attila SECURITY

Your Guide to Building a CSfC Approved Solution

Introduction

This guide is built to help individuals looking to build a Commercial Solutions for Classified (CSfC) approved solution. It provides guidance on how to use the resources available, navigate the CSfC process, and what to expect from CSfC component vendors.

This guide will help you learn about:

- Which CSfC Capability Package your solution best fits with;
- The process of combining components to build a CSfC solution;
- How to get your final solution approved and registered with the CSfC;
- Using a Trusted Integrator to build your solution;
- What you should expect from CSfC component vendors; and
- The requirements for maintaining your CSfC solution approval.

Most organizations looking to implement a CSfC solution already understand the basics of CSfC certification. This guide will get right into the meat of how to build your CSfC solution, but we've also included background information on the CSfC Program in Appendix A, should you want to bone up.

Table of Contents

Why choose a CSfC solution?

For decades, Type 1 has been the National Security Agency's most prized cybersecurity designation, denoting technology that can effectively keep the nation's most classified information under lock and key.

Recent years, however, have seen the growth of NSA's Commercial Solutions for Classified (CSfC) program, which offers an alternative to Type 1 products.

With these two competing options, it is important to understand what the difference between Type 1 and CSfC really is, and which one is best for your use case.

The technology within NSA Type 1 and CSfC is different, as are the manufacturers of this technology: the NSA itself or trusted systems integrators in the former case, and third-party commercial vendors in the latter.

However, the purpose of both is the same: helping the U.S. government to protect classified data.

The CSfC Program seeks to use the production volume of commercial vendors in order to provide alternatives to existing methods of achieving secure transmission of classified data. It allows you to more efficiently meet your needs and provides some benefits over government-off-the-shelf solutions.

It's important to note that CSfC represents an alternative to Type 1 solutions, not a replacement for them as of yet.

According to the NSA CSfC handbook: "NSA CSfC has not replaced Type 1 solutions. Based on the client's needs, the NSA will use the correct tool for the right job."

Type 1 products are still widely in use across U.S. government agencies, however they tend to be seen as more of a legacy solution. Rather than converting from Type 1 solutions to CSfC, the debate is more about selecting between Type 1 and CSfC for new initiatives and replacing legacy Type 1 solutions as IT refreshes occur.

The advantages of CSfC include:

- **Full end-to-end solutions**: Leveraging multiple vendors and approved components to build your final solution allows you to meet the unique requirements of your project and be certain that the entire end-to-end solution is secure.

- **Based on the highest standards**: All of the components that are CSfC approved leverage open, non-proprietary interoperability and security standards that are driven and monitored by NSA and its team of engineers, threat analysts and cyber experts.

- **No need for specialized training**: Using Type 1 products requires advanced knowledge that you can't develop overnight. CSfC, on the other hand, requires only knowledge of commercial technologies that already make up standard cybersecurity architectures, so in most cases, your team doesn't have to go through special training to use them.

- **The total cost of ownership (TCO)**: The up-front cost of CSfC is generally higher when compared with Type 1 solutions. But after several years, the TCO of CSfC decreases significantly, to the point where it becomes the much less expensive solution.

- **Faster to start**: Although it depends somewhat on the organization, it's usually easier to get up and running quickly with a CSfC solution. This will only become truer as the adoption of the CSfC program increases. Type 1 can sometimes be quicker because it's a known quantity for the "old guard" who have been in the field for decades, but this should change with greater awareness of CSfC.

- **Higher technical flexibility**:
If you have limited options for backhaul on your Internet connection, CSfC is often the wiser choice as it enables you to use any common type of Internet connection, from satellite to 4G. Type 1, on the other hand, often limits you to certain satellite networks or dedicated Internet connections such as MPLS links, which can be very expensive.

- **Less risk of ownership**: Using CSfC products involves a lower risk of ownership due to the less stringent security requirements and the use of commercial hardware. For example, there's no need to place all of the devices in a secure safe watched by guards 24/7, as is required with a Type 1 solution. This also means that CSfC is good for situations that are inherently higher risk.

Thanks to its flexibility and ease of getting started, CSfC excels when it comes to any type of remote work or any situation where you need to set up a temporary SOC (security operations center).

It's also easy to imagine where CSfC would shine for future use cases such as drones, which can potentially be shot down and lost to the enemy — in which case, you wouldn't want Type 1 equipment falling into the wrong hands.

See a CSfC solution in action.

