Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS “FOR OFFICIAL USE ONLY” OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

This page left blank intentionally

Cargo Security Network Access Device (NAD) Requirements

Version 1.0

U.S. Department of Homeland Security (DHS)
Science and Technology Directorate (S&T)
Cargo Security Test and Evaluation (CSTE)

Document Number CM/CS/SSC/SNL/REQ/R1.0/2010/1782
December 6, 2010

Point of Contact:
DHS Science and Technology Cargo Security Program Manager
Kenneth Concepcion
Kenneth.Concepcion@dhs.gov
(202) 254-5351

Container Security Test and Evaluation Team

Lawrence Livermore National Laboratory

Pacific Northwest National Laboratory

Sandia National Laboratories

Space and Naval Warfare Command System Center San Diego

United States Department of Homeland Security
Science and Technology Directorate

Cargo Security Integrated Test and Evaluation Program

Technical Document Disclaimer

This document presents scientific and technical data resulting from testing and evaluation activities performed within the Science & Technology (S&T) Borders and Maritime Cargo Security Integrated Test and Evaluation Program (CSTE). Where possible, CSTE testing is performed in accordance with national or international consensus standards. When testing is performed for federal acquisition programs, test criteria are derived from systems requirements for the acquisition program. In other cases, test criteria are based on CSTE technical expertise and the U.S. Government's anticipated future mission requirements.

System performance results presented herein reflect the best efforts of the CSTE technical staff, but they neither guarantee nor endorse the suitability of the system for untested applications or other system requirements. Federal, state, local, or tribal agencies seeking to use this report as source selection criteria in an acquisition action must evaluate this report against their specific mission requirements.

This report does not constitute a federal endorsement of any tested system. Use of this report in whole or in part for commercial Vendor advertising and marketing materials is strictly forbidden, and no permission for such use will be granted.

Table of Contents

List of Figures

List of Tables

1 Introduction

This Department of Homeland Security (DHS) document provides system and technical requirements for Security Device System Network Access Devices (NADs).

The primary purpose of a NAD is to enable communication between Cargo Security System Components (CSSCs) and Data Consolidation Points (DCPs), generally to retrieve data from, and, issue commands to the CSSC.

The term *Cargo Security System Component (CSSC)* as used herein encompasses the following device types: Advanced Container Security Device (ACSD), Container Security Device (CSD), Electronic Chain of Custody (ECoC) Device, and Marine Asset Tag Tracking System (MATTS) Device. Note that all CSSCs are on-conveyance[1] devices.

DCPs receive data from, and, issue commands to CSSCs. At least one DCP will be designated by DHS to be the generic end-point for CSSC-originated messages and DCP responses. This DHS-designated DCP must be trusted and able to en/decrypt and authenticate.

NADs complete the picture by providing, enabling, and enhancing command, control, and communication functionality between DCPs and CSSCs. Different NAD types allow different levels of access and command (not all NADs can perform all NAD tasks). NADs in general can:

1. Identify CSSCs that are within their RF communication range
2. Establish a wireless network connection with the identified CSSCs
3. Deliver command messages and acknowledgements from the DCP to the CSSC
4. Acquire and transport Status Messages and Event Logs from the CSSC to the DCP

Non-secure NADs generally act as simple transparent wireless bridges, while secure NADs support an interface that enables the user to issue CSSC commands and view downloaded CSSC data on the NAD. Some NADs are fixed in place as stationary read points; others are battery-powered and handheld for use by individual users.

ACSDs and CSDs as a group are referred to as *Security Devices*, as introduced in [1]. The primary purpose of a Security Device is to monitor the doors of an ISO 688 Dry Container for opening or removal while in transit from the Point of Stuffing (PoS) through a Container Security Initiative (CSI) port to a Port of Arrival (PoA), and finally to a Point of Deconsolidation (PoDC) in the United States. The Advanced CSD also monitors the sides, top, bottom, and doors of the container for any type of intrusion, including penetration.

The primary purpose of the ECoC system is to provide a secure method of monitoring opening and closing of a mechanical locking device and to track the location of cargo being moved from one secure facility to another. Cargo transport modes include air, truck, rail, and ship.

The primary purpose of MATTS is to provide a secure communication link suitable for monitoring conveyance sensor and security systems from one secure facility to another. The MATTS communications system incorporates External and Embedded Communications Modules (ECMs and CMs), Fixed and Handheld NADs (FNADs and HNADs), and DCPs.

[1] For the purposes of this document, a *conveyance* is an ISO 668 Dry Shipping Container, motor carrier trailer, or comparable rail enclosure.

2 Purpose

This document provides the requirements for NADs and is intended for vendors of Security Device System components who are developing NAD elements.

3 Document Precedence

This document addresses requirements specific to secure and non-secure NADs. All requirements pertaining to NADs that may be contained within other Security Device System Requirements Documents are applicable; however, in the event of conflict between those documents and this one, this document has precedence with respect to NAD capabilities, operations and functions.

4 Types of Network Access Device

Network Access Devices (NADs, a.k.a. "readers") include both fixed and handheld devices as described in [2]. A Network Access Device (NAD) is any appropriate mix of hardware, software, network services, and internal interfaces that satisfies the requirements specified for compatible Wireless Personal Area Networks (WPANs), including functionality, user interface, and error detection/correction. NADs have multiple physical configurations to support fixed installations, arming operations, backhaul communications, and mobile inspection activities.

NADs intended to support networks of CSSCs and DCPs need to be interoperable with all CSSCs and DCPs. There are three types of NAD: *non-secure*, *secure*, and, *arming-only*. Non-secure NADs transparently pass messages *verbatim* between CSSCs and DCPs as part of an untrusted network and are used to meet communication requirements not requiring intervention by a human agent. Secure NADs possess authorizing credentials allowing their users to issue Restricted Commands (see [1]) and access log files and encrypted messages in the same fashion as a DCP (see [2] and [3]). Secure NADs are intended to be in continuous possession and complete control of a DHS-designated Security Agent and are most likely to be portable but not required to be so. Access to DCP-issued encryption keys determines whether a NAD is secure or non-secure. A third type of NAD is the *Arming-only NAD*, which must be able to generate *only* Unrestricted, Arming, and Commissioning CSSC Commands per [1] and view only limited CSSC status information. The Arming-only NAD is not expected to be in the continuous control of a DHS-designated Security Agent and therefore is not considered a secure NAD.

Portable NADs are referred to herein as *Handheld NADs* (HNADs), and NADs installed semi-permanently in fixed locations are referred to as *Fixed NADs* (FNADs). NADs can also be implemented as subsystems integral to MATTS Devices (referred to as *host devices* herein) to provide Cellular or Satellite connection to IP services. Such integral NADs are referred to as *Embedded NADs*. Embedded NADs and Arming NADs are always considered non-secure NADs. Whether a NAD is Handheld or Fixed is essentially independent of whether it is designated as secure or non-secure.

All NADs must have the capability to communicate with a DCP per this document and [3]. Non-secure NADs must also be able to communicate wirelessly with a CSSC per [2]. Secure NADs must provide all functional capabilities of non-secure NADs and also provide:

1. Secure communications with a DCP
2. Ability to authenticate to DCP for download of encryption keys
3. Cargo Operator Interface for issuing Restricted and Unrestricted Commands (note that a Secure NAD may be limited by CSSC device type as to what commands are valid).

5 NAD Usability Requirements

5.1 Volumetric Size

The volume of the HNAD **Shall Not** exceed 100 cubic inches (1639 cubic centimeters). The volumes of FNADs and Embedded NADs **May** be determined by the Vendor.

5.2 Weight

The total weight of the HNAD and battery **Shall Not** exceed 3 lbs (1.36 kilograms). The weight of FNADs and Embedded NADs **May** be determined by the Vendor.

5.3 NAD Operating System

All NADs **May** use any operating system chosen by the vendor.

5.4 NAD Display

The view screens of all NADs incorporating view screens **Shall** be readable in bright daylight. NADs designed for outdoor use, **Shall** have a display readable in daylight.

5.4.1 NAD Display Lifetime

NAD displays **Should** be designed to withstand prolonged use in direct sunlight over a minimum period of two years.

5.4.2 NAD Display Indicators

If a display is utilized, NADs **Shall** provide the following display indicators:

1. Available volatile and nonvolatile memory on the NAD.
2. Data items residing in the Transmission Queue.
3. Messages indicating that credentials have been added to or deleted from the secure NAD.
4. Hardware, firmware, and software version numbers for the NAD upon request to do so.

5.4.3 NAD Display Update

All NADs with a user interface **Shall** update their displays not less than once every three (3) seconds (subject to delays caused by user interface operations) to reflect the most recent Status Message sent from a CSSC.

5.5 NAD Export, Licensing, and Compliance

The NAD and all components thereof **Shall** be exportable according to U.S. Law and applicable laws of countries with which the U.S. has active trade relations.

All NADs **Shall** be operational in the global supply chain without foreign government usage restrictions, with consideration of the following:

1. Human factors engineering
2. Usage within the intermodal cargo-handling environment

3. Operating, training and work environments for NADs with user interface, consistent with the global supply chain

The Vendor **Shall** identify and provide proof of compliance with all applicable licenses, permits, and contract agreements impacting these requirements.

5.6 NAD Clock

All NADs **Shall** maintain clock time to within 1 seconds of UTC.

5.7 NAD Power

All FNADs **Shall** support local power standards. All HNADs **Shall** be powered by a re-chargeable and replaceable battery with at least 8 hours of use in Operational Mode with a full charge. The power supply characteristics for Embedded NADs are at the Vendor's discretion.

