


NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Data-at-Rest
Capability Package 5.1.0 Draft 1.0

Version 5.1.0
5 February 2024


CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	0.8	July 2014	Initial draft of CSfC Data-at-Rest (DAR) requirements.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	1.0	September 2014	Official release of CSfC DAR requirements: • Introduced SWFDE/FE (SF) Solution Design. • Aligned with SW FDE Protection Profile (PP) 1.0 & FE Extended Package (EP) 1.0.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	1.8	October 2014	Initial draft of CSfC DAR Version 2 requirements.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	2.0	December 2014	Official release of CSfC DAR Version 2 requirements: • Added PE/FE (PF) Solution Design • Aligned with MDF PP 3.0.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	2.8	May 2015	Initial draft of CSfC DAR Version 3 requirements.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	3.0	March 2016	Official release of CSfC DAR Version 3 requirements: • Added HWFDE/FE and HWFDE/SW FDE (HF and HS) Solution Design. • Updated requirements to reflect new FDE Collaborative Protection Profile (cPP) 2.0. • Discussed the associated. Independent Software Vendor (ISV) technology which aligns with the FDE cPP 2.0. • Added Lost and Found (LF) use case.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	3.8	January 2017	Initial draft of CSfC DAR Version 4 requirements.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR)	4.0	January 2018	Official release of CSfC DAR Version 4 requirements: • Added Removable Media (RM)

Title	Version	Date	Change Summary
Capability Package			Solution Component and Solution Design. • Added continuous physical control. (previously positive control) guidance • Added random password generation. • Added secure file deletion guidance. • Added optional two-factor authentication. • Relocated Threat Section to a separate document available on the CSfC webpage. • Removed the Testing Section to a separate DAR Testing Annex document. • Changed DAR-PE-5 from minimum of 4 characters to minimum of 6 characters.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	4.8	September 2019	Initial Draft of CSfC DAR Version 5 Requirements.
Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package	5.0	18 November 2020	Official release of CSfC DAR Version 5 requirements: • Added Enterprise Management (EM) Use Case. • Added Unattended Operations (UO) Use Case. • Added Hardware FDE/Hardware FDE (H/H) Solution Design. • Added "optional" DAR Location Based Services capability. • Added guidance for Implementing CSfC in a High Assurance GOTS Environment. • Updated glossary and acronym list. • Removed Table 17: Lost and Found requirements table; alternatively, dispersed the requirements into existing tables, now identifiable as "LF" in the "Use Case" column. • Changed RM from a Solution Design to a Use Case.
Commercial Solutions	5.1	5 February 2024	• Expanded options and guidance

Title	Version	Date	Change Summary
for Classified (CSfC) Data-at-Rest (DAR) Capability Package			for 2FA/multi-factor authentication and passwords. • Explored options to allow shorter passwords for mobile devices • Determined if key ingestion is allowed. • Expanded DAR location-based services (DARLS) requirements and testing. • Clarified DAR location-based requirements and testing. • Added new terminology for LADAR: “DAR Location-based Services”. • Added Heartbeat definition • Clarified the Unattended Use-Case. • Clarified Supply Chain Validation (SCV). • Expanded Supply Chain Risk Management Requirements • Added a section on DAR Virtual EUDs. • Added the SWFDE/SWFDE (S2) Solution Design. • Added requirements for EUDs that are using a hypervisor.

Table of Contents

Table of Figures

List of Tables

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency (NSA) Cyber Security Directorate (CSD) publishes Capability Packages (CP) to provide architectures and configuration requirements that empower Information Assurance (IA) customers to implement secure solutions using independent, layered Commercial Off-the-Shelf (COTS) products. The CPs are product-neutral and describe system-level solution frameworks, documenting security and configuration requirements for customers and/or Integrators. It is recommended that CSfC Trusted Integrators be employed to architect, design, integrate, test, document, field, and support the solution. The list of CSfC Trusted Integrators can be found at: https://www.nsa.gov/resources/commercial-solutions-for-classified-program/trusted-integrators.

This CSfC Data-at-Rest (DAR) CP meets the demand for DAR solutions using the Commercial National Security Algorithm (CNSA) Suite. These algorithms are used to protect up to top secret data using layers of COTS products. As defined in Section 4.3.1, the *DAR CP version 5.1.0* enables customers to implement two independent layers of encryption for the purpose of providing protection for stored information on the End User Device (EUD) or DAR protected system, while in a powered off or unauthenticated state. This CP takes lessons learned from proof-of-concept demonstrations that have implemented the CNSA Suite, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

The DAR CP focuses on the implementation of cryptography to mitigate the risk of unauthenticated access to classified data when the device is powered off or unauthenticated. This CP does not protect against malicious code exploits and potential vulnerabilities from updates, operating system (OS) misconfigurations, or the persistence of remnants of key or plaintext material in volatile memory on the EUD when powered on and authenticated, as these conditions are outside of the scope for this version of the CP.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a National Information Assurance Partnership (NIAP)-validated component in a CSfC solution may invalidate its certification and require a revalidation process. To avoid delays, customers and Integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification.

In case of a modification to a component, NSA's CSfC Program Management Office (PMO) requires the component to successfully complete the NIAP Assurance Maintenance Continuity process. Modifications that trigger the revalidation process include, but are not limited to: configuring the component in a manner different from its NIAP-validated configuration, and modifying the Original Equipment Manufacturers' code (to include digitally signing the code).

2 PURPOSE AND USE

This CP provides high-level reference designs and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List available on the CSfC web page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program/components-list), for their DAR solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while at rest. As described in Section 9, customers must ensure that the components selected from the CSfC Components List provides the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold Requirements, or the corresponding Objective Requirements applicable to the selected capabilities, must be implemented, as described in Sections 8 - 12.

Please provide comments on usability, applicability, and shortcomings to your NSA/CSS Client Advocate and the DAR Capability Package maintenance team at CSfC_DAR_team@nsa.gov. DAR CP solutions must also comply with the Committee on National Security Systems (CNSS) policies and instructions. Any conflicts between CNSS or local policy and this CP should be provided to the DAR CP Maintenance team.

Additional information about the CSfC process is available on the CSfC web page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program).

3 LEGAL DISCLAIMER

This CP is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event must the United States (U.S.) Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this CP, even if advised of the possibility of such damage.

The User of this CP agrees to hold harmless and indemnify the U.S. Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of user or third parties, damage to or destruction of property of user or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 DATA-AT-REST PROTECTION OVERVIEW

The goal of the DAR solution is to protect classified data when the EUD is powered off or unauthenticated. Unauthenticated is defined as the EUD state prior to a user presenting and having their credentials (i.e., password, tokens, etc.) validated by both layers of the DAR solution. The DAR

solution is composed dual encryption layers, an outer and inner layer. The outer layer is considered the layer that is authenticated to first, while the inner layer is authenticated to secondly. The data owner determines specific data that must be protected.

In this CP, when the term "EUD" is used, it refers to any solution that contains two layers of CSfC DAR protection. Based on the context and wording of some of the CP language, other terms such as system, DAR solution, or device may be used. These terms can be used interchangeably depending on context of the customer use case, and the data that the customer is protecting. This definition is further explained in detail in Section 5.5.

4.1 Implementing CSfC in a High Assurance GOTS Environment

An option available to users of CSfC, is the concept of a blended solution that uses a CSfC solution, in combination with a High Assurance GOTS solution. For these blended solutions, a High Assurance GOTS solution can be used to replace the entire function of a CP as a whole, but not the individual layers of a solution or security functions provided by one of the layers. While CSfC uses two layers of encryption, this is not required with High Assurance GOTS, where a single layer of encryption is sufficient. For example, if desired, a CSfC DAR solution can be employed in an infrastructure where network High Assurance Internet Protocol Encryptors (HAIPEs) are also being used. The DAR solution is segmented, and its protection is provided by CSfC, while the protection of the network that the information transits is provided by a High Assurance GOTS solution. For additional details or questions about this process, please contact the CSfC PMO office at csfc@nsa.gov.

4.2 Rationale for Layered Encryption

A single layer of CNSA encryption, properly implemented, is sufficient to protect classified DAR. However, a CSfC DAR solution uses two layers of CNSA encryption; not because of a deficiency in the cryptographic algorithms, but to mitigate the risk of a failure in one of the cryptographic components due to accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability, which results in the exposure of classified information. 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 still provides the needed encryption to safeguard the classified data. If both layers are compromised or fail simultaneously, it is possible the classified data will become readable to a threat actor. 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.

4.3 Solution States

The DAR solution states are identified and described in further detail in this section. Once a device is considered classified (i.e., Powered-On with Outer Layer Authenticated State) it will not be considered unclassified (must still be handled in accordance with the implementing organizations' Authorizing Official (AO) policies) until the device is in the powered-off state.

4.3.1 EUD Solution States

Powered-Off State:

In a powered-off state, the device is completely off and not in any power saving state. The EUD is considered unclassified, but must still be handled in accordance with the implementing organizations' AO policies. This applies to all removable media when unplugged from the host system. If the RMs have their own power states, the product documentation must be consulted to determine how to independently switch the product into a powered-off state.

Powered-On and Unauthenticated State:

In a powered-on and unauthenticated state, the EUD is completely on, but the user has not initially logged into either layer. The EUD is considered unclassified, but must be handled in accordance with the implementing organizations' AO policies. This state cannot be entered by logging off after initial logon. This applies to all removable media when plugged into the host system.

Powered-On with Outer Layer Authenticated State:

In a powered-on state with the outer layer authenticated, the EUD is operational where the user has authenticated to the outer layer of encryption. The device in this state is considered classified and should be handled accordingly. This applies to all removable media when plugged into the host system.

Powered-On with Outer and Inner-Layer Authenticated State:

In a powered-on state with the outer and inner-layer authenticated, the EUD is operational when the user has authenticated to two layers of DAR encryption. The device in this state is considered classified and should be handled accordingly. This applies to all removable media when plugged into the host system.

Locked or Logged Out State:

In a locked or logged out state, the device is powered-on but most of the functionality is unavailable for use. User authentication is required to access functionality. This functions as an access control and may provide one layer of DAR protection. The device in this state is considered classified and should be handled accordingly. This applies to all removable media when plugged into the host system.

4.3.2 Enterprise Management (EM) Server & Mission Control Element (MCE) Solution States

Always on State:

The "always on state" in this section applies to the server acting as part of a remote access architecture or a client-server architecture, controlling the DAR enterprise managed solution. This state does not apply to the server that is acting as a DAR EUD with two layers of protection. The "EUD Solution States," described above in Section 4.3.1, is only applicable to a server, if that server is acting as the DAR EUD being provisioned with two encryption layers to protect the server's storage. In this CP, it is assumed that the EM server, base station, or MCE will be protected within a secured facility, as prescribed by the AO (i.e., Sensitive Compartmented Information Facility (SCIF), secured room, etc.). This CP does not provide sufficient mechanisms to protect classified data on the EM server, unless that server is also treated as a DAR EUD and is protected with two layers of DAR. In an always on state, the DAR enterprise management server, the base station, or the Mission Control Element (MCE) is always powered on to

keep processes up and running. Additional details about these components and solutions, can be found in Sections 5.6, 7.3, and 7.4.

4.4 DAR CNSA Suite

As the portability of EUDs increase, the requirements for when and how classified data is protected also increases. EUDs can be used in both physically protected and physically unprotected environments. Solutions using commercial products must protect classified data on the EUD by using two layers of encryption with the approved CNSA Suite, referenced in Table 1. The solutions presented in this CP have specific requirements for configuration, product selection, components, provisioning, authentication, key management, operations, administration, roles, and use and handling.

Table 1: Approved Commercial National Security Algorithm (CNSA) Suite for DAR

Security Service	CNSA Suite Standards	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197
Authentication (Digital Signature)	Elliptic Curve Digital Signature Algorithm over the curve P-384 with SHA-384	FIPS PUB 186-4
	RSA 3072 (Minimum)	FIPS PUB 186-4
Integrity (Hashing)	SHA-384, SHA-512	FIPS PUB 180-4
Can protect	Up to Top Secret	---------

NSA will initiate a transition to quantum resistant algorithms in the not too distant future. NSA customers using layered commercial solutions to protect classified national security information with a long intelligence life should begin implementing a layer of quantum resistant protection. Such protection may be implemented today through the use of large symmetric keys coupled with specific secure protocol standards. For more information please go to https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm.

4.5 Authentication

In this CP, each layer is required to have a "known secret" (e.g., PIN, password, or passphrase), smartcard, or Universal Serial Bus (USB) token to authenticate to each of the two encryption layers. The permitted factors may differ based on the layer. DAR encryption products must meet requirements for each of these factors during evaluation against the applicable protection profile (PP). These are considered primary (validated) authentication factors for that component.

Many products offer alternate authentication mechanisms. When implementing the DAR solution, these alternate mechanisms may be used only as a secondary (non-validated) authentication factor and

must be paired with a primary authentication factor. Secondary factors may act as an additional access control or may contribute to the product's key chain; the product's protection profile evaluation guarantees there is no loss in strength when combining keys with potentially weaker sources. A layer may use any number of authentication factors as long as one is a primary factor listed in that component's specific authentication requirement. As an example, layer one may use a known secret (primary factor) along with a biometric (secondary factor), and layer two may use a smartcard. It is important to consider the requirements, benefits, and drawbacks associated with different authentication factors. Some considerations of popular factors are discussed below.

Known secrets are memorized values that can provide a strong authentication value if well chosen (see Appendix A) and are typically supported by almost all products. They are at risk of being forgotten, as well as being seen while being keyed into the device. The majority of the time, known secrets will be weaker than tokens and are at risk of being very weak if not properly chosen. Appendix D specifies how to properly leverage known secrets in this CP.

Smartcard tokens are small integrated circuit devices that can store authentication keys. As long as they are handled and stored properly, they provide a very strong form of authentication. They provide a flexible option for authenticating a user to many devices and providing additional security through the use of a PIN to use the card. Aside from the benefits, cards are susceptible to loss and damage. In addition, they may also require a separate system for provisioning and recovery. This CP specifies handling and key size requirements for smartcards.

USB tokens are a simple form of token that provides a very strong form of authentication as long as they are handled and stored properly. Although very easy to provision, they generally have no additional security features, unless the USB device itself provides those features. Unfortunately, they are not permitted in many places. This CP specifies handling and key size requirements for USB tokens.

Biometric technology functions by taking a measurement of an element of the user's body. Common examples are fingerprints, iris scans, and facial recognition. This measurement is compared against a template that is created during provisioning; if the measurement matches the template, the user is authenticated. The vendor may use this authentication as an access control or may release a key to contribute to decryption. If a key is used, it will be important to ask how that key is protected and what authorizes the key's release, as there are currently no methods being used to derive a biometric measurement into a key. When using biometrics there may be instances when unauthorized users will be authenticated to the biometric when they should not; this is called a false acceptance, and is a condition with which all biometrics have to contend. Customers should obtain vendors' False Acceptance Rates (FAR) and determine how comprehensive their testing was to determine that rate. The other rate to address is the False Rejection Rate (FRR), which is when an authorized user's measurements fail to authenticate. This is a usability concern and should also be discussed with the vendor. The biometric template used to compare measurements is intended to be constructed so that the user's measurements are not reversible. If an adversary was able to obtain the template, they would be unable to reconstruct the user's fingerprint. However, this is not always the case; templates are not well standardized and there have been cases of reconstruction. This may be a risk to the privacy of users. The customer should ensure the vendor takes proper care to store the template information. One of the major risks of biometric is spoofing. This involves using other technology to recreate the user's measurement. Examples of spoofing include taking photos of the user's face or lifting

fingerprints. The vendor should explain how they mitigate spoofing, and users should protect the area being used to authenticate. Many biometrics need a fallback mechanism in case the area being used to authenticate to the biometric system becomes damaged, such as a finger being cut. Consideration should be given to what the fallback mechanism is or the consequences if there is none. As biometrics are not permitted to be used as a primary factor, a customer may use them for additional security in a multifactor authentication solution or as a lock screen mechanism.

Near Field Communication (NFC) is a short range signal. Generally, the devices are placed adjacently or in contact to exchange information in this method. This signal can vary in how it is used during the authentication process. There may or may not be an exchange of key material. The details of what is exchanged needs to be discussed with the vendor. Regardless of what is exchanged, the devices should be kept apart and treated like a Smartcard or USB token. NFC may not be permitted if the solution must also comply with other CPs that do not permit it.

Behavior based authentication covers a wide variety of features. The goal is to determine if an authorized user has the device, based on whether the device is being used and handled the way the authorized user normally uses the device. Based on this information the device may release a key, provide an access control, or allow for a longer time before locking the device. Factors that are taken into account include, location, connected networks, gyroscope measurements, user interaction, and other internal sensors. These features can be included in a solution to better ensure the device returns to a secure power state. The customer should take the time to understand the features provided by the solution and configure them to mission need. These features may have settings that allow lighter authentication or longer on times, the customer should ensure that these settings do not conflict with the CP. This may include false negatives and positives depending on the factors that are leveraged, this should be taken into consideration to ensure mission needs are met.

Time-based one time passwords (TOTP) are a method of generating a pin that changes based on time based on a shared seed. It is defined in RFC 6238, which the product should align with. The seed is counted on a device the user holds and also counted on the device verifying input, and if they match upon input, the authentication succeeds. When adding a TOTP, verify the following:

- Seeds are 256 bits
- Seeds are randomly generated
- Seeds are unique per client
- Seeds use HMAC-SHA-2 to generate the current password
- Seeds are sufficiently encrypted and secured
- The output length is at least 6
- There is an anti-hammer mechanism, such as throttling failed attempts
- The time-step and time drift are configured as minimum size to meet mission needs
- All communications take place over a secured channel

HMAC-based one-time passwords (HOTP) are what TOTP are built upon and function in a similar way except that HOTP is event based, instead of time based. The event is typically pressing a

button on the token to move to the next entry. They are defined in RFC 4226, which the product should align with. When adding a TOTP, verify the following:

- Seeds are 256 bits
- Seeds are randomly generated
- Seeds are unique per client
- Seeds use HMAC-SHA-2 to generate the current password
- Seeds are sufficiently encrypted and secured
- The output length is at least 6
- There is an anti-hammer mechanism such as throttling failed attempts

The look ahead window is configured as minimum size to meet mission needs.

