National Security Agency/
Central Security Service

CYBERSECURITY
SOLUTIONS

DATA AT REST COMPLIANCE CHECKLIST

Version 5.0
November 2020

Registration ID#:

Solution Name:

Date Submitted:

Data-at-Rest
Compliance Checklist

TABLE OF CONTENTS

Data-at-Rest
Compliance Checklist

LIST OF TABLES

Data-at-Rest Compliance Checklist

1 INTRODUCTION

This generic CSfC Data-at-Rest (DAR) CP meets the demand for DAR solutions using Commercial National Security Algorithm (CNSA) Suite. These algorithms are used to protect classified data using layers of COTS products.

Table 1: Approved Commercial National Security Algorithm 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	FIPS PUB 180-4
Can protect	Up to Top Secret	---------

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.
PE/FE	PF	DAR solution design that uses FE as the inner layer and PE as the outer layer.
HWFDE/FE	HF	DAR solution design that uses FE as the inner layer and HWFDE as the outer layer.
HWFDE/SWFDE	HS	DAR solution design that uses SWFDE as the inner layer and HWFDE as the outer layer.
HWFDE/HWFDE	HH	DAR solution design that uses HWFDE as the inner layer and HWFDE as the outer layer.

The solution is contained to an individual EUD. 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.

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. **as of DAR v5.0, the LF use case requirements are now dispersed in the "Use Case" column of the requirements table and no longer in a separate table. When implementing the LF use case, all Threshold requirements with "LF" must be met.*
Removable Media	RM	DAR use case that implements the SF, HF, HH, or HS solution designs.
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.
Unattended Operations	UO	DAR use case for managing unattended or remote managed DAR solutions and systems that implements HS, HF, HH, or SF.
Generally Applicable	GA	DAR use case that is generally applicable to a standalone use case and corresponding solution design.

2 DAR CONFIGURATION REQUIREMENTS

The tables of requirements in the following sections specify the solution design and use case each requirement is applicable to:

Solution Designs:

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

Data-at-Rest Compliance Checklist

Use Cases:

- LF use case: DAR solution designs include PF, HF, HH, or HS.
- RM use case: DAR solution designs include SF, HF, HH, or HS.
- UO use case: DAR solution designs include SF, HF, HH or, HS.
- 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 (e.g., 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 utilizing 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 (i.e., 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 3	Table 5
SR	Overall Solution Requirements	Section 4.1	Table 6
CR	Configuration Requirements for All DAR Components	Section 4.2	Table 7
SW	SWFDE Component Requirements	Section 4.3	Table 8
FE	FE Component Requirements	Section 4.4	Table 9
PE	PE Component Requirements	Section 4.5	Table 10
HW	HWFDE Component Requirements	Section 4.6	Table 11
EU	EUD Requirements	Section 4.7	Table 12
CM	Configuration Change Detection Requirements	Section 4.8	Table 13
DM	Device Management Requirements	Section 4.9	Table 14
AU	Auditing Requirements	Section 4.10	Table 15
KM	Key Management Requirements for All DAR Components	Section 4.11	Table 16
SC	Supply Chain Risk Management Requirements	Section 4.12	Table 17
GD	Use and Handling of Solutions Requirements	Section 5.1	Table 18
RP	Incident Reporting Requirements	Section 5.2	Table 19
TR	Testing Requirements	Section 6	Table 20

3 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.

Data-at-Rest
Compliance Checklist

Table 5: Product Selection Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM, GA, LF, RM, UO	T=O		
DAR-PS-3	The Inner and Outer DAR layer 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	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
DAR-PS-4	(Moved to DAR-SC-2)					

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-PS-5	The cryptographic libraries used by the Inner and Outer DAR layers must be independently developed and implemented.	SF, PF, HF, HS, HH	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	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, SF, HH	EM	T=O		

4 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 for how to configure the components for a DAR solution.

Data-at-Rest Compliance Checklist

4.1 Overall Solution Requirements

Table 6: Overall Solution Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	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	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	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.	SF, PF, HF, HS, HH	EM, GA, RM, UO	T=O		
DAR-SR-5	The AO must provide guidance when CE should be implemented.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	O	Optional	
DAR-SR-6	The AO must provide procedures for performing CE.	SF, PF, HF, HS, HH	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	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	LF	T=O		

4.2 CONFIGURATION REQUIREMENTS FOR ALL DAR COMPONENTS

Table 7: Configuration Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-CR-1	Default encryption keys must be changed.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
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	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	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	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	EM, GA, LF, RM, UO	O	Optional	