6 NAD Functional Requirements

6.1 Connected and Autonomous Operation

A secure NAD connected to the DCP:

1. **Shall** enable a Designated System Administrator (DSA) to log-in to the DCP
2. **Shall** enable a DSA who is logged-in to the DCP to download Encryption Key Records from the DCP.
3. **Shall** be able to transfer data verbatim from a CSSC to the DCP regardless of whether the Encryption keys for the CSSC have been downloaded.

If the secure NAD is operating autonomously (i.e., *not* connected to the DCP), it **Shall** support the ability to store CSSC data and upload the stored CSSC data to the DCP verbatim when subsequently connected to a DCP.

6.1.1 Secure NAD Mode Requirements

The secure NAD **Shall** operate in 2 Modes:

1. Operational Mode:
   - 1.1 The secure NAD in Operational Mode **Shall** be powered-on and ready to be operated by a user.
   - 1.2 The secure NAD **Shall** enable transition to the Powered-off Mode from the Operational Mode.
   - 1.3 Operational Mode **Shall** include three and only three sub-modes:
     - 1.3.1 Logged-In: A user has logged-in to the secure NAD
     - 1.3.2 Authenticated: A DSA has logged-in to the secure NAD and has been authenticated as a DSA by the DCP
     - 1.3.3 Logged-Out: No one is logged-in to the secure NAD
   - 1.4 Transition to the Logged-In sub-mode from the Logged-Out sub mode **Shall** require user completion of a Login Process.
   - 1.5 Transition to the Authenticated sub-mode **Shall** be possible only from the Logged-In sub mode and **Shall** require the following:
     - 1.5.1 The user **Shall** be authenticated as a DSA by the DCP.
     - 1.5.2 The user **Shall** be logged-in to the HNAD as a DSA.
   - 1.6 Transition to the Logged-out sub-mode **Shall** be possible from either the Logged-in sub mode or the Authenticated sub mode.
2. Powered-Off Mode
   - 2.1 The secure NAD **Shall** enable transition to the Operational Mode from the Powered-off Mode.

6.1.2 HNAD Mode Requirements

The HNAD **May** be capable of operating as a secure NAD, non-secure NAD or arming-only NAD.

6.1.2.1 Mode functionality and Data Storage for Secure NADs

Secure NAD functionality and data storage capabilities are dependent on the mode and

configuration of the NAD, as shown in overview in Table 6-1. Cells containing a checkmark (✓) indicate functionality and/or capability that **Shall** be available in the indicated mode (i.e., the mode in the leftmost column); cells containing "×" indicate functionality and/or capability that **Shall Not** be available in the indicated mode.

Table 6-1, Secure NAD Operational Configurations

	DCP Interface		CSSC Interface		User Interface	Data Storage	
Mode	Download Encryption Keys	Upload CSSC Data	Issue CSSC Commands	Receive CSSC Data	View CSSC Data	Store CSSC Data	Retain Encryption Keys
Operational Logged-In	×	✓	✓	✓	✓	✓	✓
Operational Authenticated	✓	✓	✓	✓	✓	✓	✓
Operational Logged-Out	×	×	×	×	×	✓	✓
Powered-Off	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	✓	×

Key: ✓ = Required, × = Disallowed, N/A = Not Applicable

6.1.3 User Classes, Privileges, and Processes for Secure NADs

The secure NAD **Shall**:

1. Maintain a record of users and their passwords to support the login function.
2. Support two classes of users: Operator and DSA.

The Operator **Shall** be able to use the secure NAD to:

1. Issue Restricted and Unrestricted CSSC commands
2. Download Secured CSSC Data from the CSSC to the secure NAD and view it
3. Upload Secured CSSC Data to the DCP

The DSA **Shall** have the capabilities of an Operator and **Shall** also be able to:

1. Manage secure NAD configuration and operational parameters
2. Create and manage secure NAD user accounts
3. Initiate download of Encryption Key Records to the secure NAD

The secure NAD **Shall** restrict NAD functions and operations to authorized users. Only one user **Shall** be allowed to login to the secure NAD at any given time. The secure NAD **Shall** provide a user interface to implement and support the process by which a DSA is authenticated to the DCP. Only one DSA **Shall** be allowed to authenticate to the DCP with a specific secure NAD at any given time.

Individual users **Shall** be automatically logged out of the secure NAD based on the Inactivity Timeout parameters which are set by the DSA. Individual users **Shall** have the ability to manually logout from the secure NAD.

6.1.4 CSSC Commands and Logs – All NADS

All NADs **Shall** be capable of transmitting commands to user-selected CSSCs.

6.1.5 CSSC Commands and Logs – Secure NADS

The secure NAD **Shall** be capable of issuing all valid Restricted and Unrestricted commands.

The secure NAD **Shall**:

1. Store all Event Logs received from the CSSCs
2. Be capable of storing a minimum of 20,000 combined Event Logs and Status Messages
3. Record hardware, firmware, and software version numbers specified in [4]
4. Record secure NAD user activity in the format and content specified in Section 6.3

Event Logs stored on the secure NAD **Shall Not** be subject to alteration or deletion by any user.

6.1.6 NAD-to-DCP Operational Requirements

The NAD **Shall** retain the following in non-volatile storage:

1. DCP IP Address
2. Port Number
3. LAN Gateway IP address
4. Subnet mask
5. NAD UID

These items **Shall** be programmable from the DCP in formats as described per [4].
The NAD **Shall** be configurable to connect with the DCP using either TCP or UDP protocols.
The NAD **Shall** be able to store a list of at least two DCP network IP addresses and two fully-qualified DCP domain names. The NAD **Shall** be able to automatically connect to a secondary DCP in the event that communication with a primary DCP is not possible. The NAD **Shall** establish a secure communication link to its assigned DCP as described in [4].

The NAD **Shall** relay encrypted CSSC status and log data to the DCP over the IP connection.
The NAD **Shall** receive and store encrypted commands from the DCP over the IP connection for later transmission to the CSSC.

The NAD **Shall** provide a Transmission Queue for data that is stored as messages waiting on the NAD to be uploaded to the DCP. The NAD **Shall** automatically upload all data in the Transmission Queue that has not been uploaded to the DCP, using the interface specified in [4].

All NADs **Shall** append a User Datagram Protocol (UDP) Header to CSSC Data before forwarding to a DCP as specified in [4].

The secure NAD **Shall** support download of Encryption Key Records from the DCP, singularly or in batch, per [3].

6.1.7 Secure NAD Command Interface Requirements

1. The secure NAD **Shall** enable a user to login and logout of the secure NAD.
2. The secure NAD **Shall** enable a user to manage data stored on the secure NAD, including CSSC Status Messages, secure NAD Activity Logs, and CSSC Event Logs.
3. The secure NAD **Shall** enable a user to view data stored on the secure NAD, including CSSC Status Messages, NAD Activity Logs, and CSSC Event Logs.
4. The secure NAD **Shall** be able to acquire Encryption Key Records
5. The secure NAD **Shall** enable a user to delete Encryption Key Records, this **Shall** be policy based and controlled by the DSA allowing support of site specific needs.

6. The secure NAD **Shall** enable a user to power-on and power-off the secure NAD.
7. The secure NAD **Shall** enable a user to initiate discovery of CSSCs in the secure NAD's RF communications range.
8. The secure NAD **Shall** enable a user to select individual CSSCs from a list of CSSCs within the communications range.
9. The secure NAD **Shall** provide a command to select, parameterize, format and send commands to selected CSSCs.
10. The secure NAD **Shall** be able to upload data to the DCP either automatically or via a user-initiated backup process.
11. The secure NAD **Shall** be able to download Encryption Key Records from the DCP.
12. The secure NAD **Shall** enable a user to login and be authenticated by the DCP.
13. The secure NAD **Shall** enable a user to logout from the DCP.

6.1.8 Encryption Key Record Management

The secure NAD **Shall** be capable of storing no less than 20,000 Encryption Key Records, as described in [3].

When Encryption Key Records are downloaded to the secure NAD, the secure NAD **Shall** append Encryption Key Records to the current list of Encryption Key Records.

The secure NAD **Shall** delete Encryption Key Records from the secure NAD upon any of the following conditions:

1. Expiration of individual Encryption Key records, based on expiration date parameter(s) in the Encryption Key Record.
2. On user command to delete Encryption Key Records.
3. The secure NAD enters Powered-Off Mode.
4. If the secure NAD fails or loses power, then Encryption Key Records **Shall** be cleared.

6.1.9 NAD Security Requirements

The NAD **Shall** ensure that NAD program code cannot be modified, replaced, or deleted except by the Vendor. The plaintext of any CSSC Status Message or Event Log **Shall Not** be accessible to unauthorized personnel during any NAD operational state. CSSC Encryption Keys **Shall Not** be accessible through any user interface.

6.2 Arming-Only NADs

6.2.1 Arming-Only NAD Functional Requirements

Figure 6-1 shows a notional example of the arming-only NAD configuration.

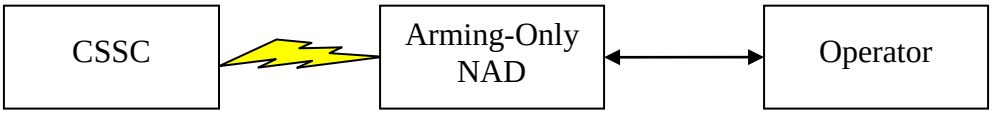

Figure 6-1, Arming-Only NAD Normal Operation

The arming-only NAD **Shall** be capable of possessing a time-sensitive encryption key provided by the DCP suitable only for Arming and Commissioning of CSSCs and viewing limited CSSC status information. The arming-only NAD **Shall** append a standard 16-byte Message Header per [2] to the Command Payload before transferring a command message to the CSSC.