DoD Agency Mobilizes Communications for Classified Networks

Attila's GoSilent implemented as a secure, portable, low cost, high-bandwidth VPN for CSfC communications campus-wide.

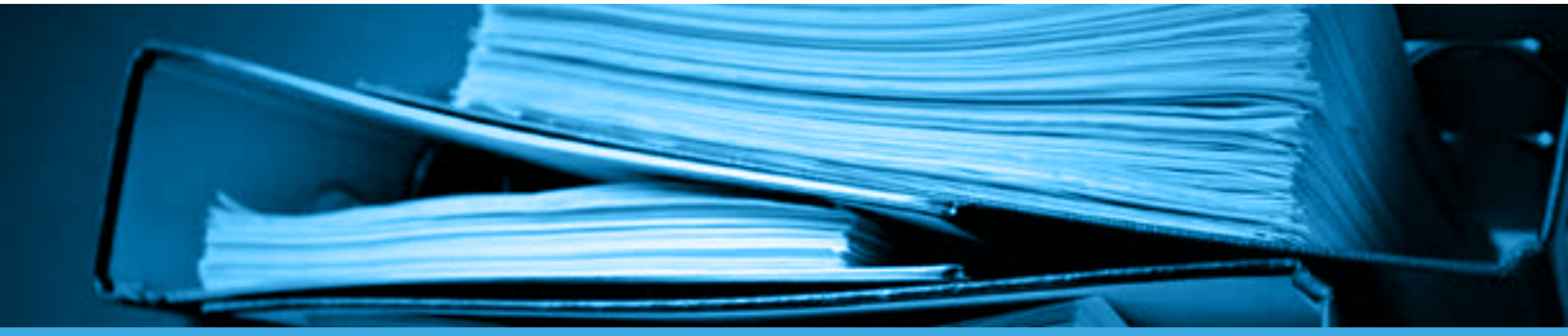
CSfC Capability Packages

As part of the CSfC program, NSA offers several Capability Packages as a starting point for users to implement their own solutions. The products, or components, used to build CSfC solutions must be selected off the CSfC Components List. These components have been certified by NSA's rigorous National Information Assurance Partnership (NIAP) certification along with Federal Information Processing Standards (FIPS) when applicable.

The CSfC Capability Packages (CPs) are reviewed, updated and re-published for use on a regular basis. CPs provide vendor-agnostic requirements for the implementation and configuration of a secure solution within a certain architectural area. There are currently four CPs:

- **Mobile Access Capability Package:** Describes how an organization can build a solution that allows remote endpoints to communicate back to the highly-protected primary network over unclassified networks or the open internet without risking security to classified information.
- **Multi-Site Connectivity Capability Package:** Describes how an organization can build a solution that connects various site networks together and allows them to communicate with each other over unclassified networks or the open internet without risking security to classified information.
- **Wireless LAN Capability Package**: Describes how an organization can build a solution that allows for campus-wide secure connectivity when protected by a physical barrier or perimeter.
- **Data-at-Rest Capability Package**: Meant to help those working to implement a solution that will protect classified data stored on end-user devices.

In addition to the CPs themselves, there are also CP Annexes. Annexes provide similar vendor-agnostic information and architecture guidance but focus on areas that apply across more than one CP.



Choosing the right Capability Package

The capability package you choose to use as the starting point for your CSfC solution will depend upon what you are trying to achieve. You will also find that your ultimate solution, or set of solutions, may need to span multiple capability packages.

Most of the time, you'll find that you start with an initial solution and then layer more components on top of that to incorporate the remaining capability packages.

For instance, a common maturity growth path begins with the implementation of a solution for remote access to your main, centralized network (Mobile Access CP), at which point you'll need to determine how the data on your end-user devices are protected in the field (Data-at-Rest CP).

Once you've implemented that solution successfully, you may be ready to take the next step and expand to multiple sites or campuses that need to connect their primary networks together (Multi-Site Connectivity CP).

And, finally, you may decide it is time to offer wireless connectivity across a physically protected campus (Wireless LAN CP).

Below, you'll find a breakdown of which capability package would be a fit for the type of goals you are looking to achieve.

Capability Package	Common Applications
Mobile Access	• Allowing team members to check email or work from home. • Supporting mobile access for traveling employees or field operatives. • Allowing network access for external vendors or suppliers. • Deployment of mobile SOCs or command centers. • Allowing connectivity over 4G, cellular or satellite networks.
Multi-Site Connectivity	• Connecting remote offices or branches on a single backbone network. • Connecting vendor or supplier networks as a separate branch. • Leased line functionality for offices requiring access to classified information.
Data-at-Rest	• Allowing storage of classified data on devices outside of a physically protected office location.
Wireless LAN	• Providing secure wireless access across an entire campus protected by a physical perimeter.

