Data-At-Rest Encryption Series: Commercial Solutions for Classified

Read About

Introduction

This white paper is the second in the series of related white papers discussing data-at-rest (DAR) encryption. The first paper explored the reasons to protect DAR, encryption basics, and possible encryptor types – Commercial Solutions for Classified (CSfC) and Type 1. Both types are National Security Agency (NSA) encryption programs that support the protection of classified DAR. This paper focuses on CSfC and provides details and background information on this vital NSA program.

The third white paper in this series examines public information regarding NSA Type 1 encryption and the last of the series compares both CSfC and Type 1 to propose a methodology for encryption selection.

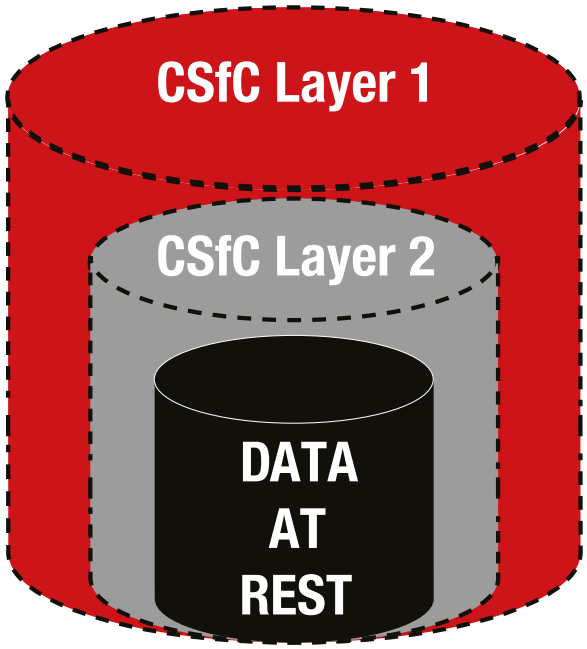

Figure 1: CSfC: Two Layers, One Solution

CSfC Terminology

Terminology specific to CSfC can be confusing. Gaining a basic understanding of the vocabulary used by the program is necessary before diving deeper into program specifics.

+ **Component**: a CSfC product developed by a COTS vendor, tested by an approved laboratory, certified by the National Information Assurance Partnership (NIAP), and approved by NSA. Typically a component comprises one layer of a two-layer solution (see Figure 2 for a simple example). The only acceptable components are:
  - Software full disk encryption (SWFDE)
  - Hardware full disk encryption (HWFDE)
  - File encryption (FE)
  - Platform encryption (PE)
+ **Solution**: two independent layers of encryption components (see Figure 2 for a simple example). Solutions must be composed of a combination of two of the component types:
  - SF = SWFDE + FE
  - PF = PE + FE
  - HF = HWFDE + FE
  - HS = HWFDE + SWFDE
  - HH = HWFDE + HWFDE (proposed in draft DAR CP 4.8 as of this writing)
+ **End User Device (EUD)**: refers to anything employed with two layers of CSfC DAR protection. Thus an EUD is a DAR-protected system. Terms like system, DAR solution, or device are equivalent.
+ **Capability Package (CP):** a product-neutral document that describes system-level solution frameworks, documenting security and configuration requirements for customers and/or integrators. It is a set of guidance provided by the NSA that describes recommended approaches to provide architectures and configuration requirements that empower IA customers to implement secure solutions using independent, layered COTS components to protect classified information. This package will point to potential products that can be used as part of this solution. CPs are used by COTS vendors, integrators, and end customers alike.
+ **Trusted Integrator (TI):** persons or companies that the NSA has vetted to architect, design, integrate, test, document, field, and support a solution. While not required, the use of a TI can be a risk mitigation factor. The current TI list can be found at: https://www.nsa.gov/Resources/Everyone/csfc/Trusted-Integrators/.
+ **Protection Profile (PP)**: a requirements document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.
+ **Collaborative Protection Profiles (cPP):** a PP that has been reviewed and accepted by the international Common Criteria community.
+ **Commercial National Security Algorithm (CNSA):** a set of commercial algorithms capable of protecting data through Top Secret level (previously known as Suite B).
+ **Full Disk Encryption (FDE):** the process of encrypting all of the data on a hard drive. Sometimes referred to as whole disk encryption, FDE encrypts all data (with certain exceptions) on the storage device and permits access to the data only after successful authorization to the FDE solution.
+ **Software Full Disk Encryption (SWFDE):** FDE accomplished with software (SW). Software like Linux's LUKS is an example of SWFDE.
+ **Hardware Full Disk Encryption (HWFDE):** FDE accomplished with hardware (HW). An ASIC like the eNova MX-256 is an example of HWFDE.