6.2.2 Arming-Only NAD Command Capability and Interface for CSSC Command

The arming-only NAD **Shall:**

1. Allow user Login
2. Allow user Logout
3. Provide the ability to power-on the arming-only NAD.
4. Provide the ability to power-off the arming-only NAD.
5. Be capable of issuing Arming and other unrestricted commands as described in [2].
6. Implement interfaces to transmit commands to user-selected CSSCs per [2].
7. Provide a command to discover CSSCs in its RF communications range per [2].
8. Provide a command to select individual CSSCs from a list of CSSCs within the communications range
9. Provide ability to upload data to the DCP either automatically or via a user-initiated backup process fully compliant with [4].

6.3 Secure NAD Activity Log

This section defines the requirements for the *secure NAD Activity Log* and the information it must contain. The *secure NAD Activity Log* is a record kept by the secure NAD of all activity it has processed. Formats for data transmitted between the secure NAD and DCP are found in [4]. Secure NAD Activity Logs are cleared and reinitialized only after transmission to the DCP, which will be accomplished only when the secure NAD is connected to the DCP. While the secure NAD is powered on, every valid Command executed and every CCSC Status Message received results in a secure NAD Activity Log Record.

1. When the secure NAD is powered-on, the Security Device **Shall** record Activity Log Records as entries in the Activity Log.
2. The secure NAD Activity Log data **Shall** be encrypted per [3] for transmittal to the DCP.
3. The secure NAD Activity Log **Shall** be transferred to the DCP per [4].
4. The secure NAD Activity Log entries **Shall** be sequentially ordered by time of the Activity Log event prior to encryption for transmittal to the DCP.
5. Each secure NAD Activity Log **Shall** be identified by the secure NAD UID.
6. Each secure NAD Activity Log **Shall** accommodate a minimum of 10,000 Activity Log Records.
7. The secure NAD Activity Log data **Shall Not** be alterable by the secure NAD user.
8. Each secure NAD Activity Log entry **Shall** include a monotonically increasing Activity Log Record Number associated with each Activity Log Record entry, starting with a value = 0 for the first Event Record entry.
9. The secure NAD Activity Log **Shall** be initialized as follows:

a. Event Number 0 in the Activity Log contains the secure NAD UID.
b. Event Number 1 in the Activity Log contains the Time and Date of the Encryption Key download from the DCP.

10. Each secure NAD Activity Log Record **Shall** include the following:
    a. The CSSC UID,
    b. The date of the event,
    c. The user ID of the person who logged into the secure NAD to execute the event,
    d. The command that was issued and the CSSC response.
11. Each of the following **Shall** generate a corresponding Event Record in the secure NAD Activity Log:
    a. Any CSSC Status Message received by the secure NAD.
    b. Any Security Device Command sent by the secure NAD successfully executed by the CSSC where the Event Data consists of the Command Payload and Command Header from the received command.
    c. Any Fault Detection by the secure NAD with the Event Data consisting of a vendor-defined fault code
12. All CSSC Commands listed in [2] that are successfully executed by the secure NAD **Shall** be recorded in the secure NAD Activity Log.
13. On secure NAD Activity Log overflow, the secure NAD **Shall** stop updating the Activity Log and leave existing Activity Log Records unchanged.
14. On secure NAD Activity Log overflow, the secure NAD **Shall** notify the user via the user interface.
15. The secure NAD Activity Log **Shall Not** be subject to alteration or deletion by the Operator.

7 Network Access Device Operational Requirements

7.1 NAD Physical and Logical Implementation

Requirements herein are not intended to specify a preferred implementation or configuration for any type of NAD. There are no requirements for a particular operating system, hardware chipset, or user interface. It is the vendor's responsibility to make the design decisions needed to satisfy the functional, interface, and operational requirements specified in herein and in [1] and [2]. All FNADs and HNADs **Shall** be assigned a 64-bit manufacturer-assigned unique identifier as a Device ID (UID). The vendor **Shall** be responsible for obtaining address space for their organization with the ID managing authority (IEEE EUI-64). The UID **May** be the 802.15.4 MAC address if it is IEEE coordinated as unique. This device UID **Shall** be unalterable by any agent other than the original device manufacturer.

7.2 Non-secure NAD Operations

There are three types of non-secure NADs: Fixed (FNADs), Handheld (HNADs), and Embedded NADs. Arming-only NADs may be either FNADs or HNADs. For all security functions, the non-secure NAD is considered transparent and part of the untrusted network. There is no login process required for either an non-secure FNAD or Embedded NAD. The non-secure NAD that is not an Arming-only NAD (see Section 6.2.2) **Shall** operate in two configurations:

1. Autonomous Configuration: The non-secure NAD is not connected to the DCP and can send only Unrestricted Commands and view only Unrestricted Status messages.
2. Connected Configuration: The non-secure NAD is connected to the DCP and transmits data verbatim between DCPs and CSSCs as described in Section 8.2 and in [2].

7.2.1 Non-secure NAD Overview of Operations

Non-secure FNADs and Embedded NADs are intended to support field operations as transparent, untrusted network devices via 802.15.4-2006, as described in [2]. The CSSC may use other available media, such as Cellular or Satellite networks, to provide additional field support. The non-secure NAD is to be used to support the field operation for CSSCs as depicted in Figure 7-1. The non-secure HNAD (includes Arming-only) does not require a real-time or persistent connection to the DCP in order to communicate with and operate a CSSC.

In the Autonomous Configuration, the non-secure NAD **Shall**:

1. Establish wireless communication with all CSSCs within the NAD's 802.15.4-2006-based RF range.
2. Allow the user to select specific CSSCs from those in range for subsequent individual interrogation and operation.
3. Retrieve and display the selected CSSC's Unrestricted Status data and execute that action if the user so indicates.
4. Display and offer to execute all available Unrestricted Commands through all modes and states where valid Unrestricted Command operations are possible per [2].

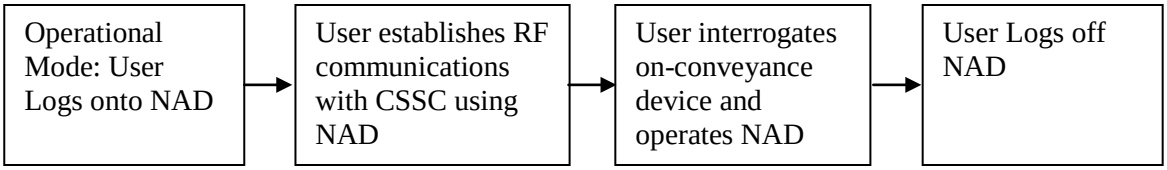

Figure 7-1, Non-secure NAD Operations with CSSCs

7.3 Non-secure NAD Utilization (Excludes Arming-only NADs)

Non-secure NADs **May** either include an integrated user interface (HNADs) or be entirely autonomous (FNADs and Embedded NADs).

Non-secure NADs intended by CONOPS to allow a user to issue Unrestricted Commands and read Unrestricted Status Messages must have an integral user interface that allows a user to select and execute these actions.

All Non-secure NADs **Shall** enable the user to:

1. Query and receive data from CSSCs
2. Store and display CSSC Non-secure Data
3. Issue Unrestricted Commands without real-time connection to a DCP

Non-secure FNADs and Embedded NADs act as transparent bridges for information moving between CSSCs and DCPs, as shown in Figure 7-2. Non-secure FNADs and Embedded NADs **Shall** transmit status and command data verbatim between CSSCs and DCPs.

Non-secure NADs **Shall Not** be able to decrypt Secured Status messages or generate Restricted Commands. Which commands are Restricted and Unrestricted and what information is Secured and Non-secure is described in [2].

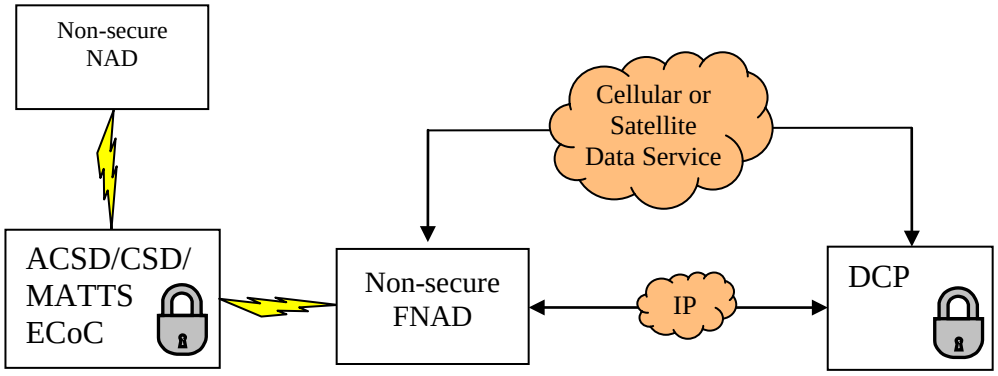

Figure 7-2, Non-secure NAD Notional Overview (without Embedded NAD)

7.3.1 Non-secure NAD Designated System Administrator Functions

The non-secure FNAD and Embedded NAD have no required DSA Functions. The non-secure HNAD **Shall** implement the following DSA Functions:

1. Account access management limiting HNAD to one user at a time
2. Maintenance of user access passwords

3. Assignment of user access privileges
4. Maintenance of user access records

The capability to maintain and manage user accounts **May** be provided via a NAD application. The DSA may use this NAD application to maintain and manage user accounts.