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-CR-6	Each DAR component must generate its own symmetric encryption keys on the EUD or received keys generated by the Enterprise Management server.	SF, PF, HF, HS, HH	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	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	EM, GA, LF, RM, UO	T=O		
DAR-CR-9	EUDs must encrypt all classified data. (Refer to Section 5.2 for additional information on FE.)	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
DAR-CR-10	All components must be implemented (configured) using only their NIAP-approved configuration settings. User may change settings that are not part of NIAP evaluation.	SF, PF, HF, HS, HH	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		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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 would then need to use a token or other factor).	HF, HS, SF, HH	EM, GA, UO	T=O		
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	EM, GA, RM, UO	O	Optional	
DAR-CR-14	At least one DAR layer must use multi-factor authentication.	HF, HS, SF, HH	EM, GA, LF, RM, UO	O	Optional	
DAR-CR-15	The removable media must not be bootable.	HF, HS, SF, HH	RM	T=O		
DAR-CR-16	The DAR Enterprise Server, must only manage one component/layer, and shall not manage the other component/layer of the DAR solution.	HF, HS, HH, SF	EM	T=O		
DAR-CR-17	All administrators must use unique identifiable accounts.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-CR-18	A baseline configuration that complies with this CP must be enforced on all registered endpoints.	HF, HS, HH, SF	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	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	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	EM	T=O		
DAR-CR-22	The administrator must configure remediation options (account lockout, key revocation, etc.) for failed authorization attempts by the user, as determined by the AO.	HF, HH, HS, SF	EM	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-CR-23	The administrator must configure remediation options (account lockout, key revocation, etc.) for failed authorization attempts by the user, as determined by the AO.	SF, PF, HF, HS, HH	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	EM	O	Optional	
DAR-CR-25	EUDs that are lost or compromised must be revoked and issue zeroize commands.	HF, HH, HS, SF	EM	T=O		

4.3 SWFDE COMPONENT REQUIREMENTS

Table 8: SWFDE Component Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-SW-1	The SWFDE must use Cipher Block Chaining (CBC) for encryption.	SF, HS	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	EM, GA, LF, RM, UO	O	DAR-SW-1	
DAR-SW-3	The SWFDE must be configured to use one of the following primary	SF, HS	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
	authentication options: • A randomly generated passphrase that meets the minimum strength set in Appendix D. of the DAR CP (Password/Passphrase Strength Parameters); 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 or Table 1 • Any combination of the above.					

4.4 FE COMPONENT REQUIREMENTS

Table 9: FE Component Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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 authentication options: • A randomly generated passphrase or password that meets minimum strength set in Appendix D of the DAR CP (Password/Passphrase Strength Parameters); 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	SF, PF, HF	EM, GA, LF, RM, UO	T=O		

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
	certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1. • Any combination of the above.					

4.5 PE COMPONENT REQUIREMENTS

Table 10: PE Component Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	
DAR-PE-4	The AO must provide policy to the user determining when data or keys must be wiped.	PF	GA, LF	T=O		

Data-at-Rest
Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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		

4.6 HWFDE COMPONENT REQUIREMENTS

Table 11: HWFDE Component Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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. of the DAR CP	HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
	(Password/Passphrase Strength Parameters); 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 orTable 1 • A combination of both of the above.					

4.7 END USER DEVICE REQUIREMENTS

Table 12: End User Devices Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-1	All EUD provisioning must be performed through direct physical access or through an enterprise management server.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest
Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	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	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	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	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

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	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
	using the EUD after it is lost					
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	EM, GA, LF, RM, UO	T=O		
DAR-EU-8	AO must provide guidance on storing and/or securing authentication factors.	SF, PF, HF, HS, HH	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	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	EM, GA, LF, RM, UO	T=O		
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	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	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	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	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.	SF, PF, HF, HS, HH	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.	SF, PF, HF, HS, HH	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 DAR CP Section 4.10)	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	O	Optional	

Data-at-Rest
Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-19	The EUD, when not in use outside of a secured facility, must be kept in an AO-approved locked container.	SF, PF, HF, HS, HH	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	EM, GA, LF, UO	O	Optional	
DAR-EU-21	All DAR FDE components must be cryptographically erased before being provisioned again.	HF, HS, SF, HH	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.	SF, PF, HF, HS, HH	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.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-26	Each EUD must be personalized by the end user. (This should not violate any other security features.)	SF, PF, HF, HS, HH	EM, GA, RM	O	Optional	
DAR-EU-27	The EUD must not be used as a smartcard/USB Authentication Token, if it is also storing encrypted user data.	HF, HS, SF, HH	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	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.	SF, PF, HF, HS, HH	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	LF	T=O		

Data-at-Rest
Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	LF	T=O		
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	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	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	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	LF	T=O		

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-36	Each EUD must be personalized by the end user. (This should not violate any other security features.)	HH, HF, HS, PF	LF	T=O		
DAR-EU-37	EUDs must use boot integrity verification. (see DAR CP Appendix A)	SF, HH, HF, HS	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	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	UO	T=O		

4.8 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 13: Configuration Change Detection Requirements

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

Data-at-Rest
Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-CM-3	Log messages generated for configuration changes must include the specific changes made to the configuration.	SF, PF, HF, HS, HH	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	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	EM, GA, LF, RM, UO	T=O		