KEY TAKEAWAY

The CSfC program has its own unique jargon. It is important to use the words component and solution properly when discussing.

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

What is the CSfC Program?

CSfC is an important part of the NSA's strategy to deliver secure cybersecurity solutions. The program leverages commercial encryption technologies, such as those employed in cars, mobile phones, tablets, and home security systems, to deliver cybersecurity solutions for classified applications quickly.

The first white paper in this series (Data-At-Rest Encryption Series: Data Threats and Protection) explained that DAR can be threatened from four different vectors, some internal and some external. For deployed DAR applications (e.g., planes, helicopters, unmanned underwater vehicles, ground vehicles), vehicles may be lost during a mission. The DAR can also be lost during transport from the deployed vehicle back and forth to the ground station. Once mission data has been safely downloaded and stored on a network, it is still at risk to relentless hackers (nation-state and independent) and to unknown internal bad actors with malicious agendas.

Layered Solutions

CSfC is founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in various applications. The key word is layered, as two layers of CSfC encryption are required to be fielded as a *solution* (see Figure 2 for a simple graphical explanation). For more information on CSfC terminology, see the white paper CSfC Series: Inner versus Outer Layer.

When properly implemented, a single layer of DAR encryption from the Commercial National Security Algorithm (CNSA) Suite is sufficient to protect classified data; however, two layers are used to mitigate risks due to a failure in one of the layers. Such a failure may result from accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability. Any of these can result in the exposure of classified DAR. The use of multiple layers, implemented with components meeting the CSfC vendor diversity requirements, reduces the likelihood that a single vulnerability can be exploited to reveal protected information.

If one of the encryption layers is compromised or fails in some way, the second layer can still provide the encryption to safeguard the classified data. If both layers are compromised or simultaneously fail, then it is possible the classified data will be readable by an adversary. The goal of the DAR solution is to provide redundant protection that either minimizes the possibility of both layers failing at the same time or requires an adversary to defeat both mechanisms. Given enough time, any encryption system may be defeated. But with two layers, that task becomes significantly more difficult.

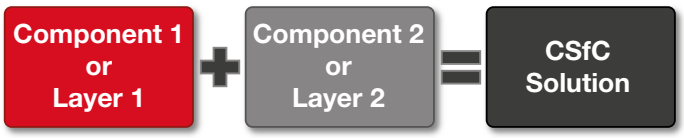

Figure 2: Basis CSfC Solution Concept

Capability Packages

The NSA has developed, approved, and published solution-level specifications called Capability Packages (CP) to provide customers with ready access to the information needed to use COTS solutions in their daily operations and protect their data against today's threats to DAR. CPs for Mobile Access, Multi-Site Connectivity, Campus Wireless LAN, and DAR solutions are now published on the CSfC website.

The CP for DAR has been available for several years. After consultation with the marketplace, the NSA has updated the DAR CP several times. Manufacturers design to the DAR CP and track the updates to the CP in order to stay current and up to date for certifications and re-certifications (more on that subject later).

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

Who uses the DAR CP?

