Classification: UNCLASSIFIED

INFORMATION ASSURANCE CAPABILITIES

Commercial Solutions for Classified

harnessing the power of commercial industry

Data at Rest Capability Package

Version 4.0

Compliance Checklist

Registration #

Solution Name:

Date Submitted:

Classification: UNCLASSIFIED

Registration ID:

TABLE OF CONTENTS

LIST OF TABLES

1 Introduction

As the portability of EUDs increases, 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. The solutions presented in this CP have specific requirements for configuration, product selection, components, provisioning, authentication, key management, operations, administration, roles, 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)	ECDSA 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	None

2 DAR Configuration Requirements

The CP provides the multiple solution designs listed in Table 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 “RM” design consists of either the SF, HF or HS architecture on removable media such as USB drives, microSD cards and removable drives. If RM is part of the design the solution must comply with requirements that meet both the RM and the additional solution design requirements. If a solution includes both host machines and RM, the customer must submit the registrations separately.

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 of the CP.
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 of the CP.
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 of the CP.
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 of the CP.
RM	RM	DAR solution design that uses RM through the use of a SF, HF, or HS solution design as described in Section 6.5 of the CP.

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," 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 it supports and should implement the Objective requirements associated with those solution designs where feasible. For example, a DAR solution utilizing an SWFDE and FE must implement only those Threshold requirements applicable to the SF design.

The customer may treat the device as being 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 3 lists the digraphs used to group together related requirements, and identifies where they can be found in the following sections.

Table 3: Requirement Digraphs

Digraph	Description	Section(s)	Table(s)
PS	Product Selection Requirements	Section 3	Table 4
SR	Overall Solution Requirements	Section 4.1	Table 5
CR	Configuration Requirements for All DAR Components	Section 4.2	Table 6
SW	Requirements for SWFDE Components	Section 4.3	Table 7
FE	Requirements for FE Components	Section 4.4	Table 8
PE	Requirements for PE Components	Section 4.5	Table 9
HW	Requirements for HWFDE Components	Section 4.6	Table 10
EU	Requirements for EUD	Section 4.7	Table 11
CM	Configuration Change Detection Requirements	Section 4.8	Table 12
DM	Requirements for Device Management	Section 4.9	Table 13
AU	Auditing Requirements	Section 4.10	Table 14

Digraph	Description	Section(s)	Table(s)
KM	Key Management Requirements for All DAR Components	Section 4.11	Table 15
SC	Requirements for Supply Chain Risk Management	Section 4.12	Table 16
LF	Requirements for Lost and Found	Section 4.13	Table 17
GD	Requirements for Use and Handling of Solutions	Section 5.1	Table 18
RP	Requirements for Incident Reporting	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.

Table 4: Product Selection Requirements

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-PS-1	The products used for the FE layer shall be chosen from the list of FE products on the CSfC Components List.	HF, SF, PF, RM	T=O		
DAR-PS-2	The products used for the SWFDE layer shall be chosen from the list of SWFDEs on the CSfC Components List.	HS, SF, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-PS-3	The Inner and Outer DAR layers shall 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, RM	T=O		
DAR-PS-4	(Moved to DAR-SC-2)				
DAR-PS-5	The cryptographic libraries used by the Inner and Outer DAR layers shall be independently developed and implemented.	HF, HS, SF, PF, RM	O	Optional	
DAR-PS-6	The products used for the PE layer shall be chosen from the list of PE products on the CSfC Components List under the Mobile Platform section.	PF	T=O		
DAR-PS-7	The products used for the HWFDE layer shall be chosen from the list of HWFDEs on the CSfC Components List.	HF, HS, RM	T=O		
DAR-PS-8	The Operating System used shall be approved by the General Purpose OS Protection Profile (OS PP).	HF, HS, SF	O	Optional	

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.

4.1 Overall Solution Requirements

Table 5: Overall Solution Requirements

Req #	Requirement Description	Solution Designs	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 shall be changed or removed.	SF, PF, HF, HS, RM	T=O		
DAR-SR-2	The DAR solution shall 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 Program Management Office (PMO) shall be contacted.	SF, PF, HF, HS, RM	T=O		
DAR-SR-3	Each DAR component shall have a unique account for each user.	SF, PF, HF, HS	O	Optional	
DAR-SR-4	All EUDs shall remain in continuous physical control at all times, as defined by the AO.	HF, HS, SF, PF, RM	T=O		
DAR-SR-5	The AO shall provide guidance when CE should be implemented.	HF, HS, PF, SF, RM	O	Optional	
DAR-SR-6	The AO shall provide procedures for performing CE.	HF, HS, PF, SF, RM	O	Optional	
DAR-SR-7	At least one layer shall use a trusted platform module for cryptographic key storage.	HF, HS, SF	O	Optional	
DAR-SR-8	If the Lost and Found use case is implemented, then the Lost and Found requirements (Table 17) shall be implemented.	SF, PF, HF, HS	T=O		