7.3.2 CSSC and NAD Communication

All communication between CSSCs and NADs **Shall** be conducted per [2]. Communication interfaces between Embedded NADs and host devices are at the vendor's discretion.

7.3.3 CSSC Operation

All CSSCs operations using non-secure NADs for security purposes are conducted per [2].

7.3.4 User Record Retention

The non-secure NAD **Shall** retain its user records when it is powered-off.

7.4 Secure NAD Operations

Secure NADs are expected to be physically protected when not in use, and, when in use, should be operated only by DHS-designated Security Agents. The intended implementation and use of secure NADs are as follows:

1. For all security functions, the secure NAD user interface requires a login to the secure NAD application(s) in order to operate the secure NAD application or external interface.
2. The secure NAD login process limits operators to those with user accounts previously set in the secure NAD by the DSA.

The Secure NAD operates in two configurations:

1. Autonomous Configuration: The secure NAD is not connected to the DCP and allows a logged-in user to send Restricted CSSC Commands and view secure CSSC messages for CSSCs whose encryption keys have been downloaded.
2. Connected Configuration: The secure NAD is connected to the DCP and can download CSSC encryption keys from the DCP and upload secure CSSC data NAD logs to the DCP. Connection may be via IP (using direct Ethernet connection or cradle) or wireless links (such as 802.11.x)

7.4.1 Secure NAD Overview of Operations

The secure NAD is used by DHS-designated Security Agents to support the field operation of conveyances equipped with CSSCs as depicted in Figure 7-3. The secure NAD does not require a real-time or persistent connection to the DCP in order to communicate with and operate a CSSC. The secure NAD does, however, require a secure connection as described in [4] to download the CSSC-specific encryption key from a DCP that enables it to read status and log files from, and successfully send secure commands to, that CSSC.

The secure NAD in the Autonomous Configuration **Shall** allow the user to:

1. Establish wireless communications with multiple CSSCs within the local RF range of the secure NAD.

2. Select specific CSSCs for interrogation and operation.
3. Acquire and display CSSC status data
4. Generate commands to operate the CSSCs through all modes and states and/or to alter CSSC Trip Information.

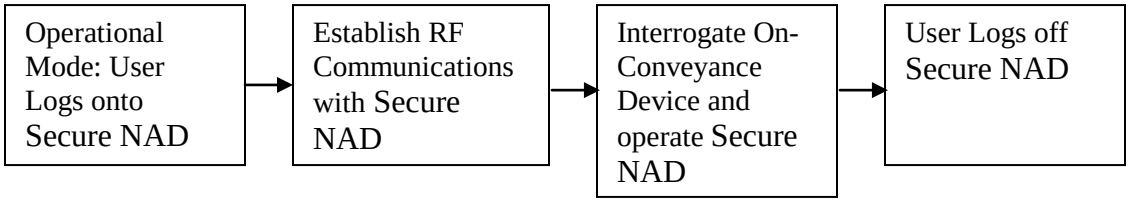

Figure 7-3, Secure NAD Operations with CSSCs

7.5 Secure NAD Utilization

Secure NADs are used by DHS-designated Security Agents to communicate with CSSCs attached to conveyances traveling throughout the global supply chain, as shown in Figure 7-4. All secure NADS have a user interface. The secure NAD **Shall** enable one and only one user to be logged-in at any given moment. The secure NAD capabilities defined in this section apply ONLY to Government Security Operations and are not applicable to commercial uses.

All secure NADs **Shall** provide the logged-in (and thereby authorized) user the ability to:

1. Query and receive data from the CSSCs
2. Transmit status and command data verbatim between a CSSC and a DCP
3. Store and view all CSSC non-secure and secure Data
4. Issue Unrestricted Commands without real-time connection to a DCP
5. Issue Restricted Commands without real-time connection to DCP, with exception of Rekey commands.
6. Store and view CSSC Encrypted Security Data
7. Upload secure NAD Activity Logs and other information to the DCP
8. Download Encryption Key and Key Records from the DCP

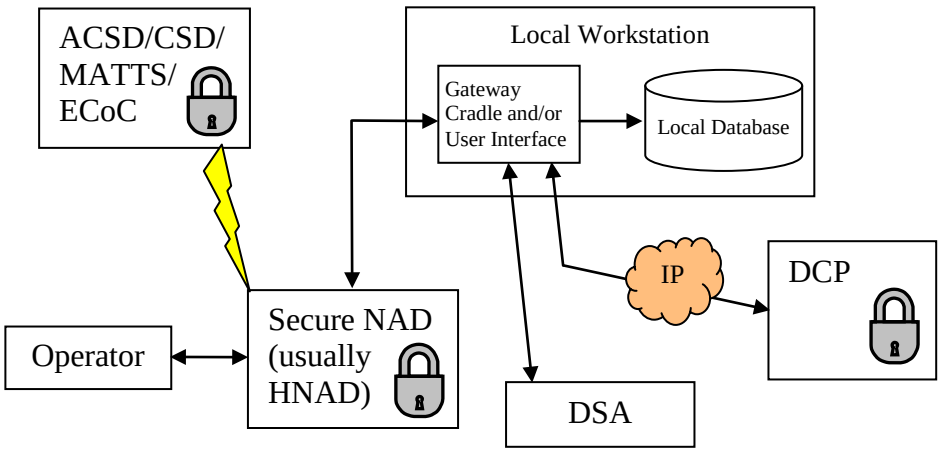

Figure 7-4, Secure NAD System Notional Overview

The secure NAD **May** support other functional capabilities, subject to the restrictions specified in this document. The presence of additional commercial-purposed functionality in the secure NAD **Shall Not** compromise the security requirements and access control requirements specified in this or related Security Network documents including [1] – [4].

7.5.1 Secure NAD Designated Systems Administrator Functions

The secure NAD must provide application interfaces and functionality to manage user accounts and operational parameters as specified below. Figure 7-5 displays an overview of the DSA's operations. A secure NAD DSA is a privileged account that would have similar capabilities to a computer system administrator. This user would be able to allow new authorized Operators to the NAD. DSA privileges may be different depending on the specific CONOPs.

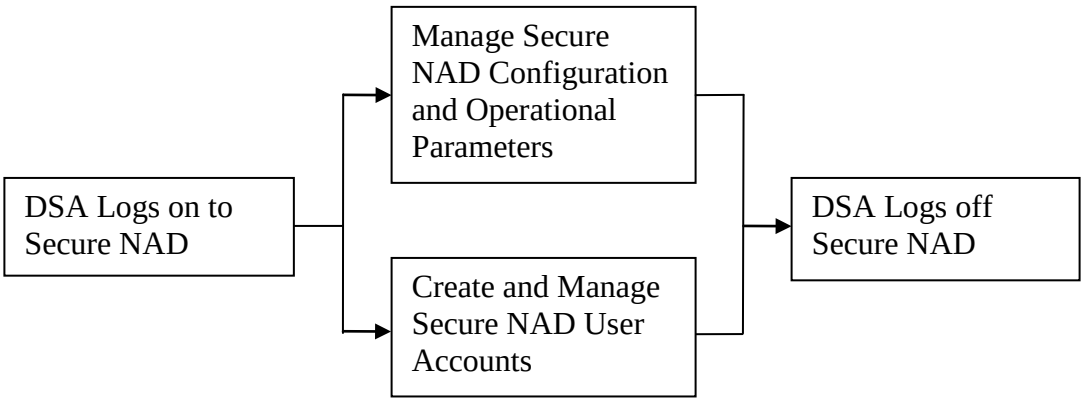

Figure 7-5, Secure NAD DSA Operations

7.5.1.1 Secure NAD DSA Authentication

The DCP supports CSSC operations, including those involving the secure NAD. Authentication to the DCP is a process that occurs at the DCP.

1. The secure NAD **Shall** provide a user interface that allows a user to execute the process of authentication as a DSA to the DCP.
2. The secure NAD **Shall** allow user access to DCP services requiring DSA-level authentication if and only if the user has successfully completed the process of authentication to the DCP.

7.5.1.2 Secure NAD DSA Operational and Configurable Parameters

Secure NADs **Shall** be configurable and support the following operations:

1. A user logs-in to the secure NAD.
2. The DSA defines and manages the primary and secondary DCP addresses per [4] that the secure NAD will use for uploading data and downloading the Encryption Key Records.
3. The DSA sets and/or changes secure NAD parameters such as the Inactivity Timeout value. Additional parameters may be needed to support specific CONOPs; this is not intended to be a comprehensive list.

7.5.1.3 Secure NAD Creation and Management of User Accounts

The secure NAD **Shall** allow a user logged-in as a DSA to:

1. Create, destroy, and modify user accounts by specifying the user names
2. Create and reset the password for each user account.
3. Establish the privileges assigned to each user account on an account-by-account basis.

7.5.2 Secure NAD CSSC Device Discovery

Communication between the CSSC and a secure NAD is initiated per [2]. Once communication has been established with all in-range CSSCs:

1. The secure NAD **Shall** display a list of CSSCs currently within range of the secure NAD that **Shall** include the CSSC UID and Operating Mode (armed/unarmed) of each CSSC.
2. The secure NAD **Shall** display the CSSC Alarm Status for each CSSC for which the secure NAD has the encryption key.

7.5.3 Secure NAD CSSC Operation

1. The secure NAD user interface **Shall** allow the user to select specific CSSCs for operation.
2. The secure NAD **Shall** allow the user to send Unrestricted Commands from the secure NAD to a CSSC selected in (1) above.
3. The secure NAD **Shall** allow the user to send Restricted Commands from the secure NAD to a CSSC selected in (1) above if and only if the secure NAD has the applicable encryption keys for those specific CSSCs.