Primarily, the DAR CP provides guidance to DAR solution integrators and end users. The CP provides specific guidance for the implementation of a solution through a virtual checklist of requirements. Each requirement is noted with Objective or Threshold. Authorizing Officials (AO) use the DAR CP to put together concept of operations (CONOPS) for each solution implementation. In addition, the DAR CP provides guidance to product (component) vendors whose products are used in DAR solutions.

+ **COTS Vendors / COTS manufacturers** → design products (components) that can be used in CSfC solutions based on DAR CP. NOTE: The terms COTS manufacturer and COTS vendor are considered interchangeable.
+ **Trusted integrators** → combine approved or in-process CSfC components into a solution for an end user based on DAR CP.
+ **End Users and AO** → define CONOPS for each application based on DAR CP and the solution used.

Protection Profiles

While the DAR CP provides guidance for solution development and implementation, it also provides guidance to COTS vendors developing components (layers). For such COTS product vendors, the NSA also develops and publishes product-level requirements in United States Government Protection Profiles (PP) after consultation with industry, government, and academia.

KEY TAKEAWAY

The "Protection Profiles" provide technology specific compliance requirements for a specific product category (ex. DAR).

NIAP lists the current approved PPs at https://www.niap-ccevs.org/Profile/PP.cfm. Any product that is to be evaluated must claim compliance to a NIAP-approved PP.

In the United States, NIAP oversees the evaluation of commercial off-the-shelf (COTS) information technology (IT) products for conformance to Common Criteria (CC). DAR devices fall under this IT category. Thus DAR storage devices like network attached storage (NAS) must be evaluated against one (or more) NIAP-approved PP.

KEY TAKEAWAY

This acceptance by CCRA can be important if you plan to export the system that uses the DAR solution to other countries besides the United States.

NIAP is a member of the international Common Criteria Recognition Agreement (CCRA). At the time this paper was written, 31 nations are members of the CCRA. A PP that the wider CCRA community has approved will be designated a collaborative Protection Profile (cPP). If a product is evaluated against a cPP, then it is likely that evaluation by NIAP will also be accepted by the CCRA without further testing and thus can be used in all 31 countries without further testing.

Where Can I Find CSfC Resources?

The best place to find more information regarding the CSfC program is on the NSA website.

1. Start here: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/ where you will find a brief video from the Chief of the NSA Cybersecurity Solutions group and others from NSA, industry, and military. This video may allay any hesitancy whether CSfC is a viable, approved encryption methodology.
2. Review the CSfC tri-fold brochure: https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/handout-trifold.pdf. The brochure introduces the CSfC program and outlines processes for component vendors and solution users.

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

a. Figure 3 shows the front page of the brochure. Contact information is available plus a workflow for component vendors. Commercial vendors can follow the CP guidelines and design a DAR product without program support from Department of Defense (DoD).

Figure 3: CSfC Tri-Fold Brochure (front page)

b. Figure 4 shows the back page of the brochure. *What is CSfC? and What is a Capability Package?* can be found here, as well as the workflow for solution providers.

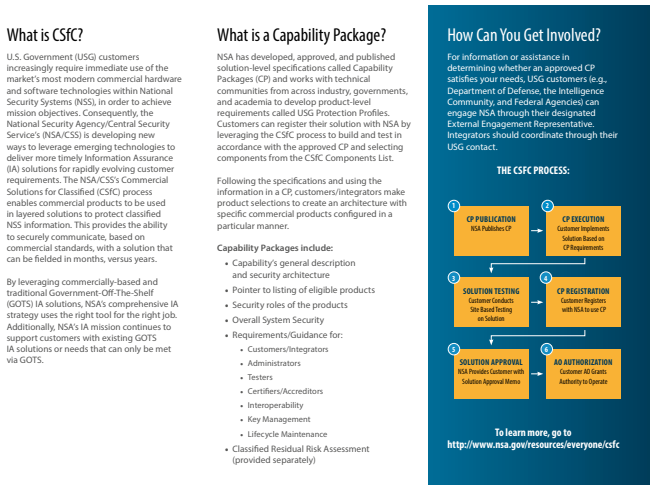

Figure 4: CSfC Tri-Fold Brochure (back page)