The solution you deploy should incorporate the architecture that best meets your overall goals, and details regarding the various architectures are spelled out in the various capability packages.

An example of this would be the differences between the architecture needed to achieve a Mobile Access solution vs. a Multi-Site solution. We will demonstrate this with some diagrams of our solutions that can be used for each.

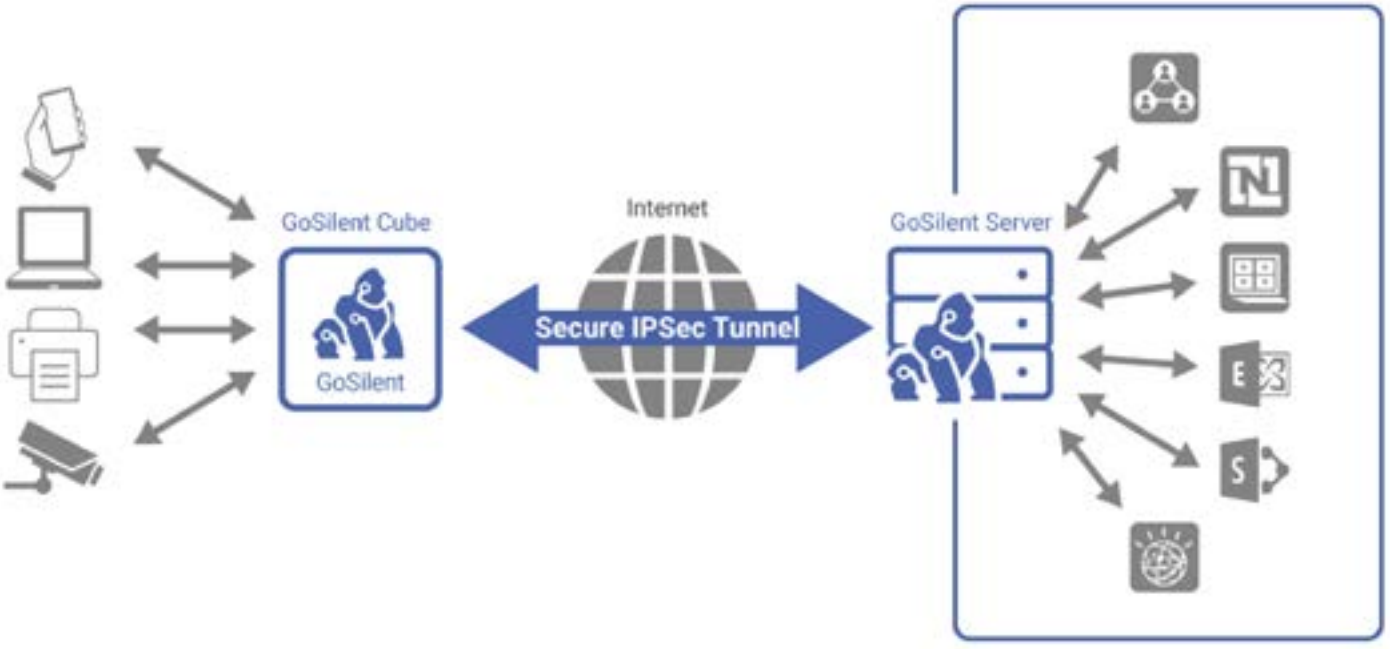
Mobile Access Solution

GoSilent Server, our **CSfC approved solution for mobile access**, works in conjunction with our GoSilent Cube to create secure connections between external devices and your protected internal network.

GoSilent secures a connection to the enterprise server and creates an "IPSec tunnel" inside the enterprise firewall. In this manner, users can securely access corporate resources without being exposed to attack over an open WiFi or Internet connection.

Once GoSilent secures a connection to the enterprise server and creates a secure "IPSec tunnel" inside the enterprise firewall, IP-enabled devices can securely retrieve, send and store data behind the corporate firewall.

You'll see that in this architecture, most of the requirements for CSfC components live on the end-user device.



Multi-Site Connectivity Solution

When combined with a GoSilent Server (GSS) virtual appliance deployed at each location, or site, GoSilent Site-to-Site, our CSfC approved solution for multi-site connectivity, connects multiple disparate Local Area Networks (LAN) together.

