs), for National Security Systems (NSS) classified data that is being protected at rest or in transit by commercial products. Commercial component developers shall meet CNSS Policy (CNSSP) No. 11 requirements. Technologies shall be procured which have been validated by Common Criteria Testing Labs, in accordance with the National Information Assurance Partnership (NIAP) PPs. CPs and the CSfC Components List can be found by visiting the CSfC Components List page. NIAP-validated products can be found at the NIAP website on the CCEVS Product Compliant List page. For a specific implementation, the developer should submit a registration package describing it for the NSA CSfC PMO to evaluate for compliance.

81. ***Are IASRD requirements used in the creation of Protection Profiles?***
IASRD requirements are not used in the creation of the PPs.

82. ***Which Protection Profiles apply to the CSfC Component List?***
The CSfC Component List Index is available on the CSfC Website. Selecting a specific component from this list will bring up specific components and the Protection Profiles that apply to them. The CSfC Component List Index is located at:

https://www.nsa.gov/resources/everyone/csfc/components-list/#list-index

Please email the CSfC PMO at csfc@nsa.gov for with additional questions.

83. ***Do the optional requirements apply to CSfC?***

In many cases, the Threshold requirement also serves as the Objective requirement (T=O). In some cases, multiple versions of a requirement may exist in a capability package. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement. Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement improves upon the Threshold requirement and may replace the Threshold requirement in future versions of the CP.

Objective requirements without a corresponding Threshold requirement are marked as "Optional", but improve upon the overall security of the solution and should be implemented where feasible.

84. ***In a VPN solution, are all of the layers end–to-end (i.e., red/black/grey gateways, authentication)? For instance, when considering three classified enclaves of computers (A, B and C) where A is connected to B with a Site-to-Site VPN solution (basically, two VPN gateways in series) and B is connected to C with a HAIPE solution, is the data being sent from A to C encrypted end-to-end?***

The data is not necessarily encrypted end-to-end, as not all layers are end-to-end. In the example above, data sent from A to C would not be encrypted end-to-end as there would be a Red gateway at B for traffic between A and C. Each VPN tunnel could authenticate its peer, however, in this example it does not yield true end-to-end authentication.

In the instance described above, the configuration would not be a CSfC solution. Specifically, HAIPE is a GOTS solution, so this example would have a mix of both GOTS and CSfC solutions, which is not a typical, or necessarily recommended, solution.

Back to Index

Solution Registration FAQs:

85. ***What is the process for solution registration and approval and what registration forms/documentation are needed?***

To assist their clients, NSA has developed Capability Packages (CPs) that contain information needed to satisfy operational requirements. They are published on the unclassified NSA website. The first step in any client's solution registration is to review these and determine if there is an existing CP that meets their needs.

For information or assistance in determining whether an approved CP satisfies their requirements, any client (e.g., Department of Defense Components, Intelligence Community Organizations, and Federal Agencies) may engage NSA through their designated NSA client advocate and the NSA client contact center. Information can be viewed at: https://www.nsa.gov/about/contact-us/#subject:iad.

Although not mandatory, CSfC strongly encourages working with a Trusted Integrator 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 CP's implementation.

The Capability Package Solution Registration process is outlined below:

- Involve the CSfC PMO early in the process
  - Customers are strongly encouraged to email csfc_register@nsa.gov to advise NSA of their plan to register a solution, before finalizing the design
  - Obtain a **Solution Registration Identification Number** from the CSfC PMO
  - Coordinate the completed Capability Package (to include the Registration Form, the CP-specific Compliance Checklists, and the network diagrams), with the CSfC PMO prior to submitting the AO-signed versions. This will allow CSfC engineers to review, advise, and assist, making recommendations to smooth the formal registration process.
- Using CSfC guidance, configure and test the system in a controlled manner
- Submit the signed Capability Package to the CSfC PMO, to include:
  - **Completed Registration Form**, *signed* by the client's Authorizing Official
  - **Completed Compliance Checklist** with brief, specific responses explaining how the solution is compliant with the CP
  - **Deviation form**s, if applicable, *signed* by the client Authorizing Official
  - **Network diagrams**
- Upon verifying compliance, NSA will provide a letter acknowledging the registration for a specific time period. Detailed information about each step in the process can be found in Section 5 of the CSfC Handbook at: https://www.nsa.gov/resources/everyone/csfc/assets/files/csfc-customer-handbook.pdf

  Registrations Forms are available at: https://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml

86. ***What does the registration form signify when it has been signed?***

By signing the registration form the Authorizing Official 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.