7.5.4 Secure NAD Log-Off

1. The secure NAD **Shall** allow the user to log-off the secure NAD.
2. The secure NAD **Shall** retain user credentials and encryption keys until the secure NAD is powered-off.
3. The secure NAD **Shall** retain user credentials and encryption keys during periods of low power operation or system time-outs that support battery/power conservation strategies.

7.5.5 Secure NAD Connected Configuration

1. When the secure NAD is connected to the DCP, the secure NAD **Shall** provide all the functionality of the Autonomous Configuration and can also upload data to the DCP.
2. The secure NAD **Shall** provide DSA s the same capability to upload data to the DCP, but also **Shall** allow download of encryption keys (see Figure 7-6).

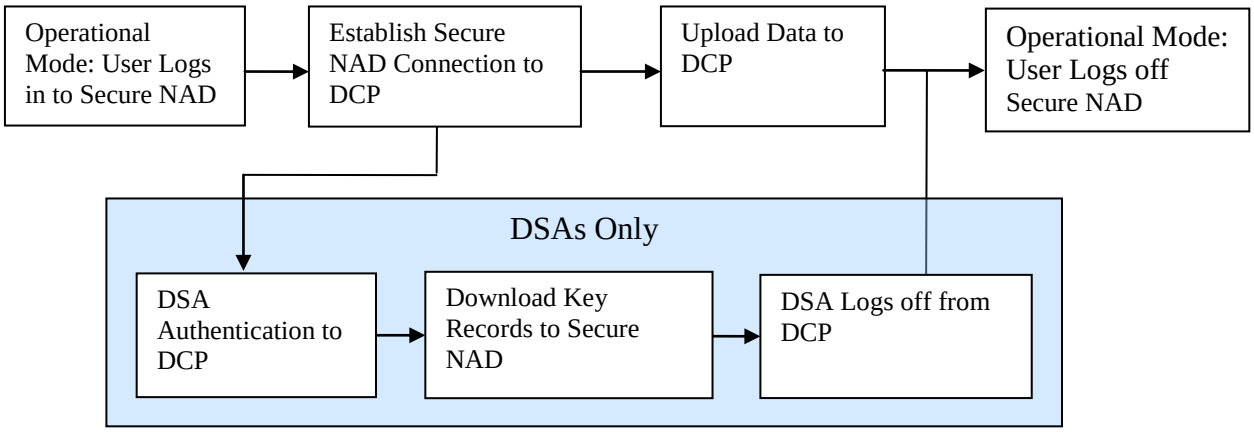

Figure 7-6, Support of Secure NAD Operations with DCP

7.5.6 Secure NAD Data Upload

On successful connection to a DCP, the secure NAD **Shall** automatically upload stored CSSC log data from the secure NAD to the DCP per [4]. The upload process will transmit to the DCP all status and logs previously acquired and not yet transmitted. The secure NAD **Shall Not** alter in any way Encrypted Event Log Content from CCSCs when uploading the Content from the secure NAD to the DCP. The secure NAD **Shall** append the appropriate message header information on all information uploaded to the DC as described in [2].

7.5.7 Secure NAD Download of Encryption Keys

The ability to view CSSC secure Data and execute Restricted Commands requires knowledge of the applicable CSSC credentials.

1. The secure NAD **Shall** provide a user interface that allows a user to create and manage credentials, record requests, and downloads between the secure NAD and the DCP.
2. The secure NAD **Shall** support two methods for acquiring keys from the DCP:
   a. The secure NAD **Shall** receive direction from DCP to download to the secure NAD Encryption Key Records that the DCP has ready for transmittal.
   b. The secure NAD **Shall** request that the DCP download to the secure NAD one or more specific Encryption Key Records indicated by user-selected CSSC UIDs or Conveyance IDs.

7.5.8 Secure NAD Log-off from DCP

When the DSA has completed all of the necessary data operations between the secure NAD and DCP, the secure NAD **Shall** allow the DSA to log-off from the DCP and terminate the secure connection. After log-off from the DCP is complete, users may operate the secure NAD using the Autonomous Configuration in support of CSSC operations.

7.5.9 User Log-off from Secure NAD

1. The secure NAD **Shall** have a log-off mechanism allowing the user to log-off the secure NAD application.
2. The secure NAD **Shall** retain the current Encryption Key Records until the secure NAD is powered-off.

3. The secure NAD **Shall** automatically log-off the current secure NAD user if the user interfaces are inactive at or beyond a timeout period adjustable by a DSA.

7.6 Arming-Only NAD Utilization

Arming-only NADs are used to support the secure arming of CSSCs at remote cargo stuffing facilities where full functioning secure NADs are not required. All arming-only NADS have a user interface. The arming-only NAD capabilities defined in this section apply to ONLY Government Security Operation minimums and are not applicable to commercial uses.

All arming-only NADs **Shall** provide the authorized user the ability to:

1. Query Status and Arm the CSSCs.
2. Forward Status and command data verbatim to and from a DCP.
3. Store Encryption Keys for CSSCs.
4. Issue Unrestricted Commands without real-time connection to a DCP.

8 Interface Requirements

All NADs except Embedded NADs **Shall** have a wireless interface that implements the RF communications and data protocols to communicate with CSSCs. Non-secure FNADS, Embedded NADs and all secure NADs require network-based communications to communicate with the DCP. All secure NADs as well as non-secure NADs also have an operational user interface to control and manage the NAD functions, interface configurations and applications.

8.1 CSSC Interface

All NADs **Shall** be compliant with all of the requirements of [2] including message structure, commands and data formats. For FNADs and HNADs (i.e. NADs that are not Embedded NADs), the NAD-to-CSSC interface **Shall** use bi-directional wireless RF communications as the primary communications mode (See [2]). For Embedded NADs the interface to the host device is at the Vendor's discretion but **Shall** be compliant with all the requirements of [2].

8.2 DCP Interface

All NADs **Shall** be capable of communicating with the DCP over IP-based communication network per [3] and **Shall** be compliant with all the requirements of [3].

8.3 User Display and Command Interface

All forms of HNADs **Shall** provide an interface to enable the user to conduct operations with the CSSCs and the DCP as described in this document. The user interface of all other types of NADs (if any) **Shall** be at the discretion of the Vendor.

8.4 Alternative Interfaces for Commercial Purposes

The Vendor **May** choose to implement alternative interfaces in order to satisfy vendor-specific commercial needs that are beyond the scope of this document. Any alternative interfaces chosen **Shall Not** compromise the data security of the CSSCs.

8.5 Arming-Only NADs

Arming-only NADs **Shall** have the capability to issue commands to CSSCs which include the Arming command (i.e., Restricted Arm with Trip Information command) and all unrestricted commands as described in [2]. This allows arming-only NADs to be used to arm devices at the start of a trip, but they are not capable of issuing other restricted commands and have access to encryption keys in such a way that only Arming and Commissioning are enabled. The arming-only NAD **Shall Not** be capable of issuing all other restricted commands identified in [2]. The DSA Functions **May** be as those described in Section 7.4.1 of this document.

Arming-only NADs **Shall** allow the user to:

1. Establish wireless communications with multiple CSSCs within the local RF range of the NAD as described in [2].
2. Provides the ability to select specific CSSCs for interrogation and operation.
3. Acquire and display Unrestricted Status data
4. Generate Arming, Unrestricted or commercial-purposed commands to operate the CSSC.

The user issues an arming-only NAD command to initiate CSSC communications. The arming-only NAD **Shall** respond to this command by transmitting the Network Access Device Announcement (NADA) to CSSCs within communications range, per [2]. The arming-only NAD displays a list of CSSCs currently within its communications range. The list **Shall** include the each CSSC UID, Conveyance ID and Operating Mode.

The user interface of the arming-only NAD **Shall** allow the user to select specific CSSCs for operation. The arming-only NAD **Shall** allow the user to send Arming or other Unrestricted Commands from the arming-only NAD to any CSSC selected.

9 Communications Requirements

9.1 NAD to CCSC

All NADs **Shall** fully support the communications requirements described in [2].

9.1.1 Network Discovery

Al NADs **Shall** provide programmable Network Access Device Announcement (NADA) transmission repetition rates (e.g. number of NADAs transmitted per second).

All NADs **Shall** be capable of transmitting NADAs at programmable time intervals indicated in the NADA Delay Coding Message Option Bits identified in [2].

All NADs **Shall** be capable of transmitting not less than 50 Network Access Device Announcement (NADA) messages as described in [2] at 20-millisecond intervals over a one (second) time period.

9.1.2 Data Formats

All NADs **Shall** be capable of supporting the data formats for wireless communications with CSSCs detailed in [2].

9.1.3 Messaging Protocols

All NADs **Shall** implement the MAC, Network and Application Layer Protocols for wireless communications with CSSCs described in [2].

9.2 NAD to DCP

9.2.1 Network Discovery

All NADs **Shall** fully implement the NAD-to-DCP Commissioning Process described in [4] as either a secure or non-secure NAD.

9.2.2 Data Formats

All NADs **Shall** be capable of supporting the data formats detailed in [4].

9.2.3 Messaging Protocols

All NADs **Shall** be capable of supporting the NAD to DCP networking requirements of [4].

10 Environmental Requirements

The following two sections describe the specific environmental requirements for FNADs and HNADs. It is assumed that all Embedded NADs must meet the environmental requirements of the specific devices they have been embedded within. For example, ECoC devices will have Embedded NADs and the ECoC device must meet ECoC device environmental requirements which therefore serve as the environmental requirements of the embedded NAD.