4.2 CONFIGURATION REQUIREMENTS FOR ALL DAR COMPONENTS

Table 6: Configuration Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-CR-1	Default encryption keys shall be changed.	SF, PF, HF, HS, RM	T=O		
DAR-CR-2	Primary user authentication credential values for each DAR layer mechanism type shall 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, RM	T=O		
DAR-CR-3	DAR components shall use algorithms for encryption selected from Table 1.	SF, PF, HF, HS, RM	T=O		
DAR-CR-4	Each DAR component shall prevent further authentication attempts after a number of failed attempts defined by the AO.	SF, PF, HF, HS, RM	O	Optional	
DAR-CR-5	Each DAR layer shall perform a CE after a number of consecutive failed logon attempts as defined by the AO.	SF, PF, HF, HS, RM	O	Optional	
DAR-CR-6	Each DAR component shall locally generate its own symmetric encryption keys on the EUD.	SF, PF, HF, HS, RM	T=O		
DAR-CR-7	Each DAR component shall permit only an administrator to disable the DAR component.	SF, HF, HS, PF, RM	O	Optional	
DAR-CR-8	All components shall have DAR protections enabled at all times after provisioning.	SF, PF, HF, HS, RM	T=O		
DAR-CR-9	All components shall encrypt all classified data. (Refer to CP Section 5.2 for additional information on FE.)	SF, PF, HF, HS, RM	T=O		
DAR-CR-10	All CSfC components shall 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, RM	T=O		

DAR-CR-11	Users shall be restricted to designated user folders.	SF, HF	T=O		
DAR-CR-12	For use in high threat environments (as defined by the AO) the two layers of DAR shall use different primary authentication factors (e.g., 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, RM	T=O		
DAR-CR-13	For use in routine threat environments (as defined by the AO) the two layers of DAR shall use different primary authentication factors (e.g., 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, RM	O	Optional	
DAR-CR-14	At least one DAR layer shall use multi-factor authentication.	HF, HS, SF, RM	O	Optional	
DAR-CR-15	The removable media shall not be bootable.	RM	T=O		

4.3 REQUIREMENTS FOR SWFDE COMPONENTS

Table 7: Requirements for SWFDE Components

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-SW-1	The SWFDE shall use Cipher Block Chaining (CBC) for data encryption.	SF, HS, RM	T	DAR-SW-2	
DAR-SW-2	The SWFDE shall use XTS or Galois/Counter Mode (GCM) for data encryption.	SF, HS, RM	O	DAR-SW-1	
DAR-SW-3	The SWFDE shall be configured to use one of the following primary authentication options:	SF, HS, RM	T=O		

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

4.4 REQUIREMENTS FOR FE COMPONENTS

Table 8: Requirements for FE Components

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-FE-1	The FE product shall use CBC for data encryption.	SF, PF, HF, RM	T	DAR-FE-2	
DAR-FE-2	The FE product shall use XTS for data encryption.	SF, PF, HF, RM	O	DAR-FE-1	
DAR-FE-3	The FE product shall use one of the following primary authentication options: • A randomly generated or user-generated passphrase or password defined by the AO that meets minimum strength set in CP Appendix D. or	SF, PF, HF, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
	• An external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1.				

4.5 REQUIREMENTS FOR PE COMPONENTS

Table 9: Requirements for PE Components

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-PE-1	The PE shall enable the "wipe sensitive data" management function for imported or self-generated keys/secrets and/or other classified data.	PF	T=O		
DAR-PE-2	The PE shall use CBC for data encryption.	PF	T	DAR-PE-3	
DAR-PE-3	The PE shall use XTS or Galois/Counter Mode (GCM) for data encryption.	PF	O	DAR-PE-2	
DAR-PE-4	The AO shall provide policy to the user determining when data or keys must be wiped.	PF	T=O		
DAR-PE-5	The PE product shall use one of the following primary authentication options: 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.	PF	T=O		