4.6 CONTINUOUS PHYSICAL CONTROL

Although the DAR solution can protect the confidentiality of data and render the EUD unclassified, it does not protect the integrity of an EUD outside the control of approved users. It is difficult to examine and determine whether or not a device has been tampered with; therefore, the EUD must remain in continuous physical control at all times. The NSA requires that implementing organizations define the circumstances in which an EUD that is part of the solution is considered outside of the continuous physical control of authorized users (i.e., "lost"). The AO will define “continuous physical control”, and this definition should align with the intended mission and threat environment for which the solution will be deployed. Each organization must also define the circumstances in which an EUD that is a part of its solution is to be considered recovered back into the continuous physical control of authorized users (i.e., "found").

This concept includes mechanisms for the Unattended Operations Use Case (described in Section 7.4). AO’s should have a variety of mechanisms to ensure control of the EUD is maintained via cameras, sensors, and other similar means. The exact means are out of scope of the DAR CP, but there should be a high degree of confidence that the EUD is not susceptible to unauthorized physical access.

This CP requires any lost device, once found, to be rigorously investigated and/or destroyed in order to mitigate threats to the integrity of the EUD and any connected systems, because upon being found, the device is considered not secure unless the device meets Lost and Found (LF) requirements that are indicated as “LF” in the Use Case column in the requirements table. AOs should consult the DAR CP Risk Assessment (RA) to help make an informed risk decision.

See Appendix F for additional requirements information and some examples of continuous physical control.

4.7 RED, GRAY, AND BLACK DATA

This CP uses the following terminology to describe the data types that compose a DAR solution. The terms Red, Gray, and Black identify the number of encryption layers applied to classified data for a specific EUD state.

Red data is unencrypted classified data being processed by the EUD. After a user successfully authenticates to the outer and inner layers of DAR encryption, the EUD is in a state of processing Red data.

Gray data contains classified information that has been encrypted once. After a user successfully authenticates to the outer layer of DAR encryption, but has not yet authenticated to the inner layer of encryption, the EUD is in a state of processing Gray data.

Black data contains classified information that has been encrypted twice. An EUD is considered black when the device is powered off and/or unauthenticated and the stored data has been encrypted with both the outer and inner layers of DAR encryption.

4.8 Cryptographic Erase (CE)

Cryptographic Erase (CE), is a method of sanitization in which an encryption key for the encrypted data is sanitized, making recovery of the decrypted data infeasible. In this CP, it is used to ensure clean re-provisioning, as an additional protection triggered by failed authentication, or as an emergency method of sanitizing the media, in the event proper destruction methods cannot be met (see DAR-EU-2 in Table 12).

4.9 Provisioning

Provisioning is the process through which EUDs are initialized before first use. During the provisioning process, the Security Administrator (SA) loads and configures the DAR components for the EUD. Provisioning is inherently an out-of-band process requiring physical access to the EUD. The DAR solution cannot be applied to an EUD that already has data stored on it.

EUD re-provisioning or reuse of DAR components is allowed as long as it is performed in accordance with this CP. If re-provisioning, the EUD must be at the same or higher classification level of the previous unencrypted data stored on the approved DAR solution. Prior to re-provisioning an EUD, old data should be removed via cryptographic erase or media zeroization, media zeroization is the full overwrite of the hard disk drives (HDD) disk. Re-provisioning EUD components from any non-CSfC solution is prohibited.

4.10 Secure File Deletion

When deleting files via normal means (i.e., deleting followed by emptying the recycle bin, shift + delete, etc.) from the computer, there is a possibility for residual data to remain on the underlying storage media for extended periods of time, recoverable by forensic techniques. While the DAR CP requires multiple layers of encryption and tries to mitigate user error, it is still possible for the device to be compromised; in that event, securely deleting files reduces the information available to the adversary. For these reasons, it is recommended to use applications to securely delete files.

Secure file deletion tools make use of more direct methods to mitigate the risk of data being recoverable. Since there is not currently a method of validation for providing secure file deletion, here are some recommendations for features to include when acquiring a secure file deletion product. When looking for a product to fulfill this purpose, the type of storage media must be considered. There are currently two primary storage drives used today, hard disk drives (HDD) and solid state drives (SSD). Flash USB drives fall into the same area as SSDs.

Normally when a file is deleted from a HDD, the reference to that file's content is removed. The majority of the data continues to reside on the disk, being treated as free space for new data to use. This makes the role of a third party product straightforward. It should claim to directly overwrite the file reference and file data with any value, as long as that value cannot contain sensitive data, such as the contents of random access memory (RAM). Products may provide options for performing multiple passes but this is not necessary, as a single pass provides sufficient security. However, if only multiple passes are supported, they will not cause any harm.

In order to understand the residual risk, it is important to understand the basics of the complications involved in erasing memory from a SSD. When a user deletes a file, the drive marks that area as free space, but will not actually overwrite the data. This is for performance reasons, the memory used by the SSD must be cleared before being written to again, which takes time. The drive works in conjunction with the operating system to perform this task in the background when the drive does not have more important tasks. Because of this, it is not possible for a third party file deletion tool to directly overwrite data. There is also an upside, as regular deletion can eventually result in a direct overwrite, unlike HDDs where the data can remain for long periods of time. Because of this, third party tools are not necessary, and files may be deleted via normal means. However, there are other factors that affect when the SSD drive's background overwrite process can take place. The restrictions below detail configurations which a user can exert control. There are other situations where a user cannot exert control, which has the potential to result in data residing on the SSD for an extended undefined period of time. This is acceptable since any residual data should be encrypted. If any of the restrictions below apply, some third party products may be able to overcome them. Otherwise, the product should issue commands that enable the SSD to clear memory as soon as possible.

- TRIM, the command issued to the SSD to clear space, may not be supported by the operating system. Most modern operating systems do support this command; check operating system documentation to ensure support for TRIM.
- The TRIM command may only be supported by the OS if certain file systems are being used. Check vendor documentation to ensure a compatible file system is used.
- The way this is checked varies between operating systems. Check operating system documentation on how to verify TRIM is enabled.
- Older SSDs may not support the TRIM command. The majority of modern drives do have support; check vendor documentation to ensure the device supports this command.
- The operating system may not support TRIM for external drives, USB flash drives, or other devices connected over USB, PCI E, M.2 and other interfaces. This is a common area where a third party product may provide additional benefit.
- The operating system may not support TRIM when a Redundant Array of Independent Disks (RAID) configuration is used.

DAR products that support encrypted volumes may interfere with the TRIM command for data within the volumes. Some products do enable TRIM to function within the encrypted volumes, check vendor documentation for verification.

4.11 DAR Location-based Services (DARLS)

Data-at-Rest (DAR) protection can include capabilities that restrict access and authorization to a device based on the EUD's location, through the use of location aware technology. In this CP, a customer has

the option of employing DAR location aware technology as an added feature to a DAR solution. This does not replace either of the two mandatory encryption layers required in a CSfC DAR solution, but is only used as a supplemental means of protection, for defense in depth. Currently, there are no PPs to validate this type of technology. Customers choosing to implement DAR location-based services, should consult with the vendor and ask about specific details concerning the mechanisms and methodologies used in their product.

DARLS provides for precise geolocation of DAR devices using methods such as, Wi-Fi Positioning System (WPS), Global Positioning System (GPS), and Radio Frequency Identification (RFID). WPS achieves precision geolocation using a layered approach and may provide more accurate and reliable geolocation for DAR systems that operate within a building, whereas GPS may be effective in outdoor locations. The precision geolocation of a DAR device configured for a DAR location service is a precursor to successfully managing a variety of unattended secure DAR storage operations through the location aware storage domain. These storage operations include:

- Storage function isolation to minimize possibility of interference
- Reliable location determination within wireless environments (e.g., IEEE 802.11ax standards)
- Location driven DAR operation that can operate within defined fixed boundaries
- Secure domain within a building driven by security policy

DARLS provides an added layer of assurance to DAR mobility by enabling administrators to track and control the location and movement of DAR devices within the confines of a building or enclave. This is achieved by creating policies for individual devices depending on one or more of the following mobility related parameters:

- Physical location - Maintain continual device location status and confirm that uninterrupted physical control (as defined by the AO) is in effect
- Network connectivity - Provide validation of device presence within approved spaces for pre-boot and decryption on authorized networks
- Time-based operation - Revoke keys and initiate full-disk erase if the device remains outside of approved spaces beyond an authorized time
- Encryption enforcement - Initiate a power down, or a key revocation, or full-disk erase to enforce DAR encryption when a device has been removed from approved spaces or considered compromised

When a device exceeds or violates any of the mobility related parameters, the location-based service executes appropriate measures to ensure that the integrity and security of data stored in the device are maintained. These measures can include key revocation, crypto erase, device power down, etc.

A heartbeat may be used to determine an active connection from an approved location. This may check for a variable amount of time, covering frequent checks to ensure the device remains on campus, or infrequent connections in cases where a device is taken off campus and is good to be checked out for a specific amount of time.

4.12 KEY INGESTION

Key ingestion, also known as, key loading, is permitted for Full Drive Encryption components. In this case the data encryption key is generated externally and provided to the product. This is different from the enterprise key management use case, in which an enterprise server provides the key remotely. In this case, additional requirements must apply to ensure the key is properly generated and handled.

4.13 DAR VIRTUAL EUDS

Virtualization, containerization, and security separation kernel technology are becoming more prevalent. It can also serve as a replacement in case that the SWaP (Size, Weight, and Power) limitations of the other solutions do not suffice.

Virtual EUDs typically involve a hypervisor or other virtualization technology. Details involve encrypting the entire EUD twice, with the inner layer encrypting the Red Data VM image, or with the inner layer deploying encryption on the Red Data VM. Only HWFDE or SWFDE solutions are suitable for the outer layer.

SWFDE/FE

For SF solution, either with the inner layer encrypting the Red Data VM image or the inner layer deployed on the Red Data VM, note that VM suspension is prohibited. The outer layer covers the hypervisor, all VMs, and all software subcomponents.

HWFDE/FE

For the HF solution, whether the inner layer is encrypting the Red Data VM image or the inner layer is deployed on the Red Data VM, VM suspension is prohibited. The outer layer covers the hypervisor, all VMs, and all software subcomponents.

HWFDE/SWFDE

For the HS solution, VM suspension is permitted if the outer layer of HWFDE is followed immediately by the inner layer of SWFDE encryption covering the hypervisor, all VMs, and all software subcomponents. However, if the inner layer is deployed on the Red Data VM, then VM suspension is prohibited.

HWFDE/HWFDE

For the HH solution, the inner layer of HWFDE immediately follows the outer layer of HWFDE. VM suspension is permitted.

SWFDE/SWFDE

S2 solution is intended for a specific virtualization use case in which the outer layer encrypts the hypervisor, and the inner layer is deployed on the Red Data VM.

For the S2 solution, in which the inner layer is deployed on the Red Data VM, VM suspension is prohibited. The outer layer covers the hypervisor, all VMs, and all software subcomponents.

See Section 6.6 for more.

5 SOLUTION COMPONENTS

This section describes the capabilities of each component. Section 6 describes the possible functional implementations of each component within the possible Solution Designs and summarizes them in Table 2.

5.1 SOFTWARE FULL DISK ENCRYPTION (SWFDE)

Software Full Disk Encryption (SWFDE), shown in Figure 1, is used to provide one layer (either the inner or outer layer depending on the solution implemented) of DAR protection. The National Institute of Standards and Technology (NIST) Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices,* defines full disk encryption as follows: "Full Disk Encryption (FDE), also known as whole disk encryption, is the process of encrypting all the data on the drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the FDE product." A user must log into the Pre-Boot Environment (PBE) with valid credentials. Once the user is authenticated to the PBE, the SWFDE decrypts and boots the OS.

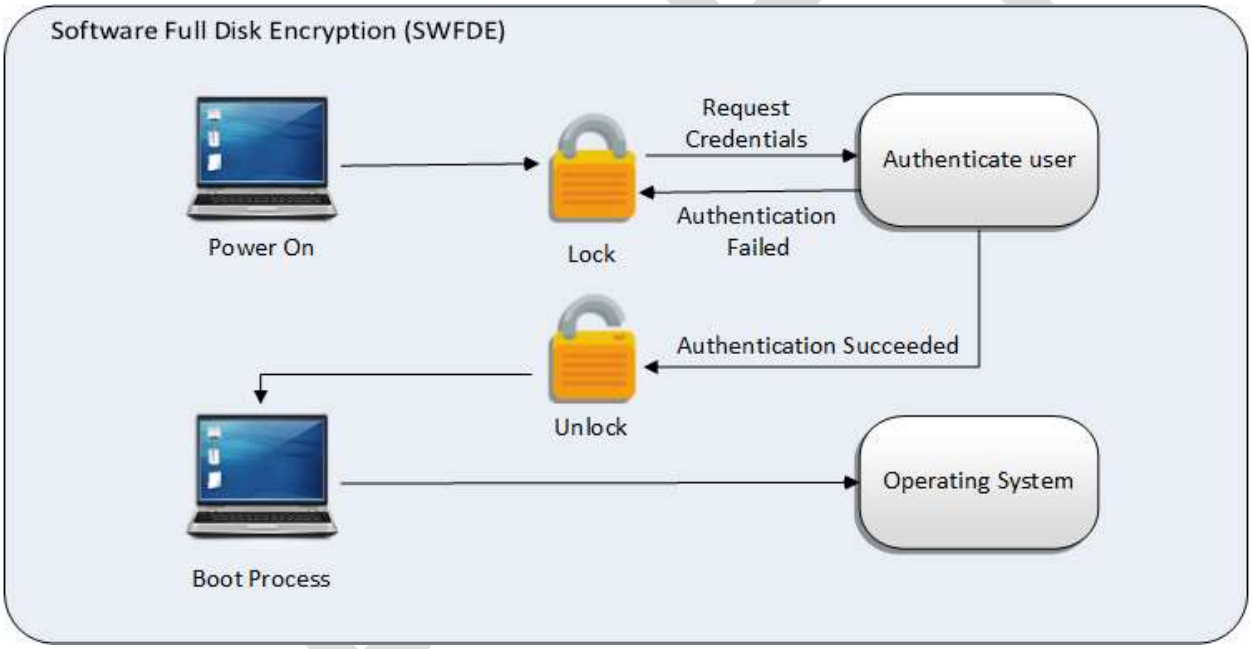


Figure 1: Software Full Disk Encryption

5.2 FILE ENCRYPTION (FE)

File Encryption (FE), shown in Figure 2, is approved to provide the inner layer of DAR protection. FE is the process of encrypting individual files or sets of files on an EUD and permitting access to the encrypted data only after proper authentication is provided.

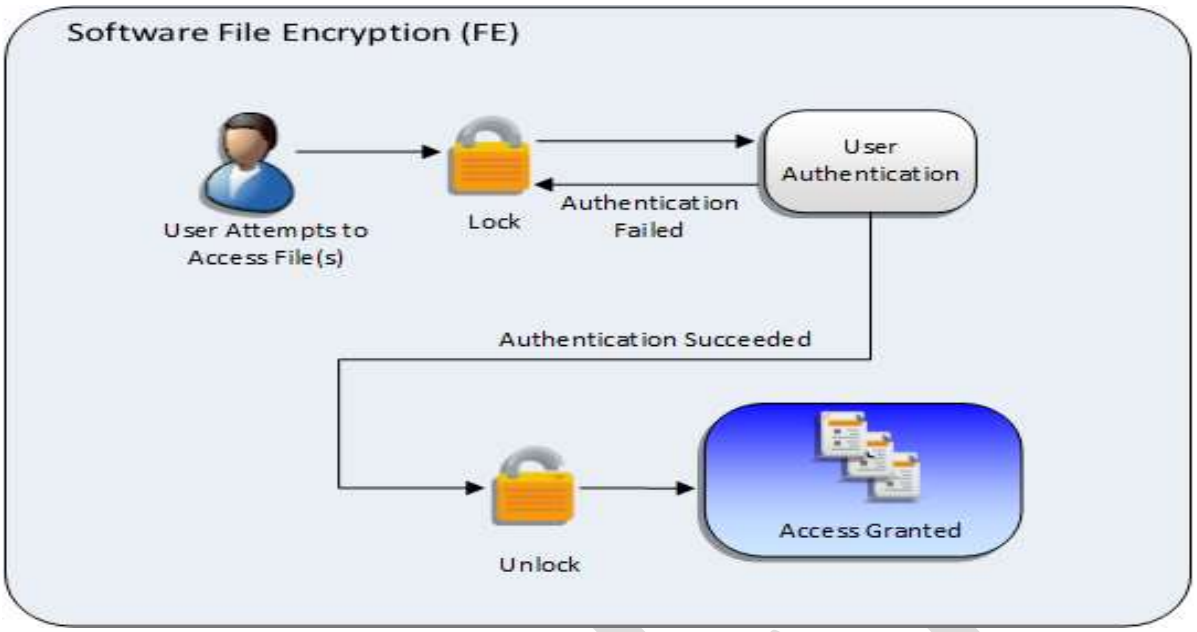


Figure 2: Software File Encryption

FE products currently on the market have a wide range of implementations. It is important for the user to understand how a specific FE product operates to ensure all classified data on the EUD is encrypted. There are many events and applications that may write data to the disk. Users should be made aware of these through user training, unless the FE product can encrypt the data without their intervention. Some examples of such events include:

1. Applications permitted to run on the EUD should be carefully considered. Applications may create files (e.g., temporary files) in unprotected locations leaving classified data at risk. If an application (e.g., file viewer) will be interacting with sensitive data and is not protected by an FE component, that application must be evaluated against the Application Software Protection Profile (ASPP) and meet the selection "not store any sensitive data" in FDP_DAR_EXT.1.1.
2. Paging files (e.g., swap files) are created when the system runs out of or becomes low on unused volatile memory, also known as RAM. When this occurs, the system may write to the non-volatile memory (e.g., hard disk) for storage. If the product cannot automatically protect this data, the solution should disable system page files.
3. Systems restore, and other features that allow data to be restored to a previous point in time create copies of the data. If this is enabled, it may allow an encrypted file to be restored to a state before it was encrypted. Unless the product accounts for these types of scenarios, these features should be disabled.
4. Memory dump files may be created when an error occurs. Memory dump files may include classified data that existed in volatile memory when the crash occurred. Since these files are created during a system crash, it is likely the product will not be able to properly encrypt them. Therefore, it is recommended this feature be used with care by individuals who understand what data will be contained within the file, or the feature should be disabled.