On each GoSilent Server, the first network interface is connected to the Local Area Network (LAN) onsite, and the second network interface is connected to the Wide Area Network (WAN), or typically the internet.

The GoSilent Servers at each location establish a secure IPSec IKEv2 VPN tunnel between each other and then the devices and applications on the two disparate Local Area Networks are able to communicate together. Administrators can also restrict the device and application communications with firewall functionality.

In this instance, most of the required CSfC components live on the server-side and there are larger requirements for performance and throughput due to the volume of data being transmitted.

Where to start

Proper implementation of CSfC requires at least half a dozen components from different vendors in which each component within your final product will need to be CSfC approved.

To simplify the process, NSA provides the **Capability Packages**, which include detailed reference architectures to be used as a starting point for building a CSfC solution. Using a Capability Package greatly increases the odds that your final CSfC solution will receive NSA certification.

You'll want to start by defining the goals of your project, and ideally, you'll want to start small. Pick one of the capability packages to focus on first, build that solution and get it approved before moving on to any of the others.

Most commonly, organizations begin by implementing a mobile access solution.

Finding CSfC component vendors

Once you have defined your goals and selected the proper capability package to use in building your architecture, it's time to find the components you need to execute.

The CSfC Components List, maintained by NSA, keeps a running list of all CSfC approved components across a variety of categories:

- Authentication Server
- Certificate Authority
- Email Clients
- End-User Device / Mobile Platform
- File Encryption
- Hardware Full Drive Encryption
- IPS
- IPsec VPN Client
- IPsec VPN Gateway
- MACSEC Ethernet Encryption Devices
- MDM
- Session Border Controller
- Enterprise Session Controller
- Software Full Drive Encryption
- TLS Protected Servers
- TLS Software Applications
- Traffic Filtering Firewall
- VoIP Applications
- Web Browsers
- WLAN Access System
- WLAN Client

Based on the architecture you are trying to achieve, you can browse the categories within the list to find vendors of the components you need that meet CSfC standards.

As you do this, keep in mind that products listed in the Archived Product list are no longer approved for use in new CSfC solutions.

Building a solution

Now you can start designing the architecture of your unique solution, which is often a process that you can work with some of your identified vendors to execute.

Layering solutions from multiple vendors, all of which have individually achieved CSfC certification, will allow you to build a unique architecture that is itself up to CSfC standards and designed to meet your goals.

You will ultimately be responsible for ensuring that your final product satisfies interoperability needs between the multiple components you combine, and that the overall architecture still meets CSfC standards. This is where the use of a **Trusted Integrator** might be helpful, as they are skilled at doing both.

Correctly utilizing the Capability Packages and available Protection Profiles will aid you in this endeavor. NIAP has created more technology-specific certifications, referred to as **Protection Profiles (PP)**. This new method of certification provides assurance that a product meets exact compliance requirements for a specific product category in order to provide repeatable and testable evaluation results across that entire product category.

It is highly recommended to involve the **CSfC Project Management Office (PMO)** early in the design process. Before finalizing your design, you can (and should) do all of the following:

- Advise NSA of your plan to register a solution, before finalizing the design.
- Obtain a Solution Registration Identification number.
- Coordinate with the CSfC PMO to provide your documentation ahead of obtaining a signed version with the Authorizing Official (AO) so that CSfC engineers can review, advise and make recommendations.
- Configure and test your system using guidance from the CSfC engineers.

CSfC Solution registration process

Once you have a finalized design, it's time to submit your solution for registration and approval by the NSA. Before submitting, it is always good to take one final review of the associated capability package and ensure you have met all the requirements outlined in it.

The CSfC Solution Registration process is as follows:

1. **Build your Capability Package documentation** (keep in mind there are separate versions of the following forms for the different capability packages):
   a. Registration Form
   b. Compliance Checklist
   c. Deviation Forms (if applicable)
   d. Network diagrams

2. **Obtain a signature from your Authorizing Official (AO):**
   Send your completed paperwork to your AO to sign. By signing, an AO is "asserting compliance with the published CP and acknowledging and accepting the risk of fielding a CSfC solution" (**source**).

3. **Submit your completed and signed documentation:**
   Completed Solution Registration packages should be emailed directly to the CSfC PMO.

4. **Letter of acknowledgment:**
   a. Once NSA verifies compliance, it will provide a letter of acknowledgment that registration was completed and the time period for which it will last.
   b. You will be required to re-register your solution at the close of that time period.