For additional information about specific standards see the following:

- IEC 60068 (Environmental Testing):
  - 60068-1
  - 60068-2-2, -2-5, -2-6, -2-9, -2-10, -2-11, -2-14, -2-18, -2-27, -2-30, -2-31, -2-33, -2-38, -2-39, -2-47, -2-57, -2-59, -2-61, -2-64, -2-68, -2-75, -2-77, -2-78, -2-80,
  - 60068-3-8
- IEC 60533 (Electrical and Electronic Installations in Ships – Electromagnetic Compatibility)
- IEC 60721 (Classification of Environmental Conditions)
  - 60721-1
  - 60721-3-2, -3-6, -3-7
  - 60721-4-61
- IEC 61000 (Electromagnetic Compatibility)
  - 61000-1-1, -1-2
  - 61000-2-5, -2-7
  - 61000-4-2, -4-3, -4-4, -4-6, -4-8, -4-9, -4-17
  - 61000-6-2
- ANSI C63.4-2003 (Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz)
  - C63.4-8, -13, -Annex D
- NAVSEA OP 3565/NAVAIR 16-1-529 Volume 2, Sixteenth Revision; June 1, 2007.

10.1 Environmental Requirements for FNADs

The following is a list of the environmental conditions any Fixed Network Access Device (FNAD) is expected to meet. It is reduced from the comprehensive set of system environmental parameters since a Fixed NAD is not expected to operate in all scenarios and environments in which a Security Device would operate. An FNAD is assumed to be a commercial device. Therefore, only operating characteristics and conditions are addressed in these requirements. Environments related to the transport of the Fixed NAD to the installation location have been determined to be the responsibility of the vendor. Packaging of equipment to arrive intact at the destination location is outside the scope of these requirements. The primary reference for operational environment requirements is *IEC 60721-3-4, Classification of groups of environmental parameters and their severities – Stationary use at non-weather protected locations*.

1. The Fixed NAD **Shall** continue to Operate in the environmental conditions listed below. Additionally, the Fixed NAD **Shall** satisfy all technical requirements as found in the applicable document (Security Device Requirements [1], MATTS Requirements [5]).

Temperature and Humidity:

2. Temperature: The Fixed NAD **Shall** Operate in the temperature range as occurs in the global ports environment, such as the -40°C to +55°C, from *IEC 60721-3-4 Table 1, Classification of climatic conditions, Class 4K4*, with the low end adjusted to -40°C instead of -65°C to address temperature environments at port installation locations. This class covers use at locations which are not weather-protected and are directly exposed to the Worldwide Group of Open-air Climates, up to and including Extremely Cold and Extremely Warm Dry climate types.
3. Thermal Shock: The Fixed NAD **Shall** Operate when subjected to the rapid temperature changes as occur in the global ports environments, such as the following temperature changes from *IEC 60721-3-4, Table 1 – Classification of climatic conditions, Class 4K4, 0.5°C/min.*
4. Humidity: The Fixed NAD **Shall** Operate at humidity levels that occur in the global ports environments, including 100% relative humidity over the temperature range from -65°C to +55°C from *IEC 60721-3-4, Table 1, Classification of climatic conditions, Relative humidity, Class 4K4.*

Structural Vibration and Mechanical Shock Environments:

5. Shock: The Fixed NAD **Shall** Operate during and after shock events that occur in the global ports environments. Such shocks are exemplified by drops that are equivalent to a three-foot handling drop, such as may occur during installation.
6. Vibration: The Fixed NAD **Shall** Survive when exposed to vibrations that occur in the global ports environments. Such scenarios include stationary random vibration events that are equivalent to the following levels from *IEC 60721-3-4, Table 6 – Classification of mechanical conditions, Stationary vibration, sinusoidal, Class 4M4,* which applies to locations where transmitted vibration from machines or passing vehicles is experienced.
    a. 3 mm displacement from 2-9 Hz
    b. 10 m/s^2 from 9-200 Hz

Precipitation Environments:

For all of the following precipitation environments, it is assumed that when devices have some measure of weather protection (such as covers, lids, protective plugs for external ports), they will be employed during evaluation of performance under these environmental conditions.

7. Salt Mist: The Fixed NAD **Shall** Operate when exposed to salt mist as it occurs in the global ports environments, such as that specified in IEC 60721-1, Table 1, Subsection 3.1, Chemically active substances, *Sea salt* (conditions of air) which lists 0.3 g/m^3 with a modified time limit of 24 hours instead of 96 hours. This time period is used to simulate total accumulated exposure over a much longer period of time, as it is unlikely the device will be cleaned both internally and externally on a daily basis to remove such potential contamination.
8. Rain: The Fixed NAD **Shall** Operate when exposed to rain as it occurs in the global ports environments, such as at a rate of 15 mm/min from IEC 60721-3-4, Table 1, *Classification of climatic conditions, Precipitation, rain,* Class 4K4.

9. Frost/Ice: The Fixed NAD **Shall** Operate when exposed to frost and ice as it occurs in the global ports environments, such as per IEC 60721-1, Table 1, Subsection 1.10, *Formation of ice and frost,* intensity of 3mm/h.
10. Sand and Dust: The Fixed NAD **Shall** Operate when exposed to sand and dust as it occurs in the global ports environments, such as 300 mg/m^3 sand and 20 mg/(m^2 x h) dust sedimentation from IEC 60721-3-4, Table 5, *Classification of mechanically active substances, Sand in air and Dust sedimentation,* Class 4S2. This class applies to use at locations in areas with sand or dust sources, including urban areas. The test criteria applied is blowing dust and sand, coarse dust, 1 g/m^3 concentration, duration 2 hours, air velocity of 10 m/s.

Radiation and Electromagnetic Environments:

11. Radiated Emissions:
    a. The Fixed NAD radiated emissions **Shall Not** exceed the limits given in 47 CFR Part 15 (FCC Rules on radio frequency devices).
    b. The Fixed NAD radiated emissions **Shall Not** exceed the emission limits for equipment installed in industrial environments, from IEC 61000-6-4, Table 1, consolidated in the table below.

Frequency Range	**Limits**
30 MHz – 230 MHz 230 MHz – 1000 MHz	40 dBμV/m, quasi-peak at 10m 47 dBμV/m, quasi-peak at 10m
0.15 MHz – 0.5 MHz 0.5 MHz – 30 MHz	97 dBμV - 87 dBμV, quasi-peak 84 dBμV - 74 dBμV, average 87 dBμV, quasi-peak 74 dBμV, average

Table 10-1: Power output limits over defined frequency ranges.

    c. The Fixed NAD radiated emissions (communications) **Shall** be characterized to determine the safe separation distances for HERO SAFE (<10 ft), HERO UNSAFE, HERO UNRELIABLE, and HERO SUSCEPTIBLE ORDANCE. The safe separation distance is calculated based on the average transmitter power, antenna gain, and operational frequency. See *NAVSEA OP 3565/NAVAIR 16-1-529, Volume 2 Sixteenth Revision* for field strength/distance general equations and HERO curves.

12. Radiated Susceptibility: The Fixed NAD **Shall** Operate when exposed to radiated emissions as occur in the global ports environments, such as power-frequency magnetic fields and radio-frequency magnetic fields as detailed below.
    a. Power-frequency magnetic field of 30A/m from 30 Hz to 2 kHz, from *IEC 61000-6-2, Table 1 – Immunity – Enclosure ports, subsection 1.1, Power-frequency magnetic field* (incorporating guidance from *IEC 61000-4-8 Table 1 – Test levels for continuous field,* and *Annex C, Class 3 with frequencies adjusted to fit application*).
    b. Radio-frequency electromagnetic fields at 30 V/m from 9 kHz to 27 MHz , at 10 V/m from 27 to 1000 MHz , and at 10 V/m from 1GHz to 40 GHz, from *IEC 61000-6-2, Table 1 – Immunity – Enclosure ports, subsections 1.2 – 1.4, Radio-frequency electromagnetic field* (incorporating guidance from *IEC 61000-2-5 Annex A, Class Type 2,* and *IEC 61000-4-3 Section 5 Annex E, Class 2 adjusted values to fit application*).

13. Static Electricity: the Fixed NAD **Shall** Operate after being subjected to electrostatic contact discharge as it occurs in the global ports environments, such as +/- 4kV and +/- 8kV contact discharge and +/- 15kV air discharge, from *IEC 61000-6-2, Table 1 – Immunity – Enclosure ports, subsection 1.5, Electrostatic discharge*.

14. Nearby Lightning: the Fixed NAD Shall operate after being subjected to nearby lightning environment as it occurs in the global ports environments, such as a nearby (100m) lightning strike with a peak current amplitude of 30kA having a transient magnetic field with a peak of 50 A/m, per *IEC 61000-4-9 Table 1, Test Levels, Level X, and Annex C, Class 3 Environment.*

10.2 Environmental Requirements for HNADs

The following is a list of the environmental conditions any Handheld NAD is expected to meet. It is reduced from the comprehensive set of system environmental parameters since a Handheld NAD is not expected to operate in all scenarios and environments that a CSD or ACSD device would operate. Operating characteristics and conditions for Handheld NADs are addressed in these requirements. Environments related to the transport of the Handheld NAD to the installation location have been determined to be the responsibility of the vendor. Packaging of equipment to arrive intact at the destination location is outside the scope of these requirements. The primary reference for the requirements is *IEC 60721-3-7, Classification of groups of environmental parameters and their severities – Portable and non-stationary use*.

1. The Handheld NAD **Shall** continue to Operate in the environmental conditions listed below. Additionally, the Handheld NAD **Shall** satisfy all technical requirements as found in the applicable document (CSD Requirements, ACSD Requirements, MATTS Requirements).