4.6 REQUIREMENTS FOR HWFDE COMPONENTS

Table 10: Requirements for HWFDE Components

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-HW-1	The HWFDE shall use CBC for data encryption.	HF, HS, RM	T	DAR-HW-2	
DAR-HW-2	The HWFDE shall use GCM or XTS for data encryption.	HF, HS, RM	O	DAR-HW-1	
DAR-HW-3	The HWFDE shall be configured to use one of the following primary authentication options: • A randomly generated passphrase or password that meets the minimum strength set in CP Appendix D Password/Pasphrase Strength Parameters or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or • A combination of both of the above.	HF, HS, RM	T=O		

4.7 REQUIREMENTS FOR END USER DEVICES

Table 11: Requirements for End User Devices

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-1	All EUD provisioning shall be performed through direct physical access.	SF, PF, HF, HS, RM	T=O		

Req #	Requirement Description	Solution Designs	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 shall 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, RM	T=O	(DAR-LF-3 if LF use case is implemented)	
DAR-EU-3	EUDs shall implement the Basic Input/Output System (BIOS) security guidelines specified in NIST SP 800-147.	SF, PF, HF, HS	O	Optional	
DAR-EU-4	All users shall sign an organization-defined user agreement before being authorized to use an EUD.	SF, PF, HF, HS, RM	T=O		
DAR-EU-5	All users shall receive an organization-developed training course for operating an EUD prior to use.	SF, PF, HF, HS, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-6	At a minimum, the organization-defined user agreement shall 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, RM	T=O		
DAR-EU-7	External USB tokens and smartcards, when used for authentication, shall be removed from the EUD upon or before shut down in accordance with AO policy.	SF, PF, HF, HS, RM	T=O		
DAR-EU-8	AO shall provide guidance on storing and/or securing authentication factors.	SF, PF, HF, HS, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-9	The SA shall disable system power saving states on EUDs (i.e., sleep and hibernate).	SF, HF, HS	T=O		
DAR-EU-10	The EUD shall power off after a period of inactivity defined by the AO.	SF, HF, HS	T=O		
DAR-EU-11	The EUDs shall be provisioned within a physical environment certified to protect the highest classification level of the data stored on the device.	SF, PF, HF, HS, RM	T=O		
DAR-EU-12	The EUD shall only be re-provisioned to the same or higher classification level of the classified data per an AO approved process.	SF, PF, HF, HS, RM	T=O		
DAR-EU-13	The EUD shall be reported as “lost” when out of continuous physical control as specified by the AO. Alternate requirement DAR-LF-2 can only be used if all LF requirements are implemented.	SF, PF, HF, HS, RM	T=O		
DAR-EU-14	System folders shall have user write permissions disabled unless authorized by an administrator.	SF, HF	T=O		
DAR-EU-15	The EUD shall be protected with anti-tamper measures.	SF, PF, HF, HS, RM	O	Optional	
DAR-EU-16	The device shall 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 shall be rebooted again before use.	HF, HS, PF, SF	T=O		
DAR-EU-17	The absence of any expected authentication prompt(s) shall be reported as possible tampering to the AO.	HF, HS, PF, SF, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-18	When data is no longer needed, it shall be overwritten or erased by secure erase tool per AO guidance. (See section 4.10)	HF, HS, PF, SF, RM	O	Optional	
DAR-EU-19	The EUD, when not in use outside of a secured facility, shall be kept in an AO-approved locked container.	HF, HS, PF, SF, RM	O	Optional	
DAR-EU-20	The BIOS/Unified Extensible Firmware Interface (UEFI) shall be configured to require a password before continuing the boot process.	HF, HS, SF	O	Optional	
DAR-EU-21	All DAR FDE components shall be cryptographically erased before being provisioned again.	HF, HS, SF, RM	T=O		
DAR-EU-22	All DAR components shall be cryptographically erased before being provisioned again.	PF	O	Optional	
DAR-EU-23	System folders shall have user write permissions disabled unless authorized by an administrator.	PF	O	Optional	
DAR-EU-24	The EUD shall enable the BIOS/UEFI password.	HF, HS, SF	O	Optional (DAR-LF-6 if LF use case is implemented)	
DAR-EU-25	If the user suspects the EUD has been compromised, the EUD user shall obtain authorization from their AO prior to use.	HF, HS, PF, SF, RM	O	Optional (DAR-LF-11 if LF use case is implemented)	

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-EU-26	Each EUD shall be personalized by the end user. (This should not violate any other security features.)	HF, HS, PF, SF, RM	O	Optional (DAR-LF-12 if LF use case is implemented)	
DAR-EU-27	A removable media EUD shall not be used as a smart card/USB Authentication Token if it is also storing encrypted user data.	RM	T=O		
DAR-EU-28	The device shall be removed from a host system before being handled by an unauthorized party (e.g., customs).	RM	T=O		