Using Trusted Integrators

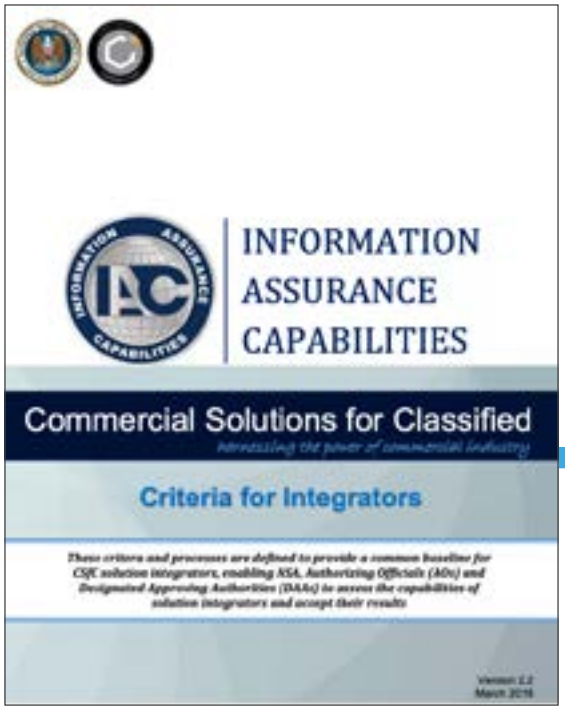
If you're daunted by the very prospect of getting started, NSA also provides **a list of Trusted Integrators** - third-party contractors who have met a **strict set of criteria**. These organizations can help you navigate the CSfC process, offering their assistance and technical expertise along the way.

Trusted Integrators have strong relationships both with the clients they serve and a deep understanding of many components on the CSfC Approved Component List. All trusted integrators are individually vetted by the CSfC PMO prior to inclusion on the list. While it is not required to use a Trusted Integrator to build your solution, it is highly encouraged by CSfC and will improve your chances of getting a solution registered quickly.

Some of the requirements that Trusted Integrators must meet in order to be included on the list are:

- 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)

Having said this, there is considerable variation in the level of experience that Trusted Integrators have with implementing CSfC solutions, so it is worth vetting the integrators you are considering working with and asking specifically about their prior successes with CSfC.



You can review the full criteria for integrators here.

The Process to get Certified

In order to get a component CSfC approved, a vendor must first go through the **NIAP certification process**. The NIAP **Product Compliant List** is a precursor for inclusion in the **Commercial Solutions for Classified (CSfC) Components List**, as well as others like the Defense Information Systems Agency (DISA) Unified Capabilities Approved Products List (DoD UC-APL).

In order to obtain NIAP Certification for a product, manufacturers must go through all of the following steps:

1. Engage and establish a contract with an accredited national laboratory;
2. Select Target of Evaluation (TOE), a product or system that will be the subject of evaluation;
3. Choose the appropriate NIAP Protection Profile(s) they fit within;
4. Establish a Security Target (ST), a set of security requirements and specifications to be used as the basis for evaluation (**You can view Attila's Security Target as an example**);
5. Submit a package with all of the above information to the NIAP office;
6. Receive approval to start the evaluation process from NIAP office (at this point, the product will be placed on the NIAP in-evaluation list);
7. Complete required documentation and testing with the previously-selected lab and submit all completed testing results to the NIAP office;
8. Receive final certification from NIAP and the Common Criteria Evaluation and Validation Scheme (CCEVS).

Once all of these steps are completed, the product will have a NIAP certification and will be placed on the NIAP Product Compliant List (PCL).

Depending upon other compliance and certification needs, the product may still need additional certifications as well, like NIST or FIPS. However, NIAP certification is the first step, or foundation, upon which these further certifications will rely.

Once NIAP certification is achieved, the component developer is required to sign a Memorandum of Agreement (MoA), a legal document that describes the terms and details of a partnership, with NSA and submit an extensive CSfC Questionnaire for each product.

NSA reviews these items and then determines if the product is suitable for inclusion on the CSfC Components List.

Encryption Requirements

The Commercial National Security Algorithm Suite (CNSA Suite) provides new algorithms for those customers migrating from Suite B algorithms.

CNSA Top Secret (TS) level encryption is the same technology used by U.S. government agencies like the NSA, DoD and other governing bodies. Previously known as Suite B, military-grade, or classified federal government standard, Advanced Encryption Standard (AES) 256-bit end-to-end encryption is the most secure solution in the marketplace. AES-256 is the first publicly accessible and open cipher approved by the NSA to protect information at a classified, top-secret level.