Temperature and Humidity:

2. Temperature: The Handheld NAD **Shall** Operate in the temperature range as occurs in the global ports environment, such as the -25°C to +70C, from *IEC 60721-3-7 Table 1, Classification of climatic conditions, Class 7K3*. This class covers use at, or transfer between, totally or partially weather protected locations in buildings of any construction, situated in geographical areas with Warm Temperate, Warm Dry, Mild Warm Dry, Extremely Warm Dry, Warm Damp, and Warm Damp Equitable[2] climate types, as well as use at, or transfer between, non weather protected locations which are directly exposed to an open-air climate covered by the Restricted Group of Open-Air Climates. This class was chosen because it is not likely to be left out in the open and it will likely reside in a Booth, a Vehicle, or similar protected area, and will be exposed to the open-air environment only when actually in use for inspections.
3. Thermal Shock: The Handheld NAD **Shall** Operate when subjected to the rapid temperature changes as occur in the global ports environments, such as the following temperature changes from *IEC 60721-3-7, Table 1 – Classification of climatic conditions, Class 7K3*:

[2] While it would seem that -25°C is Cold, the climate types listed are those as specified in the IEC specifications of global climatic types.

- from 0°C to -25°C in 4 minutes maximum,
- from -25°C to 0°C in 4 minutes maximum,
- from 0°C to 30°C in 4 minutes maximum, and
- from 30°C to 0°C in 4 minutes maximum.

4. Humidity: The Handheld NAD **Shall** Operate at humidity levels that occur in the global ports environments, including 95% relative humidity[3] over the temperature range from -25°C to +70°C from *IEC 60721-3-7, Table 1, Classification of climatic conditions, Relative humidity, Class 7K4*.

Structural Vibration and Mechanical Shock Environments:

5. Shock: The Handheld NAD **Shall** Operate during and after shock events that occur in the global ports environments. Such scenarios include drops that are equivalent to a three-foot handling drop, from *IEC 60721-3-7, Table 6, class 7M2 Mechanical Conditions – Non-stationary vibration, including shock, Spectrum Type II*, where the spectrum is shocks with medium duration and medium peak acceleration and Free Fall.

6. Vibration: The Handheld NAD **Shall** Survive when exposed to vibrations that occur in the global ports environments. Such scenarios include stationary random vibration events that are equivalent to the following levels from *IEC 60721-3-7, Table 6 – Classification of mechanical conditions, Stationary vibration, random, Class 7M1*. This class applies to use at, and direct transfer between, locations with only low-level vibrations, or with medium-level shocks.
   a. 1 m^2/s^3 from 10-200 Hz
   b. 0.3 m^2/s^3 from 200-2000 Hz

Precipitation Environments:

For all of the following precipitation environments, it is assumed that any supplied Handheld NAD weather protection measures (e.g., covers, lids, protective plugs for external ports) will be employed during evaluation of performance under these environmental conditions.

7. Salt Mist: The Handheld NAD **Shall** Operate when exposed to salt mist as it occurs in the global ports environments, such as that specified in *IEC 60721-3-7, Table 4, Chemically active substances, Sea salts (conditions of air), Class 7C2*. Use *IEC 60721-1, Table 1, Chemically active substances, Sea salts, severity 0.3 g/m^3* with a modified time limit of 24 hours instead of 96 hours. This time period is used to simulate total accumulated exposure over a much longer period of time, as it is unlikely the device will be cleaned both internally and externally on a daily basis to remove such potential contamination.

8. Rain: The Handheld NAD **Shall** Operate when exposed to rain as it occurs in the global ports environments, such as at a rate of 6 mm/min from *IEC 60721-3-7, Table 1, Classification of climatic conditions, Precipitation, rain, Class 7K4*. Duration 10 minutes.

9. Frost/Ice: The Handheld NAD **Shall** Operate when exposed to frost and ice as it occurs in the global ports environments, per *IEC 60721-3-7, Table 1, Classification of climatic conditions, Formation of frost and ice, Class 7K4*. Use *IEC 60721-1, Table 1, Section*

[3] Relative humidity, if set at the high temperature, will increase as the temperature falls due to the temperature-state properties of water and air.

1.10, Formation of ice and frost, intensity of 3mm/h for conditions of surrounding medium, air, duration 1 hour.

10. Sand and Dust: The Handheld NAD **Shall** Operate when exposed to sand and dust as it occurs in the global ports environments, such as 300 mg/m^3 sand and 20 mg/(m^2 x h) dust sedimentation from *IEC 60721-3-7, Table 5, Classification of mechanically active substances, Sand in air and Dust sedimentation, Class 7S2*. This class applies to use at, and direct transfer between, locations in close proximity to sand or dust sources. Test criteria applied is blowing dust and sand, coarse dust, 1 g/m^3 concentration, duration 2 hours, air velocity of 10 m/s.

Radiation and Electromagnetic Environments:

11. Radiated Emissions:
    a. Handheld NAD radiated emissions **Shall Not** exceed the limits given in *47 CFR Part 15 – FCC Rules on radio frequency devices*.
    b. Handheld NAD radiated emissions **Shall Not** exceed the emission limits for enclosure-port type (please see [1], Appendix B for specifics on enclosure ports) equipment installed in the bridge and deck zone of a ship or in the general power distribution zone of a ship, from *IEC 60533, Tables 2 and 3*, consolidated in the table below.

Frequency Range	**Limits**
150 kHz to 300 kHz	80 dBμV/m to 50 dBμV/m
300 kHz to 30 MHz	52 dBμV/m to 34 dBμV/m
30 MHz to 2 GHz	54 dBμV/m
Except 156 MHz to 165 MHz	24 dBμV/m

Table 10-2: Emission Limits over defined frequency ranges measured at distance of 3 meters.

    c. Handheld NAD radiated emissions (communications) **Shall** be characterized to determine the safe separation distances for HERO SAFE (<10 ft), HERO UNSAFE, HERO UNRELIABLE, and HERO SUSCEPTIBLE ORDANCE. The safe separation distance is calculated based on the average transmitter power, antenna gain, and operational frequency. See *NAVSEA OP 3565/NAVAIR 16-1-529, Volume 2 Sixteenth Revision* for field strength/distance general equations and HERO curves.

12. Radiated Susceptibility: The Handheld NAD **Shall** Operate when exposed to radiated emissions as occur in the global ports environments, such as power-frequency magnetic fields and radio-frequency magnetic fields as detailed below.
    a. Power-frequency magnetic field of 30A/m from 30 Hz to 2 kHz, from *IEC 61000-6-2, Table 1 – Immunity – Enclosure ports, subsection 1.1, Power-frequency magnetic field* (incorporating guidance from *IEC 61000-4-8 Table 1 – Test levels for continuous field*, and *Annex C, Class 3 with frequencies adjusted to fit application*).
    b. Radio-frequency electromagnetic fields at 30 V/m from 9 kHz to 27 MHz , at 10 V/m from 27 to 1000 MHz , and at 10 V/m from 1GHz to 40 GHz, from *IEC 61000-6-2, Table 1 – Immunity – Enclosure ports, subsections 1.2 – 1.4, Radio-frequency electromagnetic field* (incorporating guidance from *IEC 61000-2-5 Annex A Class*

Type 2 and *IEC 61000-4-3 Section 5 and Annex E, Class 2 adjusted values to fit application*).

13. Static Electricity: the Handheld NAD **Shall** Operate after being subjected to electrostatic contact discharge as it occurs in the global ports environments, such as +/- 4kV and +/- 8kV contact discharge and +/- 15kV air discharge, from *IEC 61000-6-2, Table 1 – Immunity – Enclosure ports, subsection 1.5, Electrostatic discharge*.

11 NAD Certification

All NADs will be independently evaluated by DHS before being certified for use. Qualitative factors, such as ease of use, clear, readable and intuitive user interfaces, minimization of the likelihood of human error, documentation quality, message displays, and system responsiveness will be assessed by DHS before certification is granted. DHS reserves the right to deny or withdraw approval of any NAD at any time.

12 Appendix C – Red Team Vulnerability Assessment

12.1 DHS Vulnerability Testing Overview

After a device is developed and the vendor has performed their own tests to ensure that the device meets all the requirements, they will submit a Supply Chain Certificate Application to DHS for approval. If the application is accepted, then DHS will need devices/systems as specified in the application to perform vulnerability tests. DHS vulnerability tests will include red team assessments, which are described in more detail in this section. A device's ability to operate securely in a system is of importance because when devices are designed, they are designed with the ability to function as a part of a system. Red team tests are system tests where the device under test is evaluated based on its interactions with other devices within a system; this could include, but is not limited to, environmental and external communication stimuli. For the purpose of this appendix the reader should note that a device could be assessed as a part of a system of devices.

12.2 Background

The DHS Container Security Test and Evaluation (CSTE) Team performs red team assessments for devices. A red team assessment is an evaluation that makes use of consequences, adversarial level, and successful exploitation of identified vulnerabilities. Red team testing is performed from the perspective of an attacker with malevolent intentions. Six steps in the red team testing process are described in more detail below.

A red team test can build on an initial defeat test. Defeat testing is usually restricted to the vulnerability/consequence path with the highest probability of success. A red team assessment, which pursues multiple attack paths requires a greater amount of time and resources. The specific tests performed during red teaming are not predetermined because they must be based upon the technologies involved. However, there are defined processes for selection and validation of tests. Some of the goals of red teaming are to identify multiple attack paths graded by level of adversary, identify critical points of failure, and identify the strengths and weaknesses of a device. The results of these tests allow for a better understanding of the risks associated with using the corresponding device in the maritime cargo handling environment. Results of red team tests can also be used by DHS to better determine the posture of international cargo security.