4.8 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 12: Configuration Change Detection Requirements

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-CM-1	A history of baseline configuration for all components shall be maintained by the SA.	SF, PF, HF, HS, RM	T=O		
DAR-CM-2	An automated process shall ensure configuration changes are logged.	SF, PF, HF, HS, RM	O	Optional	
DAR-CM-3	Log messages generated for configuration changes shall include the specific changes made to the configuration.	SF, PF, HF, HS, RM	O	Optional	
DAR-CM-4	A history of baseline configuration for all components shall be available to the auditor.	SF, PF, HF, HS, RM	T=O		
DAR-CM-5	Configuration change logs shall be kept for an AO defined period of time.	SF, PF, HF, HS, RM	T=O		

4.9 REQUIREMENTS FOR DEVICE MANAGEMENT

Table 13: Requirements for Device Management

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-DM-1	EUDs shall be physically administered.	SF, PF, HF, HS, RM	T	DAR-DM-2	
DAR-DM-2	EUDs shall be remotely administered using an NSA-approved DIT protection solution (e.g., NSA Certified Product or CSfC approved solution).	SF, PF, HF, HS	O	DAR-DM-1	
DAR-DM-3	Administration workstations shall be dedicated for the purposes given in the CP.	SF, PF, HF, HS	T=O		
DAR-DM-4	Administration workstations shall physically reside within a protected facility where CSfC solution(s) are managed.	SF, PF, HF, HS	T=O		
DAR-DM-5	Administration workstations shall be physically separated from workstations used to manage non-CSfC solutions.	SF, PF, HF, HS	T=O		
DAR-DM-6	Only authorized SAs (See Section 12 of the CP) shall be allowed to administer the DAR Components.	SF, PF, HF, HS, RM	T=O		

4.10 AUDITING REQUIREMENTS

Table 14: Auditing Requirements

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-AU-1	EUDs shall be inspected for malicious physical changes in accordance with AO defined policy.	SF, PF, HF, HS, RM	T=O	DAR-LF-7	

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-AU-2	The EUDs shall 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, RM	O	Optional	
DAR-AU-3	Auditors shall review audit logs for a time period as defined by the AO.	SF, PF, HF, HS, RM	T=O		
DAR-AU-4	Auditors shall physically account for the EUDs after an AO-defined time period.	SF, PF, HF, HS, RM	T=O		
DAR-AU-5	Administrators shall periodically compare solution component configurations to a trusted baseline configuration after an AO-defined time period.	SF, PF, HF, HS, RM	O	Optional	

4.11 KEY MANAGEMENT REQUIREMENTS

Table 15: Key Management Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-KM-1	The key sizes used for each layer shall be as specified in Table 1.	SF, PF, HF, HS, RM	T=O		
DAR-KM-2	DAR solution products shall be initially keyed within a physical environment certified to protect the highest classification level of the DAR solution.	SF, PF, HF, HS, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-KM-3	The DAR solution shall disable all key recovery mechanisms.	SF, PF, HF, HS, RM	T=O		
DAR-KM-4	The algorithms used for each layer shall be as specified in Table 1.	SF, PF, HF, HS, RM	T=O		

4.12 Supply Chain Risk Management Requirements

Table 16: Supply Chain Risk Management Requirements

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-SC-1	CSfC Trusted Integrators shall be employed to architect, design, procure, integrate, test, document, field, and support the solution.	SF, PF, HF, HS, RM	O	Optional	
DAR-SC-2	Each component selected from the CSfC Components List shall 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.)	HF, HS, SF, PF, RM	T=O		

4.13 Lost and Found Requirements

All of the following requirements must be met in order to implement the Lost and Found use case. The Lost and Found use case covers the scenario where an EUD has been recovered after having been out of continuous physical control (as defined by the AO) and the user wants to reuse the device. 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. The LF use case is also prohibited when using removable media for DAR protection as explained in Section 4.5 above.