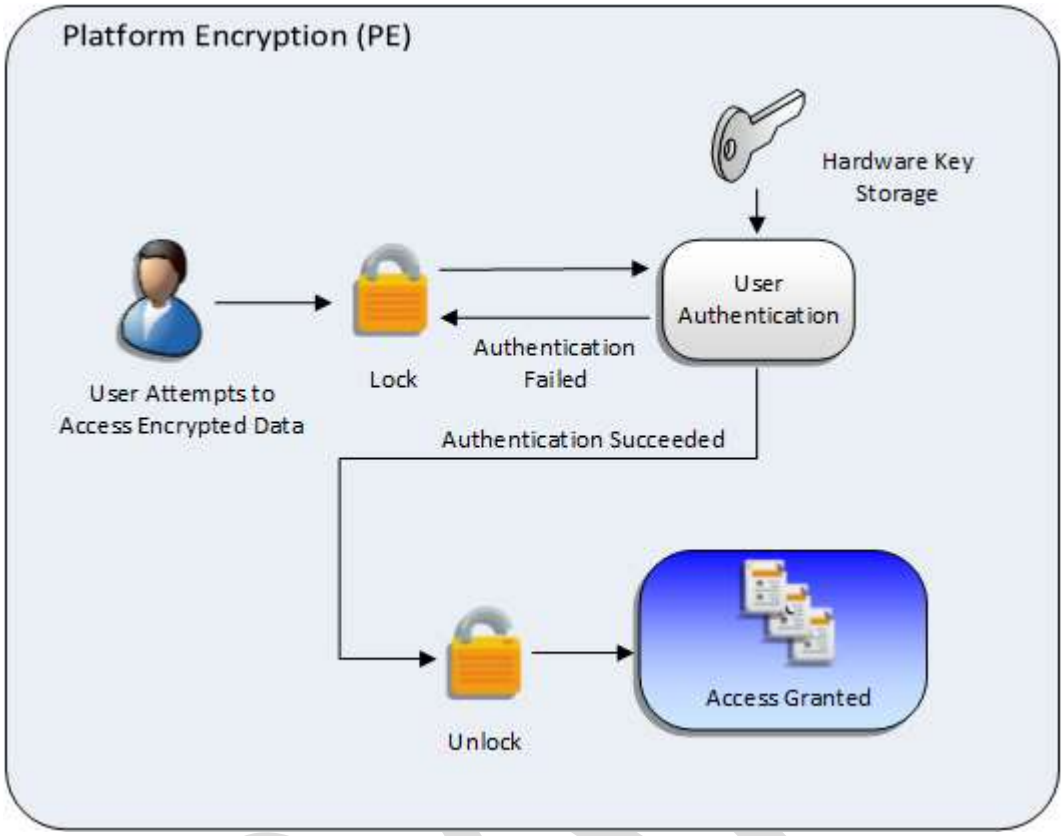
5. Printer spool files are created when a document is sent to print. These are used to hold documents while they are in queue for printing. If the solution is going to print any classified information, these files should be protected.
6. Moving or deleting files: users should be informed that moving (cut/paste) a classified file into a protected area is not sufficient for protecting it. Moving or deleting a file while it is unencrypted may leave file contents on the disk until it is overwritten by the file system. This should apply to all file movement for good practice, even though it would not apply in all cases. All files should be encrypted before being deleted or moved.

FE protects the confidentiality of individual files, folders, or volumes, and may be accomplished in several ways. The encryption may be performed by an application, platform, or the host OS. Each encrypted file, folder, or volume will be protected by a File Encryption Key (FEK). The FEK is protected by the user's authentication factor, either directly or through one or more Key Encryption Keys (KEKs).

Proper user authentication is required to decrypt the FEK. The FE product will then decrypt files or folders on an individual basis as they are requested by the user via specific applications. To ensure that no classified data is left unprotected, the AO must be responsible for providing and enforcing a policy that mandates automation and user compliance to encrypt all classified data.

5.3 Platform Encryption (PE)

Platform Encryption (PE), shown in Figure 3, is approved to provide the outer layer of DAR protection. PE is provided by the OS for platform-wide data encryption, transparently encrypting sensitive user data. The PE layer requires hardware-backed secure key storage, with the goal of reducing the need for long and complex passwords. With the exception of the hardware-specific requirements and which layer they can be used for (PE protects the outer layer while FE protects the inner layer), there is little distinction between PE and FE implementations. In all other respects, the two component implementations are virtually identical; they both provide volume and FE capabilities.



514

515 **Figure 3: Platform Encryption**

516 The PE component relies on the EUD to implement the requirements specified in the Mobile Device
517 Fundamentals (MDF) PP, along with the CSfC selected requirements. Items that meet the NIST
518 requirements for PE solutions are located in the CSfC Components List under "End User Device/Mobile
519 Platform."

520 5.4 HARDWARE FULL DISK ENCRYPTION (HWFDE)

521 Hardware Full Disk Encryption (HWFDE), shown in Figure 4, can be used to provide the inner or outer
522 layer of DAR protection. HWFDE is commonly implemented via a Self-Encrypting Drive (SED). The SED
523 can be a standard hard drive or a solid state drive.

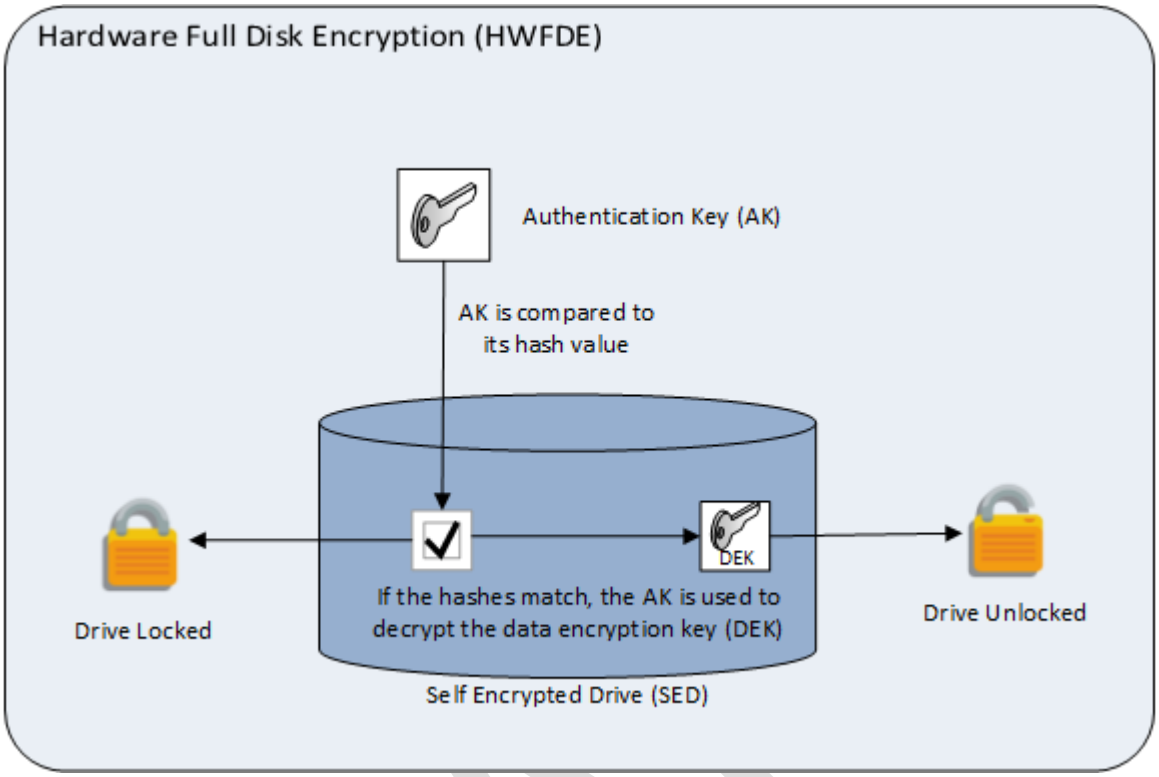


Figure 4: Hardware Full Disk Encryption

An SED contains hardware built into the drive controller chip that automatically encrypts all data written to the drive and decrypts all data read from the drive. The encryption and decryption is done transparently to the user.

In some cases, the HWFDE solution will require multiple components to create an FDE solution. Some SEDs require a product from an Independent Software Vendor (ISV) to function; this ISV commonly fills the role of collecting initial authentication and passing it to the SED. It is essential that both parts of the solution are chosen from the CSfC Components List.

The Authentication Key (AK) used in HWFDEs to encrypt or decrypt data is called the Data Encryption Key (DEK), which is protected by a chain of keys originating from the authentication factor.

A user must log into the PBE, provided by the SED or an ISV, with valid credentials. Once the user is authenticated to the PBE, the HWFDE decrypts and boots the operating system.

When discussing the use of ISVs and SEDs, the relevant information is sometimes referred to as FDE Authorization Acquisition (AA) & Encryption Engine (EE) breakout information.

5.5 End User Device (EUD)

The EUD is either: a personal computer (e.g., desktop, laptop); consumer device (e.g., smart phone, tablet); removable media (e.g., USB, CD); or a server (e.g., storage area network, network attached storage, shared drives, external storage). It is important to keep the security of different power states in mind when using these devices, referenced in Section 4.3.1. An EUD may operate within a secure

physical environment, outside of a secure physical environment, or both inside and outside of a secure physical environment as approved by the AO.

The drives that make up a Storage Area Network (SAN) or a Network Attached Storage (NAS) can be protected via the solutions presented in this CP, but that protection is provided only when the system is powered off. For powered on scenarios, consult the Mobile Access or Campus Wireless Local Area Network (WLAN) CPs on the CSfC web site.

Note as part of the solution, Multifactor must be used in compliance with Executive Order 14028: Improving the Nation's Cybersecurity. This Capability Package will be adding specific implementation language in future versions aligned with validated options which are in the process of being added to the relevant Protection Profiles.

5.6 DAR Enterprise Server (ES) and Mission Control Elements (MCE)

The DAR Enterprise Server (ES) and Mission Control Elements (MCE) are assumed to be in protected environments unless they are being treated as an EUD. Reference to the DAR ES should be distinct and separate from the DAR EUD server. In this CP, the DAR Enterprise Server may be referred to as the DAR ES or DAR EM Server, different from the DAR "EUD". The DAR ES provides functions such as account recovery, remote erase, network required authentication, and other similar functions for many endpoint EUDs. The server may integrate with services provided by the operating system to manage accounts.

The MCE acts as a system or set of systems that manage or access remote unattended EUDs, such as drones or unattended sites. In this situation, it is important to have mechanisms in place to ensure continuous physical control of the EUD is maintained, as described in Section 4.6. This solution does not need an ES, just remote access over a secure channel as described in the requirement.

6 SOLUTION DESIGNS

The CP provides the multiple solution designs listed in Figure 2. The designs describe solutions meeting a wide variety of requirements to protect classified DAR.

The "SF" design consists of SWFDE and FE. The SF architecture is typically intended for EUDs such as servers, desktops, laptops, and tablets.

The "PF" design consists of PE and FE. The PF architecture is typically intended for EUDs such as laptops, tablets, and smart phones.

The "HF" design consists of HWFDE and FE. The HF architecture is typically intended for EUDs such as servers, desktops, laptops, and tablets.

The "HS" design consists of HWFDE and SWFDE. The HS architecture is typically intended for EUDs such as servers, desktops, laptops, and tablets.

The "HH" solution design consists of two independent HWFDE layers. The HH architecture is typically intended for EUDs such as servers, desktops, laptops, and tablets.

The "S2" solution design consists of two independent SWFDE layers. The S2 architecture is typically intended for virtual EUDs such as servers, desktops, or laptops that use a hypervisor or other

virtualization technology that may employ an array of virtual machines including the Red Data VM, Inner Encryption Component VM, Outer Encryption Component VM, and Black Transport Component VM.

Table 2: Solution Design Summary

Solution Design	Designator	Description
SWFDE/FE	SF	DAR solution design that uses FE as the inner layer and SWFDE as the outer layer, as described in Section 6.1.
PE/FE	PF	DAR solution design that uses FE as the inner layer and PE as the outer layer, as described in Section 6.2.
HWFDE/FE	HF	DAR solution design that uses FE as the inner layer and HWFDE as the outer layer, as described in Section 6.3.
HWFDE/SWFDE	HS	DAR solution design that uses SWFDE as the inner layer and HWFDE as the outer layer, as described in Section 6.4.
HWFDE/HWFDE	HH	DAR solution design that uses HWFDE as the inner layer and HWFDE as the outer layer, as described in Section 6.5.
SWFDE/SWFDE	S2	DAR solution design that uses SWFDE as the outer layer and SWFDE as the inner layer, as described in Section 6.6.

Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible, solution owners must implement the Threshold version of the requirement instead.

6.1 SWFDE/FE (SF) Solution Design

The SWFDE/FE (SF) solution design requires SWFDE and file/folder/volume encryption. In the SF solution design, SWFDE will be used to provide DAR protection for the outer layer, and FE will be used to provide DAR protection for the inner layer. The SF DAR solution uses a password, passphrase, smartcard, or USB token to provide access to classified data. Once a user inputs the correct password, passphrase, smartcard token, or USB token, the system boots the operating system. Next, the user authenticates to the FE, which in turn decrypts the user's classified files.

Each layer of encryption in the SF DAR solution may use similar authentication mechanism types (e.g., passwords, passphrases, or tokens) but requires a unique authentication credential for each layer. For the first layer of encryption, the user will authenticate to the PBE provided by the SWFDE. For the second layer, the user will use their OS login credentials, application credentials, or file-specific credentials to authenticate to the FE.

Note: This SWFDE/FE solution can also work with virtualization. See Section 4.13 for more.

6.2 PE/FE (PF) Solution Design

The PE/FE (PF) solution design permits platform encryption, that allows for a device to perform DAR encryption via various implementations, all of which encrypt all sensitive data transparently. In the PF solution design, PE will be used to provide DAR protection for the outer layer, and FE will be used to provide DAR protection for the inner layer. The PF solution uses passwords to provide access to classified data. Once a user inputs the correct password, the platform is decrypted, which then provides access to user data. Next, the user authenticates to the FE, which in turn decrypts the user's classified files.

Each layer of encryption in the PF DAR solution may use similar authentication mechanism types (e.g., passwords) but requires a unique authentication credential for each layer. For the first layer of encryption, the user will authenticate to the device's encryption. For the second layer, the user will use their application credentials or file-specific credentials to authenticate to the FE.

6.3 HWFDE/FE (HF) Solution Design

The HWFDE/FE (HF) solution design requires hardware full disk encryption and file/folder/volume encryption. In the HF solution design, HWFDE will be used to provide DAR protection for the outer layer, and FE will be used to provide DAR protection for the inner layer. The HF DAR solution uses a password, passphrase, smartcard, or USB token to provide access to classified data. Once a user inputs the correct password, passphrase, smartcard, or USB token, the system boots the operating system. Next, the user authenticates to the FE, which in turn decrypts the user's classified file.

Each layer of encryption in the HF DAR solution may use similar authentication mechanism types (e.g., passwords, passphrases, smartcard, or USB token) but requires a unique authentication credential for each layer. For the first layer of encryption the user will authenticate to the PBE provided by the HWFDE. For the second layer the user will use their OS login credentials, application credentials, or file-specific credentials to authenticate to the FE.

Note: This HWFDE/FE solution can also work with virtualization. See Section 4.13 for more.

6.4 HWFDE/SWFDE (HS) Solution Design

The HWFDE/SWFDE (HS) solution design approach requires hardware full disk encryption and software full disk encryption. In the HS solution design, HWFDE will be used to provide DAR protection for the outer layer, and SWFDE will be used to provide DAR protection for the inner layer. The HS DAR solution uses a password, passphrase, smartcard or USB token to provide access to classified data. Once a user inputs the correct password, passphrase, smartcard or USB token value to the outer layer HWFDE, the inner layer SWFDE prompts the user to enter a password, passphrase, smartcard, or USB token in the PBE. Once the user authenticates to the SWFDE, the OS is loaded, and the user has access to data on the drive.

Each layer of encryption in the HS DAR solution may use similar authentication mechanism types (e.g., passwords, passphrases, or tokens) but requires a unique authentication credential for each layer. For each layer of encryption the user will authenticate to a PBE provided by the HWFDE and SWFDE, respectively.

Note: This HWFDE/FE solution can also work with virtualization. See Section 4.13 for more.

6.5 HWFDE/HWFDE (HH) Solution Design

The HWFDE/HWFDE (HH) solution design requires hardware full disk encryption. In the HH solution design, HWFDE will be used to provide DAR protection for both the inner and outer layers. The HWFDEs used to provide DAR protection for both the inner and outer layers must meet DAR-PS-3 vendor diversity requirements. The HWFDE DAR solution uses a password, passphrase, smartcard, or USB token to provide access to classified data. Once a user inputs the correct password, passphrase, smartcard, or USB token value of the outer layer HWFDE, and then the inner layer HWFDE, the operating system is loaded and the user has access to the data on the drive. This solution design is not common, and is specifically built for the purpose of providing dual hardware layers. An example of this solution design could be a self-encrypting drive paired with an inline encryptor.

Each layer of encryption in the HH DAR solution design may use similar authentication mechanism types (e.g., password, passphrases, or tokens) but requires a unique authentication credential for each layer. For each layer of encryption, the user will authenticate to a PBE, provided by each HWFDE layer.

Note: This HWFDE/HWFDE solution can also work with virtualization. See Section 4.13 for more.