Registration approval periods for exercises will be on a case-by-case basis. Client notifications will be sent via email to POCs identified on the client's registration forms. If compliance is not maintained, CSfC PMO will notify the client of its need to submit a fully documented CP deviation request via email at csfc_register@nsa.gov. If the deviation request is classified, classified delivery will be sent via email to SIPR at csfc_reg@nsa.mil.mil or NSANet at csfc_pmo@nsa.ic.gov.

87. ***How does a CSfC client renew its solution registration?***

CSfC PMO will send out 120-day, 60-day and 30-day notifications of registration expiration to the client via email to POCs listed on the client's registration forms. The client will submit updated registration/compliance checklist forms to NSA via email at csfc_register@nsa.gov. If completed forms are classified, the client should notify CSfC PMO via csfc_register@nsa.gov for appropriate delivery instructions.

Upon receipt of completed registration/compliance checklist forms, NSA will review the updated forms to ensure continued compliance with the relevant CP. As warranted, NSA may seek clarification directly from the client's POCs contained on its registration forms. If compliance is maintained, CSfC PMO will prepare a solution acknowledgement letter. Registrations will be valid for one year from the date of the acknowledgement letter. Registration approval periods for non-permanent solutions, such as for Military Exercises or Training, will be on a case-by-case basis. Customer notifications will be sent via email to POCs identified on the client's registration form.

88. ***Why do solutions need to be registered?***

Per CNSS Policy 7, CSfC solutions operating on NSS or protecting NSS information need to be registered with NSA. Registration is renewed annually. The process of registering a CSfC solution leveraging a CSfC CP as well as registration forms are located on the CSfC website: https://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml.

89. ***When during the registration process should NSA be notified about registering a solution for approval?***

Any Client is strongly encouraged to email csfc_register@nsa.gov as early as possible in the registration process to discuss their plans and approach, typically **before** procuring equipment or finalizing a design.

90. ***Who will confirm that the compliance checklist is accurate and sign the CSfC registration form****?*

The customer's Authorizing Official (AO) will confirm that the compliance checklist is accurate and will then sign the CSfC registration form. The completed, signed registration form, compliance checklist, and network diagrams are sent to the CSfC PMO. Upon verifying compliance, NSA will provide a solution registration acknowledgement.

91. ***Who is responsible for developing, approving and implementing CSfC solutions?***
NSA is responsible for creating Capability Packages (CPs) that describe CSfC approved designs. The National Information Assurance Partnership (NIAP) is responsible for approving commercial components which meet the requirements of US Government or collaborative Protection Profiles (PPs) and have been verified by NIAP testing. Clients and their AOs are responsible for implementing and approving solutions that comply with Capability Package specifications.

92. ***Who oversees solution registrations?***
The Commercial Solutions for Classified (CSfC) Program Management Office (PMO) manages all solution registrations.

93. ***How long does it take to get registered?***
The registration process varies case by case depending on all required forms being submitted and validated.

94. ***Who assumes the risk for CSfC solutions?***
The Deputy National Manager for National Security Systems (NSS) assumes the inherent risk in the solution designs as specified in the published CPs. The client's AO is responsible for ensuring the fielded solution complies with the CP specifications and remains in compliance.

Back to Index

Trusted Integrator FAQs:

95. ***Who oversees the Trusted Integrator (TI)?***
The CSfC PMO vets any Trusted Integrator prior to including them on the Trusted Integrator List. The list provides a reference that a Client can use when engaging a Trusted Integrator to assist them.

96. ***What is the role and criteria to become a Trusted Integrator for CSfC?***
Trusted Integrators support the client in the implementation of CSfC CPs. Trusted Integrators specialize in bringing together CSfC components in accordance with the CSfC CPs to ensure secure and proper solution functionality.

Trusted Integrators must be prepared to demonstrate, upon request from NSA, 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. In order to become a Trusted Integrator, the sponsoring organization must comply with one or more of the following standards:

- Management and technical requirements of the International Organization for Standardization (ISO)/International Electro Technical Commission (IEC)
- National Voluntary Lab Accreditation Program, as per NIST Handbook 150
- ISO9000, Quality Management Systems
- Capability Model Maturity Integration (CMMI)

NSA will assess, based on Trusted Integrator input, whether organizations meet the criteria for CSfC Trusted Integrators.

97. ***If a company or an integrator believes they have an innovation solution addressing CSfC requirements, what can they do?***
The company should contact the CSfC PMO at: csfc@nsa.gov.

98. ***What costs are involved in becoming a Trusted Integrator?***
There are no direct costs for becoming a Trusted Integrator. NSA, CSfC and NIAP do not charge for any evaluation oversight activities.