Table 17: Lost and Found Requirements

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-LF-1	Organizational-developed training shall include guidance on tamper awareness and detection.	HF, HS, PF	T=O		
DAR-LF-2	The EUD shall be reported as "compromised" when tampered with, as defined by AO policy, is suspected.	HF, HS, PF	T=O	Replaces EU-13	
DAR-LF-3	The EUD and/or non-volatile storage media, if found after compromise, shall 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.)	HF, HS, PF	T=O	Replaces DAR-EU-2	
DAR-LF-4	The two layers of DAR shall use different primary authentication factors (i.e., One layer may use a password but the second layer would need to use a token).	HF, HS	T=O		
DAR-LF-5	EUDs shall use boot integrity verification technology. (see glossary)	HF, HS	T=O		
DAR-LF-6	The EUD shall enable the BIOS/Unified Extensible Firmware Interface (UEFI) password.	HF, HS	T=O	Replaces DAR-EU-24	
DAR-LF-7	Prior to reuse, the EUD shall undergo tamper detection inspection as established by the AO to determine if the device has been tampered with or substituted.	HF, HS, PF	T=O		
DAR-LF-8	The EUD, when outside of a secured facility and not in use, shall be kept out of view.	HF, HS, PF	T=O		
DAR-LF-9	If an unauthorized party takes the EUD out of sight or performs	HF, HS, PF	T=O		

	unknown operations the device shall be considered compromised.				
DAR-LF-10	When using commercial modes of travel (i.e., non-secure), the EUD shall stay with the traveler and not be placed in checked baggage.	HF, HS, PF	T=O		
DAR-LF-11	If the user suspects the EUD has been compromised, the EUD user shall obtain authorization from the official appointed by the AO or local policy prior to use.	HF, HS, PF	T=O	Replaces DAR-EU-25	
DAR-LF-12	Each EUD shall be personalized by the end user. (This should not violate any other security features.)	HF, HS, PF	T=O	Replaces DAR-EU-26	

5 REQUIREMENTS SOLUTION OPERATION, MAINTENANCE, & HANDLING

5.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

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

Table 18: Requirements for the Use and Handling of Solutions

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-GD-1	Acquisition and procurement documentation shall not include information about how the equipment will be used, including that it will be used to protect classified information.	SF, PF, HF, HS, RM	T=O		
DAR-GD-2	The solution owner shall 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, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-GD-3	The AO will ensure that a compliance audit shall be conducted every year against the latest version of the DAR CP.	SF, PF, HF, HS, RM	T=O		
DAR-GD-4	Results of the compliance audit shall be provided to and reviewed by the AO.	SF, PF, HF, HS, RM	T=O		
DAR-GD-5	When a new, approved version of the DAR CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months.	SF, PF, HF, HS, RM	T=O		
DAR-GD-6	Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or fewer) months (see Section 12.3 of the CP).	SF, PF, HF, HS, RM	T=O		
DAR-GD-7	The SA, auditor, user, and all Integrators shall be cleared to the highest level of data protected by the DAR solution.	SF, PF, HF, HS, RM	T=O		
DAR-GD-8	The SA and auditor roles shall be performed by different people.	SF, PF, HF, HS, RM	T=O		
DAR-GD-9	All SAs, users, and auditors shall meet local information assurance training requirements.	SF, PF, HF, HS, RM	T=O		
DAR-GD-10	Users shall report lost or stolen EUDs to their ISSO or chain of command as defined by the AO.	SF, PF, HF, HS, RM	T=O		
DAR-GD-11	Only SAs or CSfC Trusted Integrators shall perform the installation and policy configuration.	SF, PF, HF, HS, RM	T=O		

Registration ID:

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-GD-12	Security critical patches (such as Information Assurance Vulnerability Alert (IAVAs)) shall be tested and subsequently applied to all components in the solution in accordance with local policy and this CP.	SF, PF, HF, HS, RM	T=O		
DAR-GD-13	Local policy shall dictate how the SA will install patches to solution components.	SF, PF, HF, HS, RM	T=O		
DAR-GD-14	All DAR components shall be updated using digitally signed updates provided by the vendor.	SF, PF, HF, HS, RM	T=O		
DAR-GD-15	All authorized users shall have the ability to CE keys for both layers.	SF, PF, HF, HS, RM	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, RM	T=O		
DAR-GD-17	Withdrawn				
DAR-GD-18	Withdrawn				
DAR-GD-19	AO shall define loss of continuous physical control for each use case. This definition shall 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, RM	T=O		

5.2 REQUIREMENTS FOR INCIDENT REPORTING

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 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	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, RM	T=O		
DAR-RP-2	Report any malicious configuration changes to the DAR components.	SF, PF, HF, HS, 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, RM	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, RM	T=O		

Req #	Requirement Description	Solution Designs	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-RP-5	Confirmed incidents meeting the criteria in DAR-RP-1 through DAR-RP-4 shall 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, RM	T=O		
DAR-RP-6	At a minimum, the organization shall 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, RM	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	T/O	Alternative	Compliance (Explain how your solution meets this requirement)
DAR-TR-1	The organization implementing the CP shall perform all tests listed in the DAR CP Testing Annex.	HF, HS, PF, SF, RM	T=O		