12.3 Objectives

The purpose of defeat testing is to identify high consequence, easily exploitable vulnerabilities. It is designed to find simple attacks that will circumvent a critical component or function of the device. The information obtained will be helpful in identifying how difficult it is to defeat the device, the capabilities an adversary needs to defeat the device, and the amount of time and effort required. Defeat testing provides a decision point on whether or not to pursue additional Red Teaming, which would consider a more sophisticated adversary as well as additional consequences of concern. Defeat testing is designed to:

1. Explore potential vulnerabilities
2. Determine whether a security device can be defeated by an adversary with minimal resources

3. Identify a high consequence vulnerability that can be exploited by a low to medium level adversary
4. Identify attributes of the attack such as the amount of time and effort required to accomplish the task

The purpose of a red team test is to determine if a device can be defeated by a program-specified level of adversary. The information obtained will be helpful in identifying how difficult it is to defeat the Device, the necessary capabilities of an adversary to complete the defeat, and the amount of time and effort required to accomplish the defeat. Red teaming is designed to:

1. Identify multiple attack paths graded by level of adversary
2. Identify critical points of failure
3. Identify the strengths and weaknesses of a device
4. Determine whether a device can be defeated by a program-specified level of adversary

12.4 Red Team Methodology

According to the Information Design Assurance Red Team (IDART) ™ methodology[4], red teaming consists of six steps: Planning, Data Collection, Characterization, Analysis, Reporting, and Demos and Experiments. More detail on each of these steps is given below.

12.4.1 Planning

During the planning phase, the red team seeks to bound the assessment problem, understand the threat space of concern, understand the significant mission elements of the device under evaluation, and understand what goals an adversary might attempt to achieve.

12.4.2 Data Collection

The data collection phase is typically done with cooperation of the customer to reduce the time spent in discovery and enhance the effort spent on analysis of the device architecture. Open-source information and customer/vendor provided information are used to gain device understanding. Defeat testing is done during this step as well.

Defeat testing is a subset of red teaming and usually occurs early on in the red team process. The purpose of defeat testing is to identify high consequence, easily exploitable vulnerabilities. It is designed to find simple attacks that will circumvent a critical component or function of the device. Defeat testing is performed using limited time and resources. For example, constraints could be $1,500 for materials, a few staff, and less than a week of development time. The bounds of a defeat test are, in general, budget, limits on resources for the attack, and level of adversary. Other constraints may include:

- Threat can represent either an insider or outsider
  - Successful outsider attacks are usually considered a more serious vulnerability
- Partially destructive tests will be avoided if possible
  - If a postulated destructive attack/vulnerability is considered serious it will be reported as such
- Modification of device and conveyance are within bounds

4 http://www.sandia.gov/idart/method.html

Defeat testing provides data collection, introductory views, and system understanding for in-depth red teaming. Upon discovery of one defeat, defeat testing could be considered successful; however, the defeat test guidelines specify formal repetition of tests to provide a more comprehensive understanding of the limits of the vulnerability. At the conclusion of a defeat test, a decision will be made about whether or not to proceed with the rest of the red team investigation. If further testing is recommended after the completion of a defeat test, the next two steps in the red team process will be completed.

12.4.3 Characterization

The device under study is characterized from several viewpoints in an effort to identify and understand single points of failure or high value nodes, or to identify passable security controls. Views may include physical views, logical views, functional views, network views, device views, lifecycle views, data flow views, protocol views, and temporal views.

12.4.4 Analysis

The team analyzes the viewpoints and the device for weaknesses or vulnerabilities that, when exploited by an adversary, would permit them to achieve malevolent adversary goals. In general, the core requirements for the device from a security perspective are an essential part of the design. If it does not fulfill the fundamental security requirements, the device does not fulfill its mission. In general, an adversary may have the following high-level goals when attacking the device:

1. Affect data integrity of the device
2. Adversely affect the behavior or reliability of the device.
3. Adversely affect the communications of the device to other devices in the system.

This analysis is performed to the depth and breadth specified by DHS. This phase includes an attack brainstorm and attack graph generation.

12.4.5 Report

The analysis results are recorded in a report that will include details on the techniques used against the device. The report also includes the contents of the attack graph. DHS will use this report as a decision aid to determine:

1. If further testing is required,
2. Whether or not one or more attacks should be implemented to verify their effectiveness
3. Whether the results of these tests will be included in the report.

The distribution of this report is at the discretion of DHS.

12.4.6 Demos and Experiments

If required, additional analysis and demonstration of attacks can be performed under controlled conditions, or experiments can be developed to test hypotheses about device performance under adversarial conditions. If further testing is recommended after the attack graph is generated, this step can be used for validation of potential attacks.

The distribution of the test results, demonstrations, experiments, procedures conducted are at the discretion of DHS.

Glossary

Add-on Sensor (AoS) – Any sensor used by the System that does not contribute to the Security Device security functions as specified in this document.

ACSD (Advanced Container Security Device) – A stand-alone device, or a combination of integrated components, that monitors the door status and breach status of a Container from the POS through the POA. While in transit, the ACSD is to compile and report an Event Log of all relevant Events (e.g. Alarms due to door openings, breach detections, etc.) and report ACSD Status Messages at all required read points.

Advanced Encryption Standard – A data encryption standard adopted by the U.S. government in 2001 that uses symmetric key cryptography to encrypt and decrypt data.

Alarm Status – One of two mutually exclusive states: *Alarmed* and *No Alarm*

Alarmed – The Alarm Status changes from *No Alarm* to *Alarmed* when the Operating Mode of the Security Device is *Armed* and the Door Status changes to *Door Open*.

Application Layer – The seventh layer of the Open System Interconnection (OSI) model, which defines a networking framework for implementing protocols between two end users in a network.

Arm Command – An Restricted Command directing the Security Device to transition from the Deactivated Operating Mode to the Armed Operating Mode.

Armed – One of two possible Operating Modes in which the Security Device performs security-related functions per [1].

Authorized User – a User who is designated by the appropriate authorizing agency as allowed to receive and read data and issue commands. The authority of an Authorized User will be authenticated by the CSD/ACSD System through the use of a password or other technique.

CA (Digital Certification Authority) – Trusted third party for mutual authentication by the DCP and on-container devices

Cargo Operator – A system user who accesses a NAD to read Non-secured Data and issue Unrestricted Commands.

Composite Security Container – A specific subtype of ACSD in which the breach detection components are integrated into the structure of the walls of the container itself, and which, by virtue of having been constructed of composite materials, has weather tight and water tight sides and floor.

Container – An ISO 668 Dry Shipping Container per Appendix A

Critical Failure – Loss of Critical Functionality; inability to perform one or more critical functions.

CSD (Container Security Device) – A stand-alone device or a combination of integrated components that monitors the door status of a Container from the POS through the POA. During the transit, the CSD will compile and report an Event Log of all relevant Events (e.g. Alarms due to door openings, etc.) and also report CSD Status Messages at all required read points.

CSI (Container Security Initiative) – "… One element of CBP's multi-layered approach to

cargo security … CSI is a multinational program protecting the primary system of global trade—containerized shipping—from being exploited or disrupted by international terrorists." *Container Security Initiative*, 2006-2011 Strategic Plan, U.S. Customs and Border Protection. http://www.cbp.gov/linkhandler/cgov/border_security/international_activities/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf

DCP (Data Consolidation Point) – DHS-designated sites that receive Security Device Data forwarded by NADs. The DCPs have the ability to decrypt the Secure Data from Security Devices and to generate Restricted Commands. DCPs may exist at CBP, CSI ports, the POA and the National Targeting Center (NTC) for information routing, and will receive and maintain Security Device Data. The DCP, if operated by a trusted organization, may have communications edge decryption and authentication capability. Otherwise, a DCP cannot decrypt and passes all secure messages to/from other DCPs unaltered.

Defeat Testing – A subset of red teaming that usually occurs during the first two phases of an in-depth red team evaluation. The purpose of defeat testing is to identify high-consequence, easily exploitable vulnerabilities. Defeat testing is performed with limited time and resources and is designed to find simple attacks that circumvent a critical components or functions of the system.

Device Failure – Any failure of the Security Device, including False Alarms and Critical Failures.

DHS Approved Security Device Vendors List – A DHS Security Device System Status website will identify all DHS-approved Security Device System vendors and the Security Device System components they supply. This publicly accessible website will be maintained to reflect current lists of DHS-approved Security Device Vendors and Supply Chain Certificates.

DHS-designated Security Agent – A system user authorized by DHS and authenticated by password or other technique to use NAD-types that receive and read Secure Data and Non-secured Data and issue Restricted and Unrestricted commands.

Door Status – Status parameter having one of two values, either *Door Open* or *Door Closed*

DSA (Designated Systems Administrator) – DHS-designated entity that provides oversight for encryption key exchange and user account management supporting NAD operations.

Encryption Key – A "secret" symmetric key associated with a Security Device's UUID and used to control access to Restricted Commands and Secure Data. The encryption key is set in the Security Device at time of manufacture and may be changed using the Change Encryption Key Command.

Event Log – Data structure containing the Event Records from a Trip.

Event Number – a monotonically increasing entry associated with every Event, and begins with a value of 1.

Event Record – Data structure recorded by the Security Device consisting of the Event #, Event Type, Event Data, and the Security Device Status Message..

Exportable – An item is *exportable* if it is legally suitable for export to any non-U.S. country.

False Alarm – An alarm generated when conditions did not warrant an alarm.

FNAD (Fixed