3. Review the CPs. This paper focuses on DAR solutions so it recommended going straight to the DAR CP: https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/capability-packages/dar-cp.pdf. CPs are also available for Mobile Access, Multi-Site Connectivity, amd Campus Wireless LAN solutions.
   a. The current DAR CP should be used. However, a draft CP may exist which indicates upcoming changes that may be important depending on if you are developing a solution or a component.
   b. The CSfC process is meant to be dynamic, reflecting the current best practices and known threats which keeps it up to date and relevant.
   c. Within the DAR CP, review the DAR solution options.
4. You may also wish to review the CSfC Factsheet: https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/factsheet.pdf.

KEY TAKEAWAY

The NSA provides clear and public documents for CSfC end users, solution integrators, and component vendors. If you do not find what you need in the documents, then contact the NSA CSfC group directly. You will find them very helpful.

Steps for Component Developers

The CSfC program allows and actually encourages commercial developers to create DAR products based on the DAR CP and tested against PPs. With clear guidance from the DAR CP, commercial developers can invest in new products ahead of the market need. End customers benefit from sourcing these products which are already developed, tested, and approved and thus ready for solution implementation.

Figure 5 shows the basic steps a product developer should follow. An example of a DAR product developed based on this guidance is shown in figure 6.

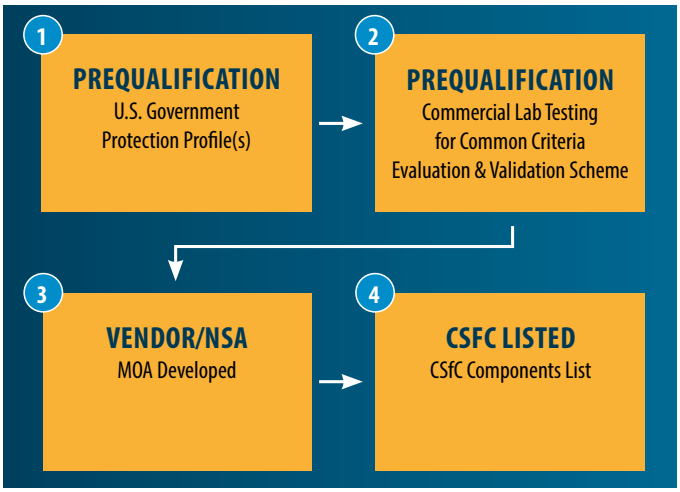

Figure 5: Component Developer Guide

1. Review the United States Government (USG) Protection Profile(s). For DAR, there are a few choices.
   a. A list of the current DAR protection profiles can be found on the NIAP website: https://www.niap-ccevs.org/Profile/PP.cfm.
   b. Four PPs are currently listed for encrypted storage. Two are for file encryption (FE) and two for full disk encryption (FDE), which apply to both HWFDE and SWFDE.
   c. The example EUD in figure 6 uses the HS solution design and thus used the two FDE profiles.
   d. Both FDE profiles are fortunately collaborative, which means that they have been accepted by the international Common Criteria community.

KEY TAKEAWAY

This product process assumes one big thing not mentioned: the vendor must actually specify, develop, and test the product to be listed. This can be a lengthy process, but is usually done ahead of the market need, as most COTS products are.