6.6 SWFDE/SWFDE (S2) Solution Design

The SWFDE/SWFDE (S2) solution design is intended for a specific virtualization use case, in which the outer layer SWFDE will provide encryption entirely encompassing the hypervisor, and inner layer SWFDE is deployed on one virtual machine, the Red Data VM storing sensitive data, in order to ensure that sensitive data is always doubly encrypted. VM suspension is prohibited, to prevent sensitive data storage outside of the two layers of protection.

See section 4.13 for other Virtual EUD options.

7 DAR USE CASES

This CP provides multiple use cases that can be leveraged using a combination of the five solution designs. When a specific use case is followed, the customer must implement all Threshold requirements, where the applicable use case is listed in the “Use Case” column of requirements tables, as well as the applicable Solution Design, listed in the “Solution Design” column. For multiple use cases, separate registrations must be submitted with applicable requirements for each use case. These use cases are listed and described in Table 3.

The “LF” Use Case provides extra protections to permit occasional brief events, where continuous physical control of the solution is absent due to the EUD being considered lost, thereby, requiring specific Lost and Found requirements. This use case allows a device to be used when the lost EUD is found.

The “RM” Use Case is employed on removable media such as USB drives, microSD cards, and removable drives for the purpose of secondary storage, or to physically move data to and from systems.

The “UO” Use Case is employed when DAR systems and devices are managed remotely, such as a one-to-one relationship via an NSA approved Data-In-Transit (DIT) communication channel. These systems or

devices may be unmanned and/or unattended, but enforce protections that are considered to be in continuous physical control, as defined by the AO.

The “EM” Use Case is employed in an enterprise environment for managing multiple devices from one centralized management server, then pushed down to individual client devices. Solution components are managed by the DAR ES, through a client-server architecture.

The "GA" Use Case is a generally applicable use case that can be largely applied to a requirement. When listed as “GA”, the requirement is applied in a standard standalone use case. GA use case is for users not implementing one of the other specific use cases.

Table 3: Use Case Summary

Use Case	Designator	Description
Lost and Found	LF	DAR use case that implements HS, HF, HH, and PF when the device or system is out of continuous physical control, as defined by the AO. Described in Section 7.1
Removable Media	RM	DAR use case that implements the SF, HF, HH, or HS solution designs as described in Section 7.2.
Enterprise Management	EM	DAR use case that implements enterprise managed solutions to manage multiple clients, implemented through the SF, HF, HH, and HS solution designs, as described in Section 7.3.
Unattended Operations	UO	DAR use case for managing unattended or remote managed DAR solutions and systems that implements HS, HF, HH, or SF, as described in Section 7.4.
Generally Applicable	GA	DAR use case that is generally applicable to a standalone use case and corresponding solution design.

7.1 Lost and Found (LF) Use Case

The Lost and Found (LF) Use Case is when a user, intentionally or unintentionally, temporarily loses control of a device (as defined by the AO) and plans to continue using it after it is recovered. This use case adjusts the continuous physical control requirements from Section 4.6 and permits the device to be used after it is found; however if the device is suspected to have been tampered with, it must be rigorously investigated and/or destroyed. Note that as of *DAR CP v5.0*, this use case no longer has its own section of requirements, instead it leverages the use case column in the requirements tables.

This use case is intended to cover situations including but not limited to: devices left in vehicles or devices forgotten in hotels for short periods of time, going through customs when traveling, and similar events. These requirements lower the risk of using devices that have been in such conditions, but they do not eliminate the risk. With this in mind, AOs should consider additional local policy to reduce the situations where devices may be vulnerable to tampering.

This use case also contains a requirement to personalize the EUD. The intent of the personalization requirement is to ensure that if an adversary removed the EUD and replaced it with another EUD of the same make and model, it would be noticed by the end user. Personalization includes: adding stickers, changing the screen’s background, etc. The administrator may also change settings to personalize the devices for subsets of users, such as a login screen wallpaper. None of these changes should undermine

any security features of the device or other relevant security policy (i.e., requiring the device to be rooted).

All of the requirements indicating "LF" in the "Use Case" column of the requirements table must be met in order to implement the Lost and Found use case. This is a high risk use case and requires a number of additional requirements to lower the risk. Note that the Lost and Found use case is optional. If it is not implemented, then the device cannot be reused if it is lost. The SF solution is not allowed for the Lost and Found use case. As explained in Section 7.2**,** the LF use case is also prohibited when using removable media for DAR protection.

7.2 Removable Media (RM) Use Case

The Removable Media (RM) use case shown in Figure 5, depicts two layers of encryption employed on the removable media device/form factor. This use case allows customers to use an external storage device between different systems to protect DAR and has different password requirements. In the RM use case, DAR protection is required for the outer layer and the inner layer, provided through the SF, HF, HH, or HS solution designs. When using the RM use case, choose from the SF, HF, HH, or HS solution designs. Requirements of the SF, HF, HH, or HS solution design should be followed with this use case. For example, if the HF solution design is chosen, both HF and RM designated requirements are applicable.

In this CP, removable media is defined as device(s) that have the primary purpose of providing external storage of data protected by DAR through implementing two layers of encryption. Removable media can include: a USB drive, a CD, a microSD card, or a removable drive. Removable media does not include other portable computing devices such as smartphones and tablets. This use case allows customers to transfer data using an external storage device between different systems or expand the storage of a single system. For example, this use case can be used to transport data via a removable media device between secured facilities, using a DAR CP compliant solution with appropriate CP components to enable decryption of the RM. This requires using two approved layers of encryption on the RM device that is provisioned within a secured facility, then transporting the RM under continuous physical control to access data on another secure workstation or device. If a solution includes both DAR host machines and a separate DAR RM device, the customer must submit separate registrations.

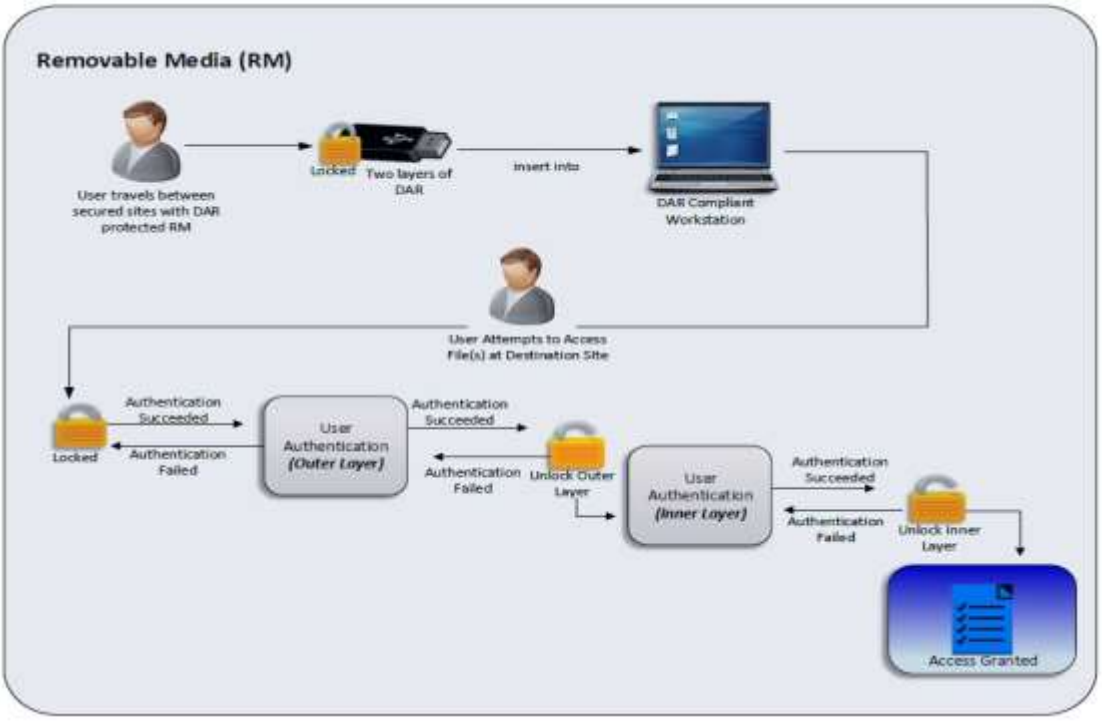


Figure 5: Removable Media Use Case

The PF solution design cannot be employed on removable media because there are several incompatibilities between their requirements. The PE layer is used only as the outer layer and requires hardware-backed secure key storage, with the goal of reducing the need for long and complex passwords. Each layer of encryption in the PF DAR solution may use similar authentication mechanism types (e.g., passwords), but requires a unique authentication credential for each layer.

The RM use case only protects endpoints as stated in this CP or in a secured facility. The LF use case is prohibited when using removable media for DAR protection. If the removable media is lost, and out of continuous physical control, users must report it to their Information Systems Security Officer (ISSO) or chain of command, as defined by the AO. The removable media is considered compromised once lost and cannot be re-used if later found. Lost and Found requirements do not guarantee or protect the integrity of the removable media once lost and out of continuous physical control.

7.3 Enterprise Management (EM) Use Case

The Enterprise Management (EM) Use Case shown in Figure 6, depicts a client-server architecture for managing a DAR enterprise solution. The figure shows the DAR EM use case using a CSfC approved DIT CP as the secure communication channel. The figure assumes that the DAR client has already been initially provisioned by an administrator. Figure 6 is one example of how the EM use case could be depicted; however, there may be other cases where the illustration would be different, such as the order of operations specific to when the user logs on versus when the DIT tunnels are established, or several other factors that are specific to the customer implementation, further explained below.

Authentication for this use case may occur in various ways. Connecting to the network to complete the authentication may or may not be required. One or both layers may have a DAR ES managing them.

The DIT solution may be CSfC or an approved High Assurance GOTS solution. If both DAR layers are enterprise managed, both servers may either exist on the Red Network or one will exist on the Gray/Red boundary while the other exists in the Red. If network access is not required for DAR authentication, or only for the inner DAR layer, allowing the OS to boot before requiring authentication to network, then connection and access to the EM server can be established as normal, as described in the relevant DIT CPs. If an enterprise managed layer requires authentication with network access before the OS can boot, then the tunnel must be established first by a pre-boot capability of the product, a network device, an approved High Assurance GOTS solution, or endpoint virtualization.

In order for the client to communicate with the server, and the server communicate with the client, there must be a secure communication link to and from the front and back end. This must be done through use of one of the DIT CPs, or an approved High Assurance GOTS link. Each implementation is required to use and comply with the latest version of the Mobile Access (MA) CP, Multi-Site Connectivity (MSC) CP, or Campus Wireless Local Area Network (WLAN) CP for applicable network and configuration requirements for establishing and setting up a secure connection that will allow the client and server to communicate. When implementing the EM use case, customers must have an existing approved DIT CP registration with the CSfC PMO, or submit a new DIT CP registration for approval.

The DAR EM server can perform, but is not limited to: sending keys, pushing updates to the EUD, pushing policy and configuration changes to the EUD, and so on. The EM use case allows customers to transfer the administrative overhead to one centralized management server, enforcing policies and configuration changes that are pushed to individual DAR client devices.

For specific details on key management of the EM solution, such as how keys will be transmitted, received, revoked, etc., refer to the requirements and details specified in the products' Protection Profile (PP). Vendors are required to meet and comply with key management requirements found in the Protection Profiles. For additional details, please refer to the "Protection Profile Module for File Encryption Enterprise Management" and the "collaborative Protection Profile Module for Full Drive Encryption – Enterprise Management." There may be additional standards leveraged for the management of keys beyond the security requirements defined by the PPs, such as Key Management Interoperability Protocol (KMIP); this is expected and per component guidance, should be followed for proper setup.

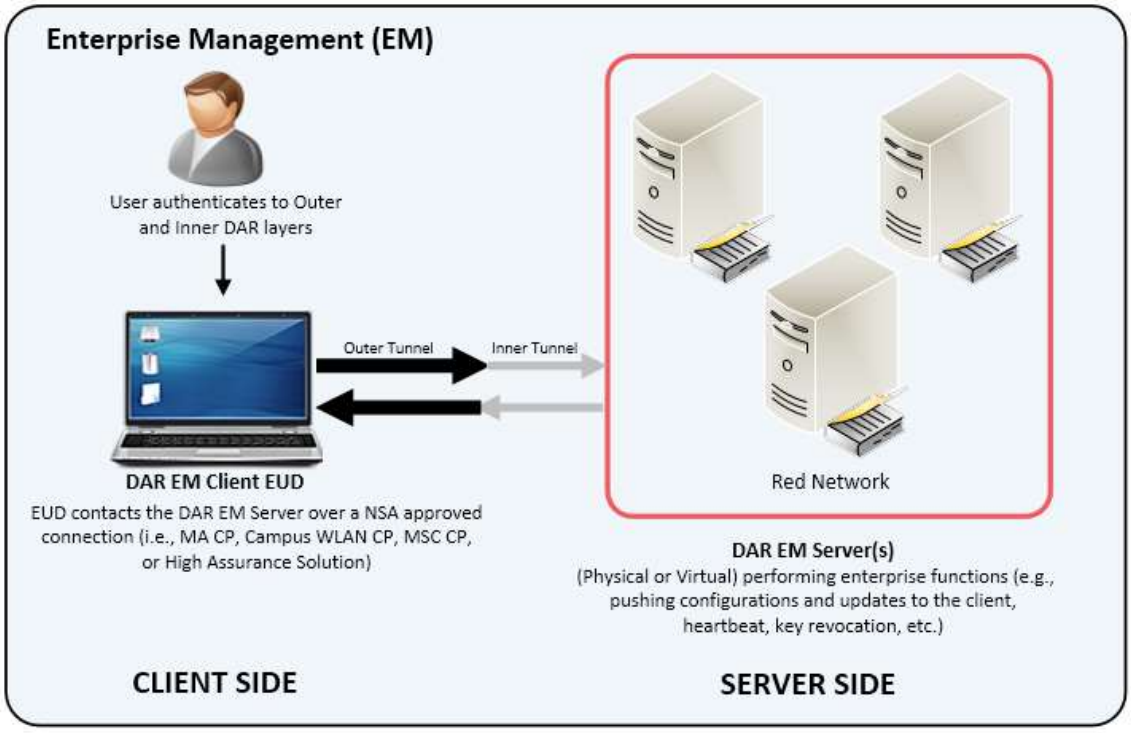


Figure 6: Enterprise Management Use Case

7.3.1 Enterprise Management via MA CP, MSC CP, or Campus WLAN CP

For implementation of a DAR EM solution via a CSfC DiT CP, the user must reference the latest DIT CPs to access the appropriate network diagrams, and requirements for setting up a secure channel for the DAR EM link from the client to server. As mentioned, the solution must be registered and approved by the CSfC PMO in order to use, in combination with the DAR EM use case.

The customer has multiple options for setting up the DAR EM solution on the Red Network. In cases where the EM servers for both layers are at the solution boundary, they may be contained in the same physical box and virtually separated. The solution boundaries are described in the corresponding CPs; the terms "after" and "before" are in reference to moving towards the Red Network.

For integration with the MA CP, there are three implementations:

MA Option 1: The location of both the EM servers is after the solution boundary of the inner layer. Integration with the MA CP will only provide limited support for EM functionality, as MA trusted channels must be connected before additional EM functionality is provided, which requires a network connection. This may render certain DAR EM products incompatible.

MA Option 2: The location of one of the EM servers is after the solution boundary of the inner layer. The location of the second EM server is before the solution boundary of the inner layer, with only the outer layer established. This EM server is its own Red enclave, with the second layer of protection provided by the trusted channel established by the ES itself. This setup will also only provide limited support for EM functionality, as one of the ES's will require both MA trusted channels to be connected before additional

EM functionality is provided, which requires a network connection. This may render certain DAR EM products incompatible.

MA Option 3: consists of enterprise managing one layer, either: after the Inner Solution boundary or before it in a separate red enclave, and the second layer managed locally.

For integration with the MA CP where one of the servers is before the Inner Solution boundary, the server must follow guidance found in the MA CP, referencing the protection of Inner TLS-Protected Servers and Clients. With this option, the DAR ES(s) must be placed between the Gray Firewall and Inner Firewall. As referenced in MA CP, Inner TLS-Protected servers must be managed from the Red administration workstation. DAR ES(s) products listed on the CSfC Component's List provide communication channels through secure protocols (e.g., TLS). Product specific functionality and assurance requirements for the DAR Enterprise Management server can be found in the applicable PP, which CSfC component vendors are required to meet to be on the list.

For integration with the WLAN CP, the DAR ES must be placed after the Inner Solution boundary. Integration with the WLAN CP will only provide limited support for EM functionality, as WLAN trusted channels must be connected before additional EM functionality is provided, which requires a network connection. This may render certain DAR EM products incompatible.

For integration with the MSC CP, the DAR ES must be placed after the Inner Solution boundary. As network devices establish the trusted channels and not the client, full EM functionality is available.

For further details as it pertains to configurations, placement, and requirements for protection of DAR ES servers on the Red Network or on the Inner Solution boundary, within a CP architecture, please reference the applicable CP sections and requirements.

7.3.2 Enterprise Management via High Assurance GOTS solution

For implementation of a DAR EM solution via a High Assurance GOTS solution, the High Assurance GOTS link will serve as the approved secure channel, therefore replacing the DiT two tunnel requirement. Reference Section 4.1 for Implementing a CSfC in a High Assurance GOTS Environment. The AO will be responsible to ensure all CSfC transmitted data is appropriately protected by the High Assurance GOTS link. As with the MSC CP, full EM functionality should be available.

7.3.3 Enterprise Management Key Recovery

EM products may provide support for recovery of credentials; these features may only be used if included in the product's evaluations per DAR-CR-10. Two general methods may be supported by DAR EM products, they are challenge response and PIN recovery.

Challenge response operates by providing some known information to be verified by the EM server, at which point the server returns a value to allow decryption. If the value is generated by the product at provisioning, it must be stored securely. The product may prompt the user to provide the initial value; if so, it must be generated according to the password rules and then stored securely. It may be generated on the server for non-electronic distribution of recovery; if this is the case, a method of verifying the user must be established. Any delivery of recovery credentials must be performed over a secure channel.