99. ***Where can the list of approved CSfC Trusted Integrators be found?***
The list of CSfC approved Trusted Integrators can be found by visiting the CSfC webpage at: https://www.nsa.gov/resources/everyone/csfc/trusted-integrator-list.shtml. Additional information can be found online at:

Unclass:	https://www.nsa.gov/resources/everyone/csfc/
SIPRNet:	https://www.iad.nsa.smil.mil/iaservices/csfc
JWICS:	https://www.iad.nsa.ic.gov/iaservices/csfc

100. ***Why is it important to become a CSfC Trusted Integrator?***
Following criteria and processes that are defined to provide a common baseline for CSfC solution integrators enable NSA and AOs to access the capabilities of solution Trusted Integrators and accept their results.

101. ***Are CSfC customers mandated to work with a Trusted Integrator?***
Although strongly recommended, it is currently not a requirement for customers to use a Trusted Integrator.

102. ***Do Trusted Integrator personnel need to hold some level of clearance to perform their duties?***
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 at least equivalent to the level of data to be processed by the solution.

103. ***Is it necessary that integrators have a secure facility?***
It is not required that an integrator have a secure facility. However, the integrator must have access to a secure facility in which to receive classified risk assessments and to test for classified vulnerabilities, if needed. The facility clearance shall be equivalent to the level of data to be processed by the solution.

104. ***If all criteria are met, how long does the process typically take between Trusted Integrator application submission, the follow-up meeting, and establishment of a Memorandum of Agreement (MOA)?***
The process usually takes approximately one month from receipt of application to signed MOA.

105. ***Is it required that a Trusted Integrator (TI) hold a certification for one of the standards listed in Section 1.1 of the*** *Criteria for CSfC Solution Integrators* ***guidance or can the organization show compliance with one of the standards without having the certification?***
Trusted Integrators are expected to satisfy all identifying criteria. Any questions concerning a specific requirement should be directed to the CSfC PMO at: csfc@nsa.gov.

106. ***Is a Facility Clearance required to be on the Trusted Integrator (TI) list?***
No, a facility clearance is not mandatory, however, a TI must be able to review protected information, such as risk assessments. A facility clearance is usually beneficial in order to be an effective TI, but workarounds are possible. During the registration process, a potential TI should enter into discussions with the CSfC PMO to discuss potential workarounds or other situations that would mitigate the need for a facility clearance.

107. ***Is prior CSfC work experience a requirement to become a Trusted Integrator?***
Prior CSfC work experience is not required, however; any relevant experience/expertise in the requested areas should be noted on the response.

Back to Index

Web Presence FAQs:

108. ***Where can the latest news and updates on CSfC be found?***

The CSfC webpage contains current program information:

Unclass:	https://www.nsa.gov/resources/everyone/csfc/
SIPRNet:	https://www.iad.nsa.smil.mil/iaservices/csfc
JWICS:	https://www.iad.nsa.ic.gov/iaservices/csfc

109. ***Where are the classified CSfC CP risk assessment located?***

Naturally, classified assessments are only available on classified systems, thus only authorized users with the appropriate access will be able to access them. Specifically:

SIPRNet: https://www.iad.nsa.smil/iaservices/csfc
JWICS: https://www.iad.nsa.ic.gov/iaservices/csfc

Back to Index

Points of Contact:

110. ***What is the best way to contact Commercial Solutions for Classified (CSfC) PMO for general inquiries?***
All inquiries and questions can be sent to the CSfC team via an email at: csfc@nsa.gov

111. ***Who is the contact for Commercial Solutions for Classified (CSfC) PMO for DoD or US Government customer inquiries?***
All inquiries and questions can be sent to the Client Contact Center:

Phone: (410)-854-4200
Email: IAD_CCC@nsa.gov

112. ***What is the best way to contact NSA?***
The mailing address for the National Security Agency is:

9800 Savage Rd, Suite 6272, Ft. George G. Meade, MD 20755

However, the best way to contact NSA is:

Phone: (301) 688-6524, or
Email: https://www.nsa.gov/

113. ***Who is the contact for US Government/IC Client Inquiries?***
US Government and/or IC Client inquiries can be directed to:

Phone: (410) 854-4790, or
Email: iad_ccc@nsa.gov

114. ***Who is the contact for industry inquiries?***
Industry inquiries can be directed to:

Phone: (410) 854-6091, or
Email: bao@nsa.gov

115. ***Who is the contact for Department of Defense (DoD)/US Government Client Inquiries?***
DoD/US Government Client inquiries can be directed to:
Phone: (410) 854-4200, or
Email: iad_ccc@nsa.gov

116. ***Where can more information about National Information Assurance Partnership (NIAP) Protection Profiles be found?***
For further questions about Protection Profiles, contact NIAP:

Phone: (410) 854-4458
Email: niap@niap-ccevs.org
Fax: (410) 854-6615

Back to Index