4.9 DEVICE MANAGEMENT REQUIREMENTS

Table 14: Device Management Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-DM-1	EUDs must be physically administered.	SF, PF, HF, HS, HH	GA, LF, RM	T	DAR-DM-2	
DAR-DM-2	EUDs must be remotely administered using an NSA-approved DIT protection solution (e.g., NSA Certified Product or CSfC approved solution).	SF, PF, HF, HS, HH	GA, LF, RM	O	DAR-DM-1	
DAR-DM-3	Administration workstations must be dedicated for the purposes given in the CP.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
DAR-DM-4	Administration workstations must physically reside within a protected facility where	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
	CSfC solution(s) are managed.					
DAR-DM-5	Administration workstations must be physically separated from workstations used to manage non-CSfC solutions.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
DAR-DM-6	Only authorized SAs (See DAR CP Section 12) must be allowed to administer the DAR Components.	SF, PF, HF, HS, HH	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	EM, UO	T=O		

4.10 AUDITING REQUIREMENTS

Table 15: Auditing Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-AU-1	EUDs must be inspected for malicious physical changes in accordance with AO defined policy.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	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	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	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	EM, GA, LF, RM, UO	O	Optional	

Data-at-Rest
Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM	T=O		

4.11 KEY MANAGEMENT REQUIREMENTS

Table 16: Key Management Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-KM-1	The key sizes used for each layer must be as specified in Table 1.	SF, PF, HF, HS, HH	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	EM, GA, LF, RM, UO	T=O		
DAR-KM-3	The DAR solution must disable all key recovery mechanisms.	SF, PF, HF, HS, HH	GA, LF, RM, UO	T=O		
DAR-KM-4	The algorithms used for each layer must be as specified in DAR CP Table 1.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
DAR-KM-5	If a physical recovery output is utilized, it must be secured as classified information, equivalent to the level of data it is protecting.	SF, HF, HS, HH	EM	T=O		
DAR-KM-6	If recovery information is distributed over a non-CSfC channel (e.g., physically, voice channel, etc.), it must be secured as classified information, equivalent to the level of data it is protecting.	SF, HF, HS, HH	EM	T=O		

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-KM-7	The AO must determine a methodology for verification of end users requesting recovery material, whether recovery information is distributed over a channel that is not provided by the CSfC solution (e.g., physically, voice channel, etc.) or distribution by a CSfC solution component which is expected to provide verification itself.	SF, HF, HS, HH	EM	T=O		

4.12 Supply Chain Risk Management requirements

Table 17: Supply Chain Risk Management Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM, GA, LF, RM, UO	O	Optional	

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-SC-2	Each component selected from the CSfC Components List must go through a Product SCRM Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product SCRM process. (See CNSSD 505 SCRM for additional guidance.)	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

5 SOLUTION OPERATION, MAINTENANCE, & HANDLING REQUIREMENTS

5.1 USE AND HANDLING SOLUTIONS REQUIREMENTS

The following requirements shall 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	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM, GA, LF, RM, UO	T=O		
DAR-GD-3	The AO will ensure that a compliance audit is conducted every year against the latest version of the DAR CP.	SF, PF, HF, HS, HH	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	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	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 DAR CP Section 13.3).	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	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	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	EM, GA, LF, RM, UO	T=O		
DAR-GD-10	User must report lost or stolen EUDs to their ISSO or chain of command as defined by the AO.	SF, PF, HF, HS, HH	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	EM, GA, LF, RM, UO	T=O		
DAR-GD-12	Security critical patches (such as Information Assurance Vulnerability Alert (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	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	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	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-GD-15	All authorized users must have the ability to CE keys for both layers.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	O	Optional	
DAR-GD-16	When using an FE Product, the user must ensure that no classified data shall 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					
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	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	LF	T=O		

Data-at-Rest
Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM	T=O		

5.2 INCIDENT REPORTING REQUIREMENTS

Table 19 lists requirements for reporting security incidents to NSA that are to be followed in the event a solution owner identifies a security incident which affects 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 4.10 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	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-RP-1	Report a security failure in any of the CSfC DAR solution components.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
DAR-RP-2	Report any malicious configuration changes to the DAR components.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM, GA, LF, RM, UO	T=O		
DAR-RP-4	Report any evidence of malicious physical tampering (e.g., missing or mis-installed parts) with solution components.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		
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 the NSA as specified in the CSfC Registration Letter.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		

Data-at-Rest Compliance Checklist

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
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	EM, GA, LF, RM, UO	T=O		

6 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 will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

Table 20: Test Requirements

Req #	Requirement Description	Solution Designs	Use Case	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-TR-1	The organization implementing the CP must perform all tests listed in the DAR Testing Requirements Annex.	SF, PF, HF, HS, HH	EM, GA, LF, RM, UO	T=O		