The second method is PIN recovery. In this case, the recovery PIN will be populated on the server for each endpoint. This method will require a means of verifying the user, and a method for the delivery of recovery credentials, which must be performed over a secure channel.

7.4 Unattended Operations (UO) Use Case

The Unattended Operations (UO) Use Case shown in Figure 7 is intended for customers operating DAR solutions that may be unattended and remotely managed, mostly represented as a one-to-one relationship. This use case differs from the EM use case, in that EM is intended for managing many devices from a central management server, represented in more of a corporate enterprise environment. Figure 7 shows an MCE managing a dual CSfC DAR solution over a validated High Assurance GOTS link or through an approved CSfC DIT solution. This use case allows customers to operate DAR solutions that in nature, are more uncommon and considered unique scenarios. The UO use case must conform to the cybersecurity requirements prescribed by CNSSP No. 28 for Unmanned National Security Systems.

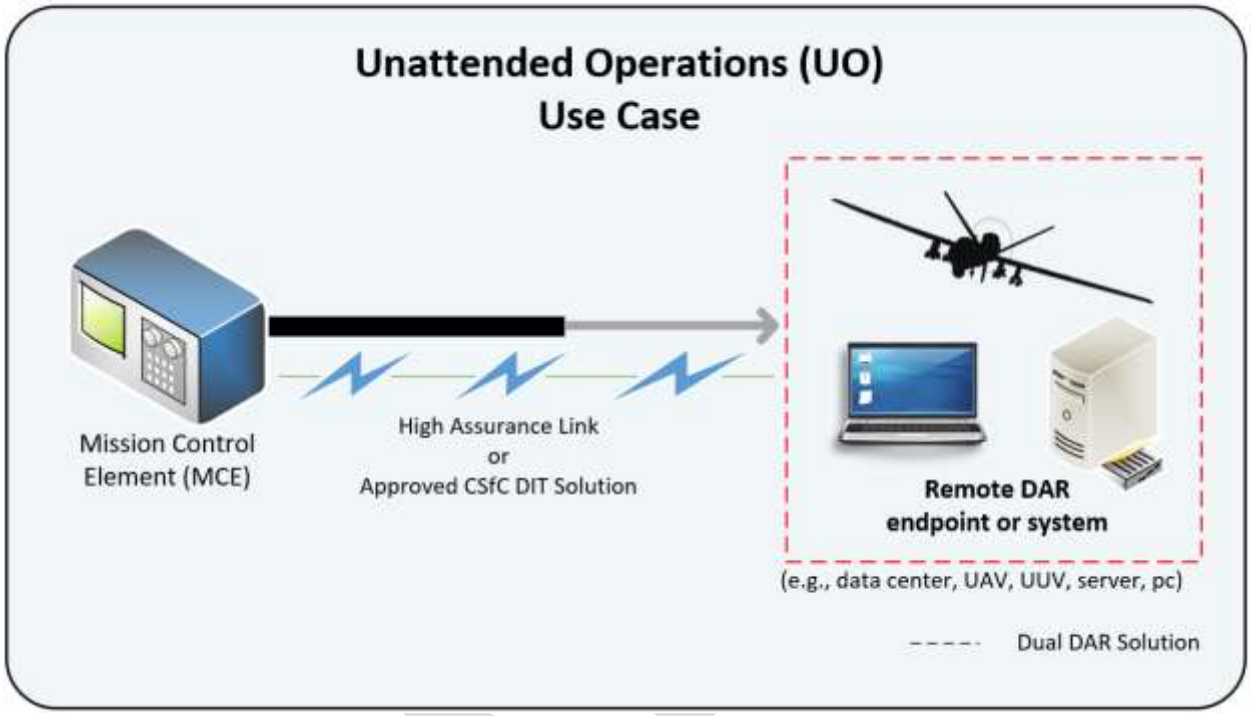
In the UO use case, continuous physical control is defined by the AO, as an acceptable definition that ensures adequate protection of the device(s) and/or system(s), and data residing there. Methods should be defined to ensure the device is protected from unauthorized access and ensuring mechanisms that will put the solution into a secure power state if such unauthorized access is detected.

The UO use case can be defined, but not limited to, an EUD in an unattended environment managed by an MCE or other secure operational capability. This use case is managed over a remote connection, but may be accessed locally to perform various functions. If remote power up or power down is required, a High Assurance GOTS link may be required. The authentication process must follow the methods defined in the requirements and should be performed via the MCE. If direct authentication of the EUD is required, it must be within a secure location and physical token must be removed afterwards. UO examples include, but are not limited to protection of data centers, overrun scenarios, and unmanned vehicles or systems (e.g., UAV, UUV). The dual DAR solution is managed by an MCE, base station, or similar solution.

When using the UO use case, some form of anti-tamper and detection capability (passive or active) is required that enables the detection of possible adversarial compromise when the solution is remotely managed without direct physical presence. These methods can include measures for monitoring and detecting, such as cameras, sensors, etc.

Note: For clarification in this Use Case, the terms “Unattended” and “Unmanned” are defined as:

- Unattended – Solutions that are remotely managed and are capable of being fully or partially unattended
- Unmanned – Solutions that are remotely managed and are incapable of being manned because of location or application (e.g., UAV, UUV)



881

882 **Figure 7: Unattended Operations Use Case**

883 # 8 CONFIGURATION REQUIREMENTS

884 Sections 8 through 12 specify requirements for implementations of the five solutions, and five use cases
885 compliant with this CP. Only one use case and one design may be selected, with the exception that EM
886 may be paired with LF. The tables of requirements in the following sections have a column that specifies
887 which solution designs and use cases the requirement applies to, and uses the following nomenclature:

888 • SF design: DAR solution components include SWFDE and FE

889 • PF design: DAR solution components include PE and FE

890 • HF design: DAR solution components include HWFDE and FE

891 • HS design: DAR solution components include HWFDE and SWFDE

892 • HH design: DAR solution components include HWFDE and HWFDE

893 • LF use case: DAR solution designs include PF, HF, HH, or HS

894 • RM use case: DAR solution designs include SF, HF, HH, or HS

895 • UO use case: DAR solution designs include SF, HF, HH or, HS

896 • EM use case: DAR solution designs include SF, HF, HH, or HS

- GA use case: DAR solution design include SF, PF, HF, HH, and HS

The CP includes two categories of requirements:

- An Objective (O) requirement specifies a feature or function that is desired or expected but may not currently be available. Organizations should implement objective requirements in lieu of corresponding Threshold requirements where feasible.

- A Threshold (T) requirement specifies a minimum acceptable feature or function that still provides the mandated capabilities if the corresponding objective requirement cannot reasonably be met (i.e., due to system maturity). A solution implementation must satisfy all applicable Threshold requirements, or their corresponding Objective requirements, in order to comply with this CP.

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 this CP. 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 this CP. Objective requirements without corresponding Threshold requirements are marked as "Optional" in the "Alternative" column, but improve upon the overall security of the solution and should be implemented where feasible.

In order to comply with this CP, a solution must, at minimum, implement all Threshold requirements associated with each of the solution designs and use cases it supports and should implement the Objective requirements associated with those solution designs and use cases where feasible. For example, a DAR solution using a SWFDE and FE must implement only those Threshold requirements applicable to the SF design. Additionally, the customer must implement Threshold requirements applicable to the chosen DAR solution use case (e.g., RM, UO, EM, LF, or GA).

The customer may treat the device as classified; however, if they do so, they must adhere to the policies and requirements for classified devices (note that those requirements exceed the requirements contained within the DAR CP).

Each requirement defined in this CP has a unique identifier digraph that groups related requirements together (e.g., KM), and a sequence number (e.g., 2). Table 4 lists the digraphs used to group together related requirements, and identifies where they can be found in the following sections.

Table 4: Requirement Digraphs

Digraph	Description	Section(s)	Table(s)
PS	Product Selection Requirements	Section 9	Table 5
SR	Overall Solution Requirements	Section 10.1	Table 6
CR	Configuration Requirements for All DAR Components	Section 10.2	Table 7

Digraph	Description	Section(s)	Table(s)
SW	SWFDE Component Requirements	Section 10.3	Table 8
FE	FE Component Requirements	Section 10.4	Table 9
PE	PE Component Requirements	Section 10.5	Table 10
HW	HWFDE Component Requirements	Section 10.6	Table 11
EU	EUD Requirements	Section 10.7	Table 12
CM	Configuration Change Detection Requirements	Section 10.8	Table 13
DM	Device Management Requirements	Section 10.9	Table 14
AU	Auditing Requirements	Section 10.10	Table 15
KM	Key Management Requirements for All DAR Components	Section 10.11	Table 16
SC	Supply Chain Risk Management Requirements	Section 10.12	Table 17
GD	Use and Handling of Solution Requirements	Section 11.1	Table 18
RP	Incident Reporting Requirements	Section 11.2	Table 19
TR	Testing Requirements	Section 13.1	Table 20

9 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are provided for maximizing the independence of components within the solution. This will increase the level of effort required to compromise this solution.

Table 5: Product Selection Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold /Objective	Alternative
DAR-PS-1	The products used for the FE layer must be chosen from the list of FE products on the CSfC Components List.	HF, SF, PF	EM, GA, LF, RM, UO	T=O	
DAR-PS-2	The products used for the SWFDE layer must be chosen from the list of SWFDEs on the CSfC Components List.	HS, SF, S2	EM, GA, LF, RM, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold /Objective	Alternative
DAR-PS-3	The Inner and Outer DAR layers must either: • Come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • Be different products from the same manufacturer, where NSA has determined that the products meet the CSfC Program's criteria for implementation independence.	HF, HS, SF, PF, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-PS-4	(Moved to DAR-SC-2)				
DAR-PS-5	The cryptographic libraries used by the Inner and Outer DAR layers must be independently developed and implemented.	HF, HS, SF, PF, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-PS-6	The products used for the PE layer must be chosen from the list of PE products on the CSfC Components List under the Mobile Platform section.	PF	GA, LF	T=O	
DAR-PS-7	The products used for the HWFDE layer must be chosen from the list of HWFDEs on the CSfC Components List.	HF, HS, HH	EM, GA, LF, RM, UO	T=O	
DAR-PS-8	The Operating System used must be approved by the General Purpose OS Protection Profile (OS PP).	HF, HS, SF, HH, S2	EM, GA, LF, UO	O	Optional
DAR-PS-9	The products used for the Enterprise Management Server must be chosen from the list of DAR Enterprise Management Servers on the CSfC Components List.	HF, HS, HH, SF, S2	EM	T=O	

10 CONFIGURATION

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance on how to configure the components for a DAR solution.

10.1 Overall Solution Requirements

Table 6: Overall Solution Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-SR-1	Default accounts, passwords, community strings, and other default access control mechanisms for all components must be changed or removed.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-SR-2	The DAR solution must be properly configured according to local policy and U.S. Government guidance (e.g., NSA guidelines). In the event of conflict between the requirements in this CP and local policy, the CSfC PMO must be contacted.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-SR-3	Each DAR component must have a unique account for each user.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-SR-4	All EUDs must remain in continuous physical control at all times, as defined by the AO.	HF, HS, SF, PF, HH, S2	EM, GA, RM, UO	T=O	
DAR-SR-5	The AO must provide guidance when CE should be implemented.	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-SR-6	The AO must provide procedures for performing CE.	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-SR-7	At least one layer must use a trusted platform module for cryptographic key storage.	HF, HS, SF, HH, S2	EM, GA, UO	O	Optional
DAR-SR-8	*(Withdrawn)*				
DAR-SR-9	At least one layer must use a trusted platform module for cryptographic key storage.	HF, HS, SF, HH, S2	LF	T=O	

10.2 Configuration Requirements for All DAR Components

Table 7: Configuration Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-CR-1	Default encryption keys must be changed.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-CR-2	Primary user authentication credential values for each DAR layer mechanism type must be unique (e.g., the password for the 1st layer will not be the same as the password for the 2nd layer).	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CR-3	DAR components must use algorithms for encryption selected from Table 1.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CR-4	Each DAR component must prevent further authentication attempts after a number of failed attempts defined by the AO.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-CR-5	Each DAR layer must perform a CE after a number of consecutive failed logon attempts as defined by the AO.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-CR-6	Each DAR component must generate its own symmetric encryption keys on the EUD, receive keys generated by the Enterprise Management server, or ingest key.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CR-7	Each DAR component must permit only an administrator to disable or alter its security functions.	SF, HF, HS, PF, HH, S2	GA, LF, RM, UO	O	Optional
DAR-CR-8	All EUDs must have DAR protections enabled at all times after provisioning.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CR-9	All EUDs must encrypt all classified data. (Refer to Section 5.2 for additional information on FE.)	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CR-10	All components must be implemented (configured) using only their NIAP-approved configuration settings. Users may change settings that are not part of NIAP evaluation.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CR-11	Users must be restricted to designated user folders.	SF, HF	EM, GA, LF, RM, UO	T=O	
DAR-CR-12	For use in high threat environments (as defined by the AO) the two layers of DAR must use different primary authentication factors (i.e., Both layers cannot use passwords. One layer may use a password but the second layer	HF, HS, SF, HH, S2	EM, GA, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
	would then need to use a token or other factor).				
DAR-CR-13	For use in routine threat environments (as defined by the AO) the two layers of DAR must use different primary authentication factors (i.e., Both layers cannot use passwords. One layer may use a password but the second layer would then need to use a token or other factor).	HF, HS, SF, HH, S2	EM, GA, RM, UO	O	Optional
DAR-CR-14	At least one DAR layer must use multi-factor authentication.	HF, HS, SF, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-CR-15	The removable media must not be bootable.	HF, HS, SF, HH, S2	RM	T=O	
DAR-CR-16	The DAR Enterprise Server, must only manage one component/layer, and must not manage the other component/layer of the DAR solution.	HF, HS, HH, SF, S2	EM	T=O	
DAR-CR-17	All administrators must use unique identifiable accounts.	HF, HS, HH, SF, PF, S2	EM, GA, LF, RM, UO	T=O	
DAR-CR-18	A baseline configuration that complies with this CP must be enforced on all registered endpoints.	HF, HS, HH, SF, S2	EM	T=O	
DAR-CR-19	Enterprise management servers that leverage a SQL platform account management, must be configured according to the guidance of the platform and any additional configuration guidance provided by the component vendor.	HF, HS, HH, SF, S2	EM	T=O	
DAR-CR-20	The two layers of DAR must use different primary authentication factors (i.e., Both layers cannot use passwords. One layer may use a password but the second layer would then need to use a token or other factor).	HF, HS, HH, S2	LF	T=O	
DAR-CR-21	Each DAR component must permit only an administrator to disable or alter its security functions.	HF, HS, HH, SF, S2	EM	T=O	
DAR-CR-22	The administrator must configure	HF, HH,	EM	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
	remediation options (account lockout, key revocation, etc.) for failed authentication attempts by the user, as determined by the AO.	HS, SF, S2			
DAR-CR-23	The administrator must configure remediation options (account lockout, key revocation, etc.) for failed authentication attempts by the user, as determined by the AO.	HF, HH, HS, PF, SF, S2	GA, LF, RM, UO	O	Optional
DAR-CR-24	EUDs must require network access to complete the authentication process for decryption.	HF, HH, HS, SF, S2	EM	O	Optional
DAR-CR-25	EUDs that are lost or compromised must be revoked and issue zeroize commands.	HF, HH, HS, SF, S2	EM	T=O	
DAR-CR-26	If leveraging virtualization, the EUD must configure VM suspension according to Section 4.13.	HF, HH, HS, SF, S2	EM, GA, LF, UO	T=O	
DAR-CR-27	EUDs must be configured with a heartbeat function. Upon loss of the heartbeat, it will initiate an appropriate remediation action such as a shutdown, lock, or wipe.	HF, HH, HS, PF, SF, S2	GA	O	Optional
DAR-CR-28	EUDs must be configured so that if the EUD is seen at the exit point, or any area defined as a location boundary for the device, it will initiate an appropriate remediation action such as a shutdown, locking, or wiping.	HF, HH, HS, PF, SF, S2	GA	O	Optional
DAR-CR-29	An FDE that ingests an externally generated key must protect that key according the requirements of a USB or Smartcard authentication factor.	HF, HH, HS, SF, S2	EM, GA, LF, UO	T=O	
DAR-CR-30	An FDE that ingests an externally generated key must generate that key via the NSA provided key generation tool or via a type 1 product.	HF, HH, HS, SF, S2	EM, GA, LF, UO	T=O	
DAR-CR-31	An FDE that ingests an externally generated key must have included “accept a DEK that is generated by the RBG provided by the host platform” or	HF, HH, HS, SF, S2	EM, GA, LF, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
	"accept a DEK that is wrapped as specified in FCS_COP.1(d)" in its Security Target for the Full Drive Encryption collaborative Protection Profile.				
DAR-CR-32	Any component using AES-GCM must configure a 128 authentication tag.	HF, HH, HS, SF, S2, PF	GA	O	Optional

941 ## 10.3 SWFDE COMPONENT REQUIREMENTS

942 **Table 8: SWFDE Component Requirements**

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-SW-1	The SWFDE must use Cipher Block Chaining (CBC) for data encryption.	SF, HS, S2	EM, GA, LF, RM, UO	T	DAR-SW-2
DAR-SW-2	The SWFDE must use XEX-based tweaked-codebook mode with cipher text stealing (XTS) or Galois/Counter Mode (GCM) for data encryption.	SF, HS, S2	EM, GA, LF, RM, UO	O	DAR-SW-1
DAR-SW-3	The SWFDE must be configured to use one of the following primary authentication options: • A randomly generated passphrase or password that meets the minimum strength set in Appendix D, or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token, or • An external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1, or • Any combination of the above.	SF, HS, S2	EM, GA, LF, RM, UO	T=O	

10.4 FE Component Requirements

Table 9: FE Component Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-FE-1	The FE product must use CBC for data encryption.	SF, PF, HF	EM, GA, LF, RM, UO	T	DAR-FE-2
DAR-FE-2	The FE product must use XTS or GCM for data encryption.	SF, PF, HF	EM, GA, LF, RM, UO	O	DAR-FE-1
DAR-FE-3	The FE product must use one of the following primary authentication options: • A randomly generated passphrase or password that meets the minimum strength set in Appendix D, or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token, or • An external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1, or • Any combination of the above.	SF, PF, HF	EM, GA, LF, RM, UO	T=O	