2. Choose a Testing Lab.
   a. NIAP-approved Common Criteria Testing Laboratories (CCTL) are listed at: https://www.niap-ccevs.org/Documents_and_Guidance/cctls.cfm.
   b. These IT security testing laboratories are all accredited by the National Institute of Standards and Technology (NIST) under their National Voluntary Laboratory Accreditation Program (NVLAP) and meet the Common Criteria requirements to conduct IT security evaluations.
3. The vendor (product or component developer) and NSA sign a Memo of Agreement (MOA).
   a. This MOA process begins after the product is in formal evaluation with a CCTL. Products in Evaluation (PINE) will be listed: https://www.niap-ccevs.org/Product/PINE.cfm. This step can be important for a vendor because it shows evidence that the product is moving through the approval process.
   b. The MOA will be initiated by NSA once the formal evaluation process has begun at the CCTL.
   c. You will likely find the MOA to be relatively straightforward and not onerous.
4. Product (component) is listed on the CSfC Component List.
   a. After testing by the CCTL is completed, the resulting report(s) must be reviewed and the product certified by NIAP.
   b. NIAP then lists the product on its Product Compliant List: https://www.niap-ccevs.org/Product/index.cfm.
   c. Once certified by NIAP, NSA reviews those results and adds the product to the appropriate CSfC Component List: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/.

Figure 6: Curtiss Wright DTS1 Network Attached Storage

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

Steps for Solution End Users

Prospective CSfC end users can follow the steps outlined in the CSfC Brochure.

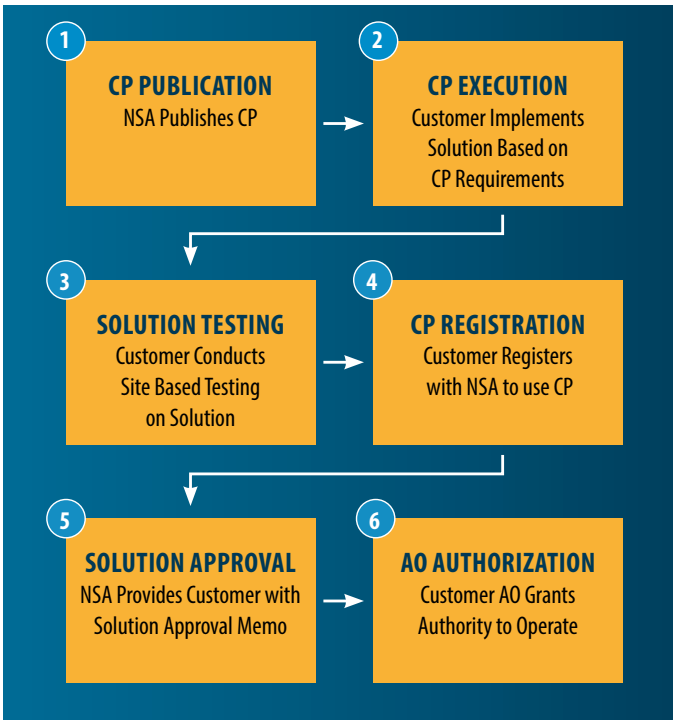

Figure 7: CSfC Solution Guidance

1. Review the CSfC Capability Packages
   a. Select the proper CP for your application.
   b. For DAR, the current CP is version 4.0 located at: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Capability-Packages/.
   c. It is suggested that you also review any draft CP (currently 4.8) which will provide future guidance. For more information on the changes in CP 4.8 read the first white paper in our CSfC Series: Data-at-Rest Capability Package 4.8
2. Customer develops and implements the CSfC solution based on the selected CSfC components.
   a. This is often a lengthy but normal development process required to integrate the two components.
   b. If a trusted integrator is used, they will likely be involved with this step.
3. Customer performs site-based testing of the CSfC solution.
   a. If the solution is to be deployed, testing will occur both in a lab with a simulated system and on the actual vehicle.
   b. If a trusted integrator is used, they will certainly be involved with this step.
4. Once tested, the customer completes a CSfC Solution Registration.
   a. If you have not discussed the application with NSA prior to this step, those discussions will certainly begin at this point in the process.
   b. More details on the solution registration process and the actual forms can be found at: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Solution-Registration/.
   c. These solution registrations are not publicly listed like the component registrations.
5. After review (and likely negotiations), NSA will provide a Solution Approval Memo.
   a. These memos are not publicly listed.
6. After receiving the Solution Approval Memo, the customer AO will grant an Authority to Operate (ATO).
   a. Remember the AO assumes more responsibility in the CSfC process.
   b. Of course, the AO will likely generate additional requirements and procedures as part of the process prior to deployment.