With over 14 rounds of encryption, each 256-bit encryption key scrambles the data and divides into 128-bit blocks. The number of possible keys in the AES 256-bit encryption is 2 to the power 256 (a 78-digit number), making the code virtually impossible to crack by brute force attack. Additionally, with Top Secret level encryption, both the sender and the receiver must know and apply the same secret 256-bit key. The key is never stored on any server, and only those communicating have access.

Additionally, users who want to send and receive mobile data, including voice and video calls, need to encrypt this data using a **double VPN tunnel**.

Requirements and maintaining Certification

Requirements, Protection Profiles, and even the capability packages themselves undergo regular updates to account for new security capabilities, address new vulnerabilities, and to align with updated industry best practices.

Updates to Protection Profiles can be found on the NIAP website.

As updates happen, products on the CSfC Component List may lose their certification. Vendors also may choose not to renew certifications when their renewal period expires. For this reason, CSfC maintains an **Archived Components List.**

If you have a solution that includes any component that is moved to the Archived Component List, you'll have two years to transition from that component to a new solution that is currently approved.

Using and maintaining your CSfC Solution

You and your Authorizing Official (AO) will be responsible for ensuring your solution, once fielded, remain in compliance. Doing so will mean ensuring that all configurations of your solution stay true to the original, approved design.

When your renewal period is approaching, the CSfC PMO will send notifications at 120 days, 60 days and 30 days out to remind you to renew your certification. You'll be responsible for submitting an updated registration form and compliance checklist to renew your certification.

NSA will review your updated forms to ensure you remain in compliance, and none of your components have moved to the **Archived Components List**. If approved, you'll receive a new acknowledgment letter with a new period of certification.

Common CSfC FAQ

Below is a common FAQ about building a CSfC solution.
NSA has also developed a full list of FAQs.

When implementing a Mobile Access solution, what protection do I need for the data stored on my End-User Device?

The CSfC Mobile Access Capability Package provides specific details on the differences between types of end-user devices (EUD) which may connect to a network from the outside. To successfully implement Data-at-Rest (DAR) requirements, your end device must be one of the following:

- **EUD with DAR:** The DAR solution implemented on the EUD must be approved by the NSA. It has to be registered with NSA's DAR Capability Package and approved as a solution for the protection of classified information at the Red Network level. In this case, continuous physical control of the EUD must be maintained without fail.

- **Classified EUD:** If this design option is chosen, the EUD must be treated as a classified device and can only be used when applying appropriate physical security measures. The EUD must also use encryption capabilities to protect any private keys and classified information stored on the device. Again, in this case, continuous physical control of the EUD must be maintained without fail.

- **Thin EUD:** This option implements techniques to design and build the EUD in such a way that it prevents any classified information from being saved in persistent storage on the physical device. Some methods for achieving this include using a virtual desktop infrastructure (VDI) configured to stop any Red Network-level data from being saved on the EUD, restricting the virtual machine to a non-persistent state, and configuring the operating system on the EUD to stop users from saving data locally. In this instance, the EUD must again use encryption capabilities to protect any private keys and classified information stored on the device. Again, in this case, continuous physical control of the EUD must be maintained without fail.

Appendix A:
General Information About the CSfC Program & Glossary

The Commercial Solutions for Classified (CSfC) program was established in order to enable U.S. government agencies and their customers to take advantage of affordable and readily available commercial off-the-shelf (COTS) IT solutions that meet the NSA's stringent security guidelines for the transmission of classified data.

Capability Packages: As part of the CSfC program, NSA offers several Capability Packages as a starting point for users to implement their own solutions. The products, or components, used to build the CSfC solutions must be selected off the CSfC Components List. These components have been certified by NSA's rigorous NIAP certification along with FIPS when applicable.

The CSfC Components List: A running list, maintained by NSA, of all CSfC, approved components.

NIAP: NIAP certification is a commercial cybersecurity product certification that is mandated by federal procurement requirements (CNSSP 11) for use in U.S. National Security Systems (NSS). Its primary purpose is to certify commercial technology or products which will be used to handle sensitive data.

NIAP Product Compliant List: A running list, maintained by NIAP, of all NIAP Certified Products.

Protection Profiles (PP): Exact compliance requirements for a specific NIAP product category in order to provide repeatable and testable evaluation results across that entire product category and achieve certification.

Trusted Integrators: A list, maintained by NSA, of organizations that can help you navigate the CSfC process, offering their assistance and technical expertise along the way.

attila
SECURITY

attilasec.com