10.5 PE Component Requirements

Table 10: PE Component Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-PE-1	The PE must enable the "wipe sensitive data" management function for imported or self-generated keys/secrets and/or other classified data.	PF	GA, LF	T=O	
DAR-PE-2	The PE must use CBC for data encryption.	PF	GA, LF	T	DAR-PE-3
DAR-PE-3	The PE must use XTS or GCM for data encryption.	PF	GA, LF	O	DAR-PE-2

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-PE-4	The AO must provide policy to the user determining when data or keys must be wiped.	PF	GA, LF	T=O	
DAR-PE-5	The PE product must use one of the following primary authentication options: A minimum of a randomly generated six-character, case-sensitive alphanumeric password with the length defined by the AO, or a randomly generated passphrase with the length defined by the AO.	PF	GA, LF	T=O	

10.6 HWFDE COMPONENT REQUIREMENTS

Table 11: HWFDE Component Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-HW-1	The HWFDE must use CBC for data encryption.	HF, HS, HH	EM, GA, LF, RM, UO	T	DAR-HW-2
DAR-HW-2	The HWFDE must use GCM or XTS for data encryption.	HF, HS, HH	EM, GA, LF, RM, UO	O	DAR-HW-1
DAR-HW-3	The HWFDE must be configured to use one of the following primary authentication options: • A randomly generated passphrase or password that meets the minimum strength set in Appendix D, or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token, or • An external smartcard or software capability containing a software certificate with RSA or ECC key pairs per Table 1, or • Any combination of the above.	HF, HS, HH	EM, GA, LF, RM, UO	T=O	

10.7 END USER DEVICES REQUIREMENTS

Table 12: End User Device Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-EU-1	All EUD provisioning must be performed through direct physical access or through an enterprise management server.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-2	If found after being lost, the EUD's non-volatile storage media must be destroyed per NSA/CSS Storage Device Sanitization (NSA/CSS Policy Manual 9-12). (This does not preclude having the device forensically analyzed by the appropriate authority.)	SF, PF, HF, HS, HH, S2	EM, GA, RM, UO	T=O	
DAR-EU-3	EUDs must implement the Basic Input/Output System (BIOS) security guidelines specified in NIST SP 800-147.	SF, PF, HF, HS, HH, S2	EM, GA, LF, UO	O	Optional
DAR-EU-4	All users must sign an organization-defined user agreement before being authorized to use an EUD.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-5	All users must receive an organization-developed training course for operating an EUD prior to use.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-EU-6	At a minimum, the organization-defined user agreement must include each of the following: • Consent to monitoring • Operational Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when, where, and under what conditions the EUD may be used • Responsibility for reporting security incidents • Verification of IA training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities • An overview of what constitutes continuous physical control and the risks associated with using the EUD after it is lost	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-7	External USB tokens and smartcards, when used for authentication, must be removed from the EUD upon or before shut down in accordance with AO policy.	SF, PF, HF, HS, HH, S2	EM, GA, LF, UO, RM	T=O	
DAR-EU-8	AO must provide guidance on storing and/or securing authentication factors.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-9	The SA must disable system power saving states on EUDs (i.e., sleep and hibernate).	SF, HF, HS, HH, S2	EM, GA, LF, UO	T=O	
DAR-EU-10	The EUD must power off after a period of inactivity defined by the AO, unless this is not supported by the device.	SF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-EU-11	The EUDs must be provisioned within a physical environment certified to protect the highest classification level of the data stored on the device.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-12	The EUD must only be re-provisioned to the same or higher classification level of the classified data per an AO approved process.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-13	The EUD must be reported as "lost" when out of continuous physical control as specified by the AO.	SF, PF, HF, HS, HH, S2	EM, GA, RM, UO	T=O	
DAR-EU-14	System folders must have user write permissions disabled unless authorized by an administrator.	SF, HF	EM, GA, LF, UO	T=O	
DAR-EU-15	The EUD must be protected with anti-tamper or detection capabilities.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM	O	Optional
DAR-EU-16	The device must be powered down before being handled by an unauthorized party (e.g., customs) and inspected afterwards. If the unauthorized party required the device to be powered on again for inspection, the device must be rebooted again before use.	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-17	The absence of any expected authentication prompt(s) must be reported as possible tampering to the AO.	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-18	When data is no longer needed, it must be overwritten or erased by secure erase tool per AO guidance. (See Section 4.10)	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-EU-19	The EUD, when not in use outside of a secured facility, must be kept in an AO-approved locked container.	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-EU-20	The BIOS/Unified Extensible Firmware Interface (UEFI) must be configured to require a password before continuing the boot process.	HF, HS, SF, HH, S2	EM, GA, LF, UO	O	Optional

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-EU-21	All DAR FDE components must be cryptographically erased before being provisioned again.	HF, HS, SF, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-22	All DAR components must be cryptographically erased before being provisioned again.	PF	GA, LF	O	Optional
DAR-EU-23	System folders must have user write permissions disabled, unless authorized by an administrator.	PF	GA, LF	O	Optional
DAR-EU-24	If supported, the EUD must have the BIOS/UEFI password enabled.	HF, HS, SF, HH, PF, S2	EM, GA, UO, LF	T=O	
DAR-EU-25	If the user suspects the EUD has been compromised, the EUD user must obtain authorization from their AO prior to use.	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-26	Each EUD must be personalized by the end user. (This should not violate any other security features.)	HF, HS, PF, SF, HH, S2	EM, GA, RM	O	Optional
DAR-EU-27	The EUD must not be used as a smart card/USB Authentication Token, if it is also storing encrypted user data.	HF, HS, SF, HH, S2	RM	T=O	
DAR-EU-28	The EUD must be removed from a host system before being handled by an unauthorized party (e.g., customs).	HF, HS, SF, HH, S2	RM	T=O	
DAR-EU-29	Administrators and endpoint users must be restricted from making configuration changes based on what the product supports, using a model of least privilege.	HF, HS, HH, PF, SF, S2	EM, GA, LF, RM, UO	T=O	
DAR-EU-30	The EUD must be reported as “compromised” when tampering is suspected, as defined by AO policy.	HH, HF, HS, PF, S2	LF	T=O	
DAR-EU-31	The EUD and/or non-volatile storage media, if compromised, must be destroyed per NSA/CSS Storage Device Sanitization (NSA/CSS Policy Manual 9-12). (This does not preclude having the device forensically analyzed by the appropriate authority.)	HH, HF, HS, PF, S2	LF	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-EU-32	Prior to reuse, the EUD must undergo tamper detection inspection as established by the AO to determine if the device has been tampered with or substituted.	HH, HF, HS, PF, S2	LF	T=O	
DAR-EU-33	The EUD, when outside of a secured facility and not in use, must be kept concealed from potential adversaries.	HH, HF, HS, PF, S2	LF	T=O	
DAR-EU-34	If an unauthorized party takes the EUD out of sight or performs unknown operations, the device must be considered compromised.	HH, HF, HS, PF, S2	LF	T=O	
DAR-EU-35	When using commercial modes of travel (e.g., non-secure), the EUD must stay with the traveler and not be placed in checked baggage.	HH, HF, HS, PF, S2	LF	T=O	
DAR-EU-36	Each EUD must be personalized by the end user. (This should not violate any other security features.)	HH, HF, HS, PF, S2	LF	T=O	
DAR-EU-37	EUDs must use boot integrity verification. (see Appendix A)	SF, HH, HF, HS, S2	EM, GA, UO, LF	T=O	
DAR-EU-38	EUDS must implement "DAR Location based Services" features and restrict decryption of data to only approved locations.	SF, HF, HS, PF, HH, S2	EM, GA, LF, UO	O	Optional
DAR-EU-39	The EUD must be protected with anti-tamper or detection capabilities.	SF, PF, HF, HS, HH, S2	UO	T=O	

10.8 Configuration Change Detection Requirements

Table 13: Configuration Change Detection Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-CM-1	A history of baseline configuration for all components must be maintained by the SA.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CM-2	An automated process must ensure configuration changes are logged.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-CM-3	Log messages generated for configuration changes must include the specific changes made to the configuration.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-CM-4	A history of baseline configuration for all components must be available to the auditor.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-CM-5	Configuration change logs must be kept for an AO defined period of time.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	

10.9 Device Management Requirements

Table 14: Device Management Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-DM-1	EUDs must be physically administered.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T	DAR-DM-2
DAR-DM-2	EUDs must be remotely administered using an NSA-approved Data-In-Transit (DIT) protection solution (e.g., NSA Certified Product or CSfC approved solution).	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	DAR-DM-1
DAR-DM-3	Administration workstations must be dedicated for the purposes given in the CP.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-DM-4	Administration workstations must physically reside within a protected facility where CSfC solution(s) are managed.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-DM-5	Administration workstations must be physically separated from workstations used to manage non-CSfC solutions.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-DM-6	Only authorized SAs (See Section 12) must be allowed to administer the DAR Components.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-DM-7	EUDs must be remotely administered, but local administration may still be performed.	SF, HF, HS, HH, S2	EM, UO	T=O	

10.10 AUDITING REQUIREMENTS

Table 15: Auditing Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-AU-1	EUDs must be inspected for malicious physical changes in accordance with AO defined policy.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-AU-2	The EUDs must be configured to generate an audit record of the following events: • Start-up and shutdown of any platform audit functions • All administrative actions affecting the DAR encryption components • User authentication attempts and success/failure of the attempts • Software updates to the DAR encryption components	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-AU-3	Auditors must review audit logs for a time period as defined by the AO.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-AU-4	Auditors must physically account for the EUDs after an AO-defined time period.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-AU-5	Administrators must periodically compare solution component configurations to a trusted baseline configuration after an AO-defined time period.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-AU-6	For DAR EM products that support auditing functions, audit records must be generated and recorded for: • Encryption status of endpoints • Recovery attempts and success/failure of the attempts • Out of date endpoint versions • Platform changes • Registration of new endpoints • Revocations of endpoints • Key escrow from endpoints • Cryptographic erase of endpoints • Changes to administrator account • Changes to policies pushed to endpoints	HF, HS, HH, SF, S2	EM	T=O	

10.11 KEY MANAGEMENT REQUIREMENTS

Table 16: Key Management Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-KM-1	The key sizes used for each layer must be as specified in Table 1.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-KM-2	DAR solution products must be initially keyed within a physical environment certified to protect the highest classification level of the DAR solution.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-KM-3	The DAR solution must disable all key recovery mechanisms.	SF, PF, HF, HS, HH, S2	GA, LF, RM, UO	T=O	
DAR-KM-4	The algorithms used for each layer must be as specified in Table 1.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-KM-5	If a physical recovery output is used, it must be secured as classified information, equivalent to the level of data it is protecting.	SF, HF, HS, HH, S2	EM	T=O	
DAR-KM-6	If recovery information is distributed over a non-CSfC channel (i.e.,	SF, HF, HS, HH, S2	EM	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
	physically, voice channel, etc.), it must be secured as classified information, equivalent to the level of data it is protecting.				
DAR-KM-7	The AO must determine a methodology for verification of end users requesting recover material, whether recovery information is distributed over a channel not provided by the CSfC solution (i.e., physically, voice channel, etc.) or distribution by a CSfC solution component which is expected to provide verification itself.	SF, HF, HS, HH, S2	EM	T=O	

959

960 ## 10.12 Supply Chain Risk Management Requirements

961 **Table 17: Supply Chain Risk Management Requirements**

962

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-SC-1	CSfC Trusted Integrators must be employed to architect, design, procure, integrate, test, document, field, and support the solution.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-SC-2	Each component selected from the CSfC Components List must go through a Product Supply Chain Risk Management (SCRM) Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product SCRM process. (See Committee on National Security System Directive (CNSSD) 505 SCRM for additional guidance.)	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-SC-3	Each layer that contains a TPM must provide a Platform Certificate and a corresponding CA certificate chain. The Platform Certificate must be compliant with the latest version of the TCG Platform Certificate Profile specification and the TCG PC Client Firmware Integrity Measurement (FIM) specification.	SF, PF, HF, HS, HH, S2	SF, PF, HF, HS, HH	O	Optional
DAR-SC-4	Each layer that contains UEFI firmware must provide a Reference Integrity Manifest (RIM) Bundle and a corresponding CA certificate chain. For products that are compliant with the UEFI specification, the platform certificate must be stored on the device in compliance with the TCG specifications. The RIM bundle should be compliant with the latest version of the TCG PC Client RIM specification and the PC Client Firmware Integrity Measurement (FIM) specification. The RIM must be stored on the device in compliance with the TCG specifications.	SF, PF, HF, HS, HH, S2	SF, PF, HF, HS, HH	O	Optional

*__NOTE__: Artifacts defined by the Trusted Computing Group (TCG) can be used to provide supply chain integrity checks and attestation of firmware. For a DAR component, the TCG Platform Certificate and Reference Integrity Manifest (RIM) can be used as part of an acceptance test. (Refer to NIST publication 1800-34 “Validating the Integrity of Computing Devices” for guidance on how to use TCG artifacts when performing an acceptance test.)
https://www.nccoe,nist.gov/publications/practice-guide/validating-integrity-computing-devices-nist-1800-34-practice-guide

11 SOLUTION OPERATION, MAINTENANCE, & HANDLING REQUIREMENTS

11.1 USE AND HANDLING OF SOLUTION REQUIREMENTS

The following requirements must be followed regarding the use and handling of the solution.

Table 18: Use and Handling of Solutions Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-GD-1	Acquisition and procurement documentation must not include information about how the equipment will be used, including that it will be used to protect classified information.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-2	The solution owner must allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure that it meets the latest version of the CP.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-3	The AO must ensure that a compliance audit is conducted every year against the latest version of the DAR CP.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-4	Results of the compliance audit must be provided to and reviewed by the AO.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-5	When a new, approved version of the DAR CP is published, the AO must ensure compliance against this new CP within 6 months.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-6	Solution implementation information, which was provided to NSA during solution registration, must be updated every 12 (or fewer) months (see Section 13.3).	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-GD-7	The SA, auditor, user, and all Integrators must be cleared to the highest level of data protected by the DAR solution.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-8	The SA and auditor roles must be performed by different people.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-9	All SAs, users, and auditors must meet local information assurance training requirements.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-10	Users must report lost or stolen EUDs to their ISSO or chain of command as defined by the AO.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-11	Only SAs or CSfC Trusted Integrators must perform the installation and policy configuration.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-12	Security critical patches (such as Information Assurance Vulnerability Alerts (IAVAs)) must be tested and subsequently applied to all components in the solution in accordance with local policy and this CP.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-13	Local policy must dictate how the SA installs patches to solution components.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-14	All DAR components must be updated using digitally signed updates provided by the vendor.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-15	All authorized users must have the ability to CE keys for both layers.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	O	Optional
DAR-GD-16	When using an FE Product, the user must ensure that no classified data must be put into the file's metadata (e.g., filename).	SF, PF, HF	EM, GA, LF, RM, UO	T=O	
DAR-GD-17	Withdrawn				
DAR-GD-18	Withdrawn				

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-GD-19	AO must define loss of continuous physical control for each use case. This definition must cover the following topics: • User handling • EUD Transportation • EUD Storage • Anti-tamper mechanisms and related policies, if any are used. • Device integrity measures and related policies, if any are used.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-GD-20	Organizational-developed training must include guidance on tamper awareness and detection.	HH, HF, HS, PF, S2	LF	T=O	
DAR-GD-21	Organizational-developed training must include the following topics if they are included in the solution for both administrators and users: • Checking the encryption status of endpoints • Using the recovery mechanisms supported in the NIAP evaluated configuration • Checking for out of date endpoint versions • Detecting platform changes • The registration process for endpoints • The revocation process for endpoints • The key escrow process for endpoints • The cryptographic erase process for endpoints • The process for pushing policy changes to endpoints	SF, HF, HS, HH, S2	EM	T=O	

11.2 Incident Reporting Requirements

Table 19 lists requirements to report security incidents to NSA regarding incidents affecting the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that SAs and auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for Operations and Maintenance (O&M) will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary, but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Table 19 only provides requirements directly related to the incident reporting process. See Section 10.10 for requirements supporting detection of events that may reveal that a reportable incident has occurred.

Table 19: Incident Reporting Requirements

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-RP-1	Report a security failure in any of the CSfC DAR solution components.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-RP-2	Report any malicious configuration changes to the DAR components.	SF, PF, HF, HS, HH, S2	EM, GA, LF, UO, RM	T=O	
DAR-RP-3	Report any evidence of a compromise of classified data caused by a failure of the CSfC DAR solution. Compromise, in this context, includes reporting real or perceived access to classified data (e.g., user or administrator access that occurs without proper authentication or through the use of incorrect credentials).	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-RP-4	Report any evidence of malicious physical tampering (i.e., missing or misinstalled parts) with solution components.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-RP-5	Confirmed incidents meeting the criteria in DAR-RP-1 through DAR-RP-4 must be reported within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter.	SF, PF, HF, HS, HH, S2	EM, GA, LF, RM, UO	T=O	
DAR-RP-6	At a minimum, the organization must provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities Is Technical Support from NSA requested? (Yes/No)	SF, PF, HF, HS, HH, S2	GA, EM, LF, UO, RM	T=O	

12 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are detailed below, along with doctrinal requirements for these roles.