Are CSfC Solutions Being Deployed?

The short answer is yes. CSfC solutions are being proposed and deployed in increasing numbers. Approved CSfC solutions have increased 255% between 2019 and 2020. Approved DAR solutions have increased 43% between 2019 and 2020. Even more striking is the number of DAR solutions being processed, which has gone up 500% year over year.

These dramatic increases in solution processing and approval speak to several possible factors.

+ End customers like the US Army, Navy, and Air Force are accepting CSfC solutions to meet their encryption and data protection requirements. They are now using requirement phrases like 'NSA approved encryption', which opens it up to the possibility of using a CSfC solution.
+ Solutions developers (like Boeing, Lockheed, or Northrop Grumman) are responding to the End Users, new requirements by including CSfC components as well as other alternatives in their trade studies.
+ Components vendors are investing IRAD funds in the development of new COTS encryption products.
+ The NSA has done a great job of listening to the marketplace and supporting vendors and customers alike. Without their responsiveness, this type of success would not have been possible.

KEY TAKEAWAY

CSfC solutions are increasing year over year and finding acceptance by both integrators and end users.

Table 1: CSfC Solutions Metrics 2019 vs. 2020

	February 2020	February 2019	YTD % Increase
Approved DAR Only Solutions	10	7	43%
In-Processing DAR Only Solutions	15	3	500%
Preliminary DAR Only Solutions*	6	N/A	-
Approved Total CSfC Solutions	51	20	255%
In-Processing Total CSfC Solutions	45	45	0%
Preliminary Total CSfC Solutions*	47	41	15%

* Requested ID but has not submitted.

Conclusion

It is critical in today's world that DAR is protected. Internal and external threats are increasing, which dictates the physical security and encryption of DAR. For deployed applications, the vehicle (fighter, UUV, UAV, etc.) may be lost during the mission putting the critical data at risk to exploitation by an adversary.

The CSfC program is robust and growing. COTS developers like Curtiss-Wright are investing significantly in IRAD well ahead of the end customer's needs to ensure CSfC components are developed, tested, and approved for proposal into CSfC solutions. The number of approved CSfC solutions is increasing year over year. Large defense contractors are embracing designing these solutions into new vehicles that will be deployed for many years, if not decades.

Employing a CSfC solution to protect Top Secret mission data is one possible approach. However, one must examine all the factors such as export, certification length, cost, size, weight, and power, before selecting a path.

The next white paper in the Data-At-Rest Encryption Series discusses NSA Type 1 encryption devices using publicly available information. The fourth paper examines the necessary factors to consider when deciding on an encryption approach.

Authors

Steven Petric
Senior Product Manager, Data Solutions
Curtiss-Wright Defense Solutions

Paul Davis
Director, Product Management, Data Solutions
Curtiss-Wright Defense Solutions

Learn More

Products

- Data-at-Rest Encryption Guide
- DTS1 - Network Attached Storage Device

White Papers

- Data-at-Rest Encryption Series

- Part 1: Data Threats and Protection
- Part 2: Commercial Solutions for Classified (CSfC)
- Part 3: NSA Type 1 Encryption
- Part 4: NSA CSfC vs. Type 1 Encryption

- CSfC Series

- CSfC Series: Inner vs. Outer Layer
- CSfC Series: Data-at-Rest Capability Package 4.8

- Choosing the Best Location for Your Data-At-Rest Encryption Technology
- Using Software Full Disk Encryption and Disk Partitioning to Protect and Isolate Network Attached Storage Functions
- COTS Encryption for Data-at-Rest

Case Studies

- Upgrading an Electronic Warfare Suite with an Integrated System Solution
- Rugged Encrypted Data Storage for an ISR Pod

More Resources

- NIST Publication 800-111 Guide to Storage Encryption Technologies for End User Devices

How would you rate this white paper?

1 (low) 2 3 4 5 (high)

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.