End User – An end user may operate an EUD from physical locations not owned, operated, or controlled by the Government. The end user must be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. End user duties include, but are not limited to the following:

1. Ensure that the EUD is only operated in physical spaces that comply with the end user agreement.

2. Alert the Security Administrator immediately upon an EUD being lost, stolen, or suspected of being tampered with.

Security Administrator – The SA must be responsible to maintain, monitor, and control all security functions for the entire suite of products composing the DAR solution. Security Administrator duties include, but are not limited to:

1. Ensure that the latest security critical software patches and updates (such as IAVAs) are applied to each product in a timely fashion
2. Document and report security-related incidents to the appropriate authorities
3. Coordinate and support product logistic support activities including integration and maintenance. Ensuring that the implemented DAR solution remains compliant with the latest version of the CP
4. Provision and maintain EUDs in accordance with this CP

Auditor - The auditor must be responsible to review the actions performed by the SA and events recorded in the audit logs to ensure that no action or event represents a compromise of the DAR solution. The role of auditor and SA must not be performed by the same individual. Auditor duties include but are not limited to:

1. Review, manage, control, and maintain security audit log data
2. Document and report security-related incidents to the appropriate authorities
3. Access all audit records

Integrator – Integrator duties may include but are not limited to:

1. Acquire the products that compose the solution
2. Configure the DAR solution in accordance with the CP
3. Test the DAR solution
4. Document the solution and its compliance to the CP
5. Troubleshoot the solution

In certain cases, an external integrator may be used to implement a DAR solution based on the CP. A CSfC Trusted Integrator is one such entity. Although not required, the use of CSfC Trusted Integrators is highly recommended. A CSfC Trusted Integrator is defined as a selected organization that has demonstrated competency in:

1. System integration
2. The technologies to be integrated

3. Formal testing processes
4. Generating evidence for system authorization

Chosen CSfC Trusted Integrator applicants are required to sign a Memorandum of Agreement (MoA) with NSA.

13 INFORMATION TO SUPPORT THE AO

This section details items that will likely be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:

- The customer, possibly with support from an Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a test plan and perform testing of the DAR solution, see Section 13.1.
- The customer has system assessment and authorization performed using the RA information referenced in Section 13.2.
- The customer provides the results from testing and from system assessment and authorization to the AO for use in making an approval decision. The AO is ultimately responsible to ensure that all requirements from the CP have been properly implemented. NSA publishes compliance matrices requiring a short description of how requirements are met. NSA recommends that the AO require the compliance matrix as part of their body of evidence.
- The customer registers the solution with NSA and re-registers annually to validate its continued use as detailed in Section 13.3. NSA publishes registration forms at: http://www.nsa.gov/resources/commercial-solutions-for-classified-program/solution-registration.
- Customers who want to use a variant of the solution detailed in this CP will contact NSA early in their design phase to determine ways to obtain NSA approval.
- The AO must ensure that a compliance audit is conducted annually against the latest version of the DAR CP, and the results must be provided to the AO.

13.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a DAR solution. This T&E is a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution must be tested. The following is a general, high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the DAR solution. The entire solution, to include each component described in Section 5, is addressed by this test plan.

1. Set up the baseline network design and configure all components.

2. Document the baseline network design configuration. Include product model and serial numbers, and software version numbers as a minimum.

3. Develop a test plan for the specific implementation using the test objectives from the DAR CP Testing Annex. Any additional requirements imposed by the local AO should also be tested, and the test plan must include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.

4. Perform testing using the test plan derived in Step 3. System testing will consist of both black box testing and gray box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution must be documented.

5. Compile findings, including comments and vulnerability details as well as possible countermeasure information, into a final test report to be delivered to the AO for their approval of the solution.

6. The testing requirement in Table 20 was developed to ensure that the DAR solution functions properly and meets the configuration requirements from Section 8. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 20: Test Requirement

Req #	Requirement Description	Solution Designs	Use Case	Threshold/ Objective	Alternative
DAR-TR-1	The organization implementing the CP must perform all tests listed in the DAR CP Testing Annex.	HF, HS, PF, SF, HH, S2	EM, GA, LF, RM, UO	T=O	

13.2 Risk Assessment

The DAR solution Risk Assessment (RA) presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/CSS Customer Advocate to request the RA, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the RA is available on the SIPRNet CSfC website. The AO must be provided a copy of the NSA RA for their consideration in approving the use of the solution.

13.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems (NSS) must register their solution with NSA prior to operational use. Customers will provide their compliance checklists and registration forms to NSA. This registration will allow NSA to track where DAR CP solutions are instantiated and to provide AOs at those sites with appropriate information, including all significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process, as well as the compliance matrices and

registration forms, are available at http://www.nsa.gov/resources/commercial-solutions-for-classified-program/solution-registration.

Solution registrations are valid for one year, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When the D/NM approved version of this CP is published, customers will have six months to bring their solutions into compliance with the new version and re-register them (see requirement DAR-GD-5). Customers are also required to update their registrations whenever the information provided on the registration form changes.

14 TESTING REQUIREMENT

The DAR solution testing requirements are located in a separate DAR CP Testing Annex. This annex contains the specific tests that allow the Security Administrator or Integrator to ensure the solution is properly configured. Contact the CSfC PMO to obtain the DAR CP Testing Annex.

APPENDIX A: GLOSSARY OF TERMS

Administration Workstation - This device is commonly used for logging, configuration review, and management of the EUD.

Anti-Tamper Measures - These measures serve to deter or delay modification of an EUD. Passive anti-tamper measures aid in detecting attempts to modify the EUD or inject a substitute device. Active anti-tamper measures serve the same purpose as passive measures, while actively detecting and securing the EUD. Examples include personalization options such as stickers, screen savers, wall papers, or other personalization methods which do not interfere with the configuration of the device.

Assessment - The technical evaluation of a system's security features performed as part of, and in support of, the approval/accreditation process that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Assessment and Authorization - A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

Assurance - A measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Audit - The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Authentication - The process of confirming the identity of a user.

Authorizing Official (AO) – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorization - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls (NIST 800-37). It can also be the decision to allow or deny a subject access to an object. For example, after a user has been authenticated, authorization determines if the user has the rights to perform specific actions on the device.

Boot Integrity Verification - These features ensure no code is executed during the boot process that has not first been verified for its integrity and authenticity. Each step in the boot process should verify the integrity of the next piece of code to execute before handing execution over to it. In current PC

technology, this operates in two stages. First, the integrity and authenticity of the firmware is verified using a platform/vendor specific technology. Second, UEFI secure boot verifies the option ROMs, and the OS loader before execution is handed over to the operating system.

Capability Package (CP) - The set of guidance provided by NSA that describes recommended approaches to provide architectures and configuration requirements that empower CS 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. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and Integrators.

Commercial National Security Algorithm (CNSA) - Set of commercial algorithms capable of protecting data through Top Secret level (previously known as Suite B).

Committee on National Security Systems Policy No. 15 (CNSSP-15) - Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems.

Compromise - Any computing resource whose confidentiality, integrity, or availability has been adversely impacted, either intentionally or unintentionally.

Continuous Physical Control - The AO defines what is considered "Continuous Physical Control." Previously called "positive control."

Cryptographic Erase - A method of sanitization in which an encryption key for the encrypted data is sanitized, making recovery of the decrypted data infeasible.

DAR Component - Consists of a component that is part of the DAR solution (e.g., HWFDE, SWFDE, PE).

DAR Solution - A DAR Solution consists of two layered components (e.g., HWFDE and SWFDE).

Enterprise Management (EM) - DAR use case that employs a client-server architecture to provide management of DAR components at an enterprise level.

End User Device (EUD) - Any computing or storage device that can store data when it is powered off (in the context of this DAR document).

False Acceptance – When a different user will pass the biometric when they should not. Measured by false acceptance rate (FAR).

False Rejection – When an authorized user's measurements fail to authenticate. Measured by false rejection rate (FRR).

Federal Information Processing Standards (FIPS) - A set of standards that describes the handling and processing of information within governmental agencies.

File Encryption (FE) - File encryption is the process of encrypting individual files or sets of files on an EUD and permitting access to the encrypted data only after proper authentication is provided.

Found Device - A lost device that has been recovered. (See Lost Device definition.)

Full Disk Encryption (FDE) - Also known as whole disk encryption, is the process of encrypting all the data on the drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the FDE product.

GA- DAR use case that doesn't use a specific use case such as RM, UO, EM or LF. This is generally applicable to requirements and used in a standalone implementation.

HF - DAR solution design that uses HWFDE as the outer layer, and FE as the inner layer.

HH- DAR solution design that uses HWFDE as the outer and inner layers.

Heartbeat - Heartbeat is a periodic network activity performed by a server to monitor the health or connectivity status of a client. Monitoring a heartbeat is useful for inventory, assurance, tracking, and geofencing. If a heartbeat is not detected at its predetermined regular interval, a predefined administrator action, such as forced shutdown, can be performed to mitigate the theft of data.

High Assurance GOTS solution - cryptographic equipment, assembly, or component that is classified or certified by the NSA for encrypting and decrypting classified or sensitive national security information when appropriately keyed. *(Previously referred to as Type 1)*

HS - DAR solution design that uses HWFDE as the outer layer, and SWFDE as the inner layer.

IA Product - Product whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks.

ISV - An independent software vendor is a separate vendor that provides a product for managing a self-encrypting drive and provides a user interface to the drive. This definition is unique to this CP.

Known Secret - PIN, password, or passphrase.

Layer - Every DAR solution protects classified data with two layers (e.g., HWFDE, SWFDE, FE, and PE).

Lost Device - A device that is removed from the control of the physical security procedures defined by the AO.

Mission Control Element (MCE) - The location and system from which a connection occurs to a remote EUD using the UO use case.

Network Attached Storage (NAS) - A file-level computer data storage server connected to a computer network providing data access to a group of clients. A NAS is a specialized computer built for storing and serving files.

PF - DAR solution architecture that features a PE layer under the FE layer.

Platform Encryption (PE) - A device that has met the requirements (and high assurance use case) of the MDF PP.

Pre-Boot Environment (PBE) - The initial software that is executed on start-up of the EUD that requires a user to authenticate successfully before decrypting and booting an operating system. This is the layer of authentication for the SWFDE or HWFDE product.

Protection Profile (PP) - A 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.

Removable Media (RM) – A device which has the primary purpose of providing external storage of data, protected by DAR via two layers of encryption.

Radio Frequency Identification (RFID) – Technology that uses electromagnetic fields to automatically identify and track tags attached to objects. A mechanism that can be used with DAR location services.

Rooted - The process of modifying a device such that it allows users to attain administrative privileges (i.e., root access).

Salt - A salt is random data that is added to a one-way function which hashes a password or passphrase in order to defeat dictionary attacks and pre-computed rainbow tables.

Secure Erase - The process of removing specified data from a device via overwrite of that data.

Self-Encrypting Drive (SED) – A drive that contains hardware built into the drive controller chip that automatically encrypts all data written to the drive and decrypts all data read from the drive.

SF - DAR solution architecture that features an SWFDE layer under the FE layer.

Software Full Disk Encryption (SWFDE) - A software product that provides Full Disk Encryption.

Storage Area Network (SAN) - A dedicated network that provides access to consolidated, block level data storage. SANs devices appear like locally attached devices to the client operating system.

Supply Chain Risk Management (SCRM) - A program to establish processes and procedures to minimize acquisition-related risks to critical acquisitions including hardware components and software solutions from supply chain threats due to reliance on global sources of supply.

Unauthenticated State - The state an EUD is in when the identity of a user, user device, or other entity has not been verified.

Unattended Operations (UO) - DAR use case that operates using a remote managed architecture to manage an unattended DAR solution. Continuous physical control is defined by the AO.

Volume - A collection of separate units of logically divided media (partition) acting as a single entity that has been formatted with a file system.

1251 # APPENDIX B: ACRONYMS

Acronym	Meaning
AA	Authorization Acquisition
AES	Advanced Encryption Standard
AK	Authentication Key
AO	Authorizing Official
ASPP	Application Software Protection Profile
AU	Auditing Requirements
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CE	Cryptographic Erase
CM	Configuration Change Detection Requirements
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf
CP	Capability Package
cPP	Collaborative Protection Profile
CR	Configuration Requirement
CSfC	Commercial Solutions for Classified
CSS	Central Security Service
DAR	Data-at-Rest
DEK	Data Encryption Key
DIT	Data-In-Transit
DM	Device Management Requirements
D/NM	Deputy National Manager
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
EE	Encryption Engine
EM	Enterprise Management
EU	EUD Requirements

Acronym	Meaning
EUD	End User Device
EP	Extended Package
FAR	False-Acceptance-Rate
FRR	False-Rejection-Rate
FE	File Encryption
FE EP	File Encryption Extended Package
FEK	File Encryption Key
FDE	Full Disk Encryption
FIM	Firmware Integrity Measurement
FIPS	Federal Information Processing Standards
GA	Generally Applicable
GCM	Galois/Counter Mode
GD	Requirements of Use and Handling of Solutions
GPS	Global Positioning System
GOTS	Government-off-the-Shelf
HAIPE	High Assurance Internet Protocol Encryptor
HDD	Hard Disk Drive
HF	HWFDE and FE
HH	HWFDE and HWFDE
HS	HWFDE and SWFDE
HW	Requirements for HWFDE Components
HWFDE	Hardware Full Disk Encryption
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
ISSO	Information System Security Officer
ISV	Independent Software Vendor
IT	Information Technology
JIMS	Joint Incident Management System
KEK	Key Encryption Key
KM	Key Management Requirements
KMIP	Key Management Interoperability Protocol
LAN	Local Area Network

Acronym	Meaning
LF	Lost and Found
MA	Mobile Access
MCE	Mission Control Element
MDF	Mobile Device Fundamentals
MoA	Memorandum of Agreement
MSC	Multi-Site Connectivity
NAS	Network Attached Storage
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
O&M	Operations and Maintenance
OCONUS	Outside the Continental United States
OEM	Original Equipment Manufacturer
OPSEC	Operational Security
OS	Operating System
PBE	Pre-Boot Environment
PE	Platform Encryption
PF	PE and EE
PIN	Personal Identification Number
PIV	Personal Identity Verification
PMO	Program Management Office
POC	Point of Contact
PP	Protection Profile
PS	Product Selection
PUB	Publication
RA	Risk Assessment
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFID	Radio Frequency Identification
RIM	Reference Integrity Manifest
RM	Removable Media
RP	Requirements for Incident Reporting

Acronym	Meaning
RPG	Random Password Generation
RSA	Rivest Shamir Adelman
SA	Security Administrator
SAN	Storage Attached Network
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SED	Self-Encrypting Drive
SF	SWFDE and FE
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIM	Subscriber Identity Module
SIPRNet	Secret Internet Protocol Router Network
SR	Solution Requirements
SSD	Solid State Drive
SW	Requirements for SWFDE
SWFDE	Software Full Disk Encryption
T&E	Test and Evaluation
TR	Test Requirements
UAV	Unmanned Aerial Vehicle
UUV	Unmanned Underwater Vehicle
UEFI	Unified Extensible Firmware Interface
UO	Unattended Operations
U.S.	United States
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
WPS	Wi-Fi Positioning System
XEX	XOR Encrypt XOR
XOR	Exclusive OR
XTS	XEX-based tweaked-codebook mode with cipher text stealing

1252

APPENDIX C: CSFC INCIDENT REPORTING TEMPLATE

CSfC Incident Reporting Template	
Point of Contact (POC) name, phone, email:	
Alternate POC name, phone, email:	
CSfC Registration Number:	
Classification level of affected system:	
Name of affected network(s):	
Affected component(s) manufacturer/vendor:	
Affected component(s) model number:	
Affected component(s) version number:	
Date and time of incident:	
Description of incident:	
Description of remediation activities:	

CSfC Incident Reporting Template	
Is Technical Support from NSA Requested? (Yes/No)	

1254

1255

APPENDIX D: PASSWORD/PASSPHRASE STRENGTH PARAMETERS

This appendix provides password and passphrase parameters for use in DAR products to address attacks directly based on the strength of the password or passphrase. The information below, describes the factors that provide strength to passwords and passphrases, and sets a minimum standard for use.

Strength

Entropy is used as a measure of strength for passwords and passphrases. According to NIST SP 800-63-2, *Electronic Authentication Guideline*, entropy is a measure of the amount of uncertainty that an attacker faces to determine the value of the secret. Entropy is usually stated in bits; for example, an unpredictable password with 10 bits of entropy would have 2^{10} or 1,024 possible combinations. The greater the number of possible combinations, the greater the amount of time on average it will take an attacker to find the correct password or passphrase.

Random vs. User Generated

Passwords and passphrases are required to be randomly generated as of *DAR CP version 5.0*. A randomly generated value has the benefit that it will provide an objective amount of entropy, but can be difficult for a user to remember. A user generated value may be easier to remember, but may be predictable, therefore, lowering the entropy calculation reducing the strength of the password or passphrase. If random generation is not a workable solution for the mission use case, then a deviation from the DAR CP is required. There are many suggested methods for the user generation of passwords; more information on these can be found in NIST SP 800-63B, *Digital Identity Guidelines*. These methods attempt to reduce the predictability while maintaining length and memorability, but because they are user chosen, they are all still at risk of being predicable. If the password or passphrase is predicable, an attacker could try a much shorter list of common or personal values, reducing the average time to find the correct password or passphrase. The most effective way to ensure the password or passphrase has an appropriate amount of entropy is by applying random generation. The remainder of this appendix addresses random generation.

Randomly Generated Passwords

The strength of a password is determined by the character set and the length. The character set describes the group of unique characters that may be chosen to create the password, such as numbers, lower case letters, upper case letters, special characters, etc. The length simply describes the number of characters chosen.

Randomly Generated Passphrases

The strength of a passphrase is determined by the number of words in the passphrase and the number of words in the word list, the pool of unique words that can be chosen for the passphrase. The word list can be adjusted by the properties of the words it includes, such as minimum word length, maximum word length, and complexity (includes factors such as the difficulty of the word, capitalization, character substitutions, etc.) per word. Each property has a tradeoff between strength and usability. A minimum word length of four is recommended to maintain the effectiveness of the passphrase. This is based on entropy per word from a word list ranging from 10,000 to 450,000, and entropy per character from a

character set of 26. This ensures the entropy per set of characters of a given word is greater than the entropy provided from selecting a word from the word list.

Multi-Factor Authentication

If a password/passphrase is being used as part of a multi-factor authentication solution per DAR-CR-14 and another factor is being used as a primary factor for that component, then the password or passphrase does not need to comply with these rules. It is still recommended to comply with these rules. If the other factor is not a primary factor and used as secondary, these rules still apply.

Assumptions

The product is assumed to meet one of the DAR protection profiles. All password and passphrase conditioning assumes salting is performed, making pre-computed attacks infeasible. A salt is a random value that is used in a cryptographic process to ensure that the results of the computations for one instance cannot be reused by an attacker. The product is assumed to be kept up to date and the protection mechanisms used in calculations cannot be bypassed.

Minimum Strength Calculations

CSfC provides a tool for random generation, which is available on GitHub at https://github.com/nsacyber/RandPassGenerator. This tool must be used to generate random passwords and passphrases. When using this tool to generate passwords and passphrases, it should be ran on a network capable of protecting the classification of the data that is being protected. The tool should be sent to the appropriate classified network through a Data Transfer Agent (DTA) for further use. During registration instructions on how to download, verify, and use the tool will be provided. Alternatively, contact the CSfC PMO at csfc_register@nsa.gov for further instructions. The provided tool is set to a default strength of 160 bits, this may be set lower, but must not be set below 102 bits. The solution will provide a minimum of 112 bits of entropy with at least 10 bits provided by the product's password conditioning function. If using custom word lists or character sets and not using the provided tool, Tables 21 and 22 show the required minimum length of a password and passphrase given, a set of characters or words, to reach 102 bits of entropy. The provided tool is capable of using custom word lists. The user must define the size of the character set or word list they will use. To use the tables, find the value that is less than or equal to your character set (or word list) size in the Character Set Size (or Word List Size) column and the corresponding value in the Minimum Password Length (or Minimum Passphrase Length) column for that row reflects the minimum password (or passphrase) length that must be used.

Table 21: Randomly Generated Minimum Password Length

Randomly Generated Passwords	
Character Set Size	**Minimum Password Length**
83	16
64	17
51	18
42	19
35	20

Randomly Generated Passwords	
Character Set Size	**Minimum Password Length**
29	21
25	22
22	23
20	24
17	25
16	26
14	27
13	28
12	29
11	30

1326

1327 **Table 22: Randomly Generated Minimum Passphrase Length**

Randomly Generated Passphrases	
Word List Size	**Minimum Passphrase Length**
1383605	5
131072	6
24347	7
6889	8
2581	9
1177	10

1328

1329

APPENDIX E: CONFIGURATION GUIDANCE

A number of the DAR requirements listed in the main body of this CP might require additional configuration information in order to be fully understood by customers who are using them as the basis for preparing Registration Packages for CSfC solutions. The list that follows, includes the additional information on requirements that may provide further guidance in order for customers to prepare and complete the Registration Packages. Please reference the requirements tables to see which solution design and use case these requirements apply. If there are questions about requirements that are not discussed in this list, please submit questions to the DAR CP maintenance team and a response will be provided for considerations in future updates of the CP.

Requirement	Clarification
DAR-SR-1: Default accounts, passwords, community strings, and other default access control mechanisms for all components must be changed or removed.	Not all products will have defaults. If the product does not have a default, no action is needed for compliance with this requirement. If defaults do exist, vendors are required to provide guidance on how to change their authentication factors during their protection profile validation. Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document.
DAR-SR-6: The AO must provide procedures for performing CE.	Vendors are required to provide guidance on how to perform a cryptographic erase of the encrypted data, this may also be referred to as changing the DEK or TSF. Wipe during their protection profile validation. Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document.
DAR-CR-1: Default encryption keys must be changed.	Not all products have default encryption keys. If the keys are generated upon provisioning, no action is needed for compliance with this requirement. If default encryption keys do exist, please follow the guidance in DAR-SR-6 to perform a cryptographic erase along with any other vendor guidance provided.
DAR-CR-3: DAR components must use algorithms for encryption selected from Table 1.	Not all products allow for changing of algorithms or key sizes used. If more than one is supported, the vendor is required to provide guidance for selecting those options. Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document. If no options are listed, you can confirm vendor algorithm and key size selection in the Security Target document, which is posted on the NIAP page.

Requirement	Clarification
DAR-CR-4: Each DAR component must prevent further authentication attempts after a number of failed attempts defined by the AO.	Vendors may not include this functionality in their product, however, they may include other non-configurable mitigations. For full disk encryptors, vendors are required to provide one of the following options: Cryptographic erase, forced delay between attempts, or institute a block after a number of consecutive attempts. If your FDE consists of two products, these settings are required for the EE and optional for the AA. The vendor is required to provide guidance for any configurable limits. Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document. For information on the selection the vendor made please refer to the Security Target document. For file encryptors, vendors are not required to provide this functionality. Refer to any guidance provided by the vendor. For platform encryption products, vendors are required to implement throttling between authentication attempts. There is no configuration needed for this. The vendor is also required to provide for a cryptographic erase of all protected data upon a configurable number of failed authentication attempts. The vendor is required to provide guidance on how to configure the number of attempts. Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document.
DAR-CR-5: Each DAR layer must perform a CE after a number of consecutive failed logon attempts as defined by the AO.	Please refer to the guidance given in DAR-CR-4.
DAR-CR-10: All CSfC components must be implemented (configured) using only their NIAP-approved configuration settings.	Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document for assistance in configuring the product into a compliant state.

Requirement	Clarification
DAR-CR-11: Users must be restricted to designated user folders.	There are multiple ways to accomplish this requirement depending on the OS and software used; any method is acceptable. Here are common ways to accomplish this on the most used Operating Systems. For all restricted directories do the following: Linux: Run the Nautilus file browser, right click the folder, and select Properties. In the Permissions tab, change the Access drop down to Read Only for all end users, then select Change. Mac: Select the folder, select File, click the arrow next to the gear icon to display further options, select Get Info, and click the drop down for sharing and permissions (may have to scroll all the way to the bottom down to see this). For all end users and groups on the device: Select the user or group and choose Read Only. Then select the gear icon and apply all changes. For additional information please see this page: https://support.apple.com/kb/PH18894?locale=en_US&viewlocale=en_US Windows: Right click on the folder, select Properties, and select the Security tab. For all end users and groups on the device: Select the user or group, check the Deny box for the write permission and then click Apply. For additional information please see this page: https://technet.microsoft.com/en-us/library/bb456977.aspx
DAR-SW-3:The SWFDE must be configured to use one of the following primary authentication options: • A randomly generated passphrase or password that meets the minimum strength set in Appendix D, or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or • An external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1. Any combination of the above.	Reference random password/passphrase generation tool, reference multifactor authentication section.

Requirement	Clarification
DAR-FE-3: The FE product must use one of the following primary authentication options: • A randomly generated passphrase or password that meets the minimum strength set in Appendix D, or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or • An external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1. Any combination of the above.	Reference random password/passphrase generation tool, reference multifactor authentication section.
DAR-PE-1: The PE must enable the "wipe sensitive data" management function for imported or self-generated keys/secrets and/or other classified data.	Vendors are required to provide guidance on how to perform the "wipe sensitive data" management function; this may also be referred to as TSF Wipe, during their protection profile validation. Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document.
DAR-PE-5: The PE must use the following for authentication: • A minimum of a six-character, case sensitive alphanumeric password with the length and complexity as defined by the AO, or • A passphrase with the length and complexity as defined by the AO.	Reference random password/passphrase generation tool, reference multifactor authentication section.
DAR-HW-3: The HWFDE must be configured to use one of the following primary authentication options: • A randomly generated passphrase or password that meets the minimum strength set in Appendix D, or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or • An external smartcard or software capability containing a software certificate with RSA or ECC key pairs	Reference random password/passphrase generation tool, reference multifactor authentication section.

Requirement	Clarification
per Table 1. Any combination of the above.	
DAR-EU-9: The Security Administrator (SA) must disable system power saving states on EUDs (e.g., sleep and hibernate).	There are multiple ways to accomplish this requirement depending on the OS and software used; any method is acceptable. Here are common ways to accomplish this on the most used Operating Systems: Linux: Please refer to vendor guidance on your specific distribution. Mac: Open Apple menu, select system preference, and select Energy Saver. For all power plans: Drag to slider for computer sleep to Never for sleep. Display sleep does not need to be changed. Windows: Open control panel. Select small icons in the top right, then select power options. For all power plans: Select Change Plan Settings, select Change Advanced Power Settings, expand the sleep list and set Sleep and Hibernate to Disabled.
DAR-EU-10: The EUD must power off after a period of inactivity defined by the AO.	There are multiple ways to accomplish this requirement depending on the OS and software used, any method is acceptable. Here are common ways to accomplish this on the most used Operating Systems: Linux: Please refer to vendor guidance on your specific distribution. Mac: This function must be provided by third party software or running a script. Windows: Open task scheduler, select create task. Under the general tab: Fill in a name. Select run whether user is logged on or not. Make sure run with highest privileges is checked. Under the triggers tab: Click new, select daily, then select ok. Under the actions tab: click new and enter shutdown in the program/script box. Enter /l and /f under the add arguments (optionally) box. Under the conditions tab: Check the box for start the task only if the computer is idle for and Under the settings tab: Check the box if the task fails restart every time and select an increment shorter than the AO defined period. Uncheck the box start the task only if the computer is on AC power. Under the attempt to restart up to box enter 999.

Requirement	Clarification
DAR-EU-14: System folders must have user write permissions disabled unless authorized by an administrator.	Please refer to guidance on DAR-CR-11 and ensure end users are restricted from writing to system folders.
DAR-EU-20: The BIOS must be configured to require a password before continuing the boot process.	This is a password to continue the boot process, creating a password prompt before the FDE and/or OS login. Not all motherboards support this feature. Generally the first screen will indicate which button is used to change BIOS/UEFI settings; if not please refer to product documentation. Once in the settings, browse for an option to require a password to continue the boot process and enable it. The password does not need to be strong, the absence of the password would indicate tampering.
DAR-EU-21: All DAR FDE components must be cryptographically erased before being provisioned again.	Please refer to DAR-SR-6 guidance on how to perform a cryptographic erase.
DAR-EU-22: All DAR components must be cryptographically erased before being provisioned again.	Please refer to DAR-SR-6 guidance on how to perform a cryptographic erase.
DAR-EU-24: If supported, the EUD must have the BIOS/ UEFI password enabled.	This is a password that is required before allowing access to change BIOS/UEFI settings. Not all motherboards support this feature. Generally the first screen will indicate which button is used to change BIOS/UEFI settings; if not please refer to product documentation. Once in the settings, browse for an option to set a BIOS/UEFI password.
DAR-EU-26: Each EUD must be personalized by the end user. (This should not violate any other security features.)	Personalization means making device changes specific to each end user that would be noticed before both layers are authenticated. This can include stickers, markings, wallpapers, etc.
DAR-EU-36: Each EUD must be personalized by the end user. (This should not violate any other security features.) *(previously DAR-LF-12)*	Please refer to DAR-EU-26 to personalize devices.
DAR-EU-37: EUDs must use boot integrity verification technology. *(previously DAR-LF-5)*	This requirement is based on device acquisition. Not all devices support these features. The specific features will have to be discussed with the device vendor and then configured according to that vendor's specifications.
DAR-KM-3: The DAR solution must disable all key recovery mechanisms.	If the product supports key recovery mechanisms they are required to state how to disable those mechanisms in their documentation. Please refer to the NIAP Product Compliant List, select your component, and view the Administrative Guidance document. Does not apply to the EM use case.

APPENDIX F: CONTINUOUS PHYSICAL CONTROL

Since the NSA requires that implementing organizations define the circumstances in which an EUD that is part of the solution is considered outside of the continuous physical control of authorized users (i.e., "lost"), Authorizing Officials will define “continuous physical control”, and that definition should align with the intended mission and threat environment for which the solution will be deployed. Organizations must also define the circumstances in which an EUD that is a part of that organization's solution is to be considered recovered back into the continuous physical control of authorized users (i.e., "found").

In order to provide some guidance to clients who may not have experience with handling continuous physical control issues, we have consulted several experienced organizations that have provided examples of the criteria they use to define “continuous physical control”. The intent of this is to cite a number of potential generic measures that can be taken as additional Continuous Physical Control guidance without attribution to the source of these measures.

DAR customers have provided several ideas of measures they are considering to deal with particular circumstances. Listed are some of the ideas being considered for handling EUDs:

- Package using clear one-use bags.
- Use tamper evident stickers with recorded unique serial numbers on critical screws.
- Use commercial backpacks with-pick-resistant locks.
- Lock in automobile glove box and lock the car.

Some users currently handle the issue by simply not authorizing the removal of any EUDs from the secure location where they are housed.

Continuous Physical Control Examples:

(U) To assist in the development of well thought out definitions of continuous physical control, segments of good definitions used by previous registrations have been provided. These examples should be reviewed to ensure that the definition given for a registration follows the intent of the requirement.

Traveling with EUDs. Commands will create local policy to address specifics on traveling with EUDs, to include outside the continental U.S. (OCONUS) locations, in accordance with (IAW) local security procedures.

The following general actions apply while traveling with EUDs:

a. Prior to travel:
   (1) Do not take your device if you can do without it.
   (2) Do not take information you do not need, including sensitive contact information.
   (3) Ensure that the latest, most current, up-to-date antivirus protection, spyware protection, OS security patches, and a personal firewall have been pushed and enabled by the responsible Information Technology (IT) support.
   (4) Disable infrared ports and features you do not need.

b. During travel:

(1) Keep the EUD under physical control at all times when traveling.
(2) Never place the EUD in checked luggage.
(3) Never store the EUD in an airport, train station, bus station, or any public locker.
(4) If leaving the EUD in a vehicle that an AO determines is sufficient to keep the EUD safe, then the EUD should be kept out of sight.
(5) Do not leave EUDs unattended unless required activities demand so. In the event that they must be unattended, stow them securely and out of sight after removing the battery and SIM card. Keep the battery and SIM card under control at all times to maintain the protection of its information.
(6) Avoid leaving the EUD in a hotel room.
(7) Be prepared for airport security checks. Have the EUD's batteries charged or a power cord handy to demonstrate if necessary that it is functional.
(8) Heighten vigilance at any security or luggage-scanning checkpoint. Place EUD on the conveyer belt only after the belongings of the person ahead of you have cleared the scanner. If delayed, keep the EUD in view.
(9) Exercise diligence when traveling in foreign countries because criminals or local intelligence may target the EUD for the information it contains.
(10) Do not display any sensitive information on the EUD screen when in any public place (such as an airport terminal, train or bus station, airplane, train, bus, or taxi).
(11) Terminate connections when not using them.
(12) If the device or information is stolen, report it immediately to your home organization and the local U.S. embassy or consulate.

c. Return from travel:
(1) Change the password.
(2) Have your command or unit examine the device for the presence of malicious software.

APPENDIX G: REFERENCES

Application Software PP	*Protection Profile for Application Software Version 1.2. (File Encryption component).* www.niap-ccevs.org/Profile/Info.cfm?id=394	April 2016
Campus WLAN CP	*Campus WLAN CP. Available on the CSfC web page* https://www.nsa.gov/resources/commercial-solutions-for-classified-program/capability-packages	Latest version
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
CNSSI 1253	*CNSS Instruction No. 1253, Security Categorization and Control Selection for National Security Systems*	March 2014
CNSSI 4004	*Committee on National Security Systems Instruction (CNSSI) No. 4004 Destruction and Emergency Protection Procedures for COMSEC and Classified Material*	January 2008
CNSSI 4009	*CNSSI 4009, Committee on National Security Systems (CNSS) Glossary* www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2015
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	October 2016
CNSSP 28	*CNSS Policy (CNSSP) Number 28, Cybersecurity of Unmanned National Security Systems*	July 2018
CSfC Components List	*CSfC Components List. Available on the CSfC web page* https://www.nsa.gov/resources/commercial-solutions-for-classified-program/components-list	Current update
FDE cPP AA	*Collaborative Protection Profile for Full Disk Encryption- Authorization Acquisition Version 2.0. (Software or Hardware FDE component)* www.niap-ccevs.org/Profile/Info.cfm?id=406	September 2016
FDE cPP EE	*Collaborative Protection Profile for Full Disk Encryption- Encryption Engine Version 2.0. (Software or Hardware FDE component)* www.niap-ccevs.org/Profile/Info.cfm?id=407	September 2016
FE Module	*PP-Module for File Encryption. (File Encryption component)* www.niap-ccevs.org/Profile/Info.cfm?id=415	July 2019
FE EM Module	*PP-Module for File Encryption Enterprise Management. (File Encryption Enterprise Management component)* www.niap-ccevs.org/Profile/Info.cfm?id=427	July 2019

FIPS 140-2	*Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules*	May 2001
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	August 2015
FIPS 186-4	*Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201-2	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	August 2013
MA CP	*Mobile Access CP. Available on the CSfC web page* https://www.nsa.gov/resources/commercial-solutions-for-classified-program/capability-packages	Latest version
MDF PP	*Protection Profile for Mobile Device Fundamentals. (Platform Encryption component)-* www.niap-ccevs.org/Profile/Info.cfm?id=417	June 2017
MSC CP	*Multi-site Connectivity CP. Available on the CSfC web page* https://www.nsa.gov/resources/commercial-solutions-for-classified-program/capability-packages	Latest version
NIAP Product Compliant List	*NIAP Product Compliant List.* www.niap-ccevs.org/products/	Current update
NIST SP 800-111	*NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices*	November 2007
NIST SP 800-131A (Rev 1)	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths. E. Barker.*	November 2015
NIST SP 800-132	*Recommendation for Password-Based Key Derivation*	December 2010
NIST SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines. D. Cooper, et. al.*	April 2011
NIST SP 800-56A (Rev 3)	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. E. Barker, D. Johnson, and M. Smid*	April 2018

NIST SP 800-56B (Rev 2)	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. E. Barker, et. al.*	March 2019
NIST SP 800-56C (Rev 2)	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion. L. Chen.*	August 2020
NIST SP 800-63-2	*NIST Special Publication 800-63-2, Electronic Authentication Guideline*	August 2013
NSA CNSA	*NSA Guidance on CNSA Cryptography* https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm	No Date Specified
NSA/CSS Policy Manual 9-12 Storage Device Sanitization	*NSA/CSS Storage Device Declassification* https://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf	December 2014
OS PP	*Protection Profile for General Purpose Operating Systems.* https://www.niap-ccves.org/Profile/Info.cfm?id=400	March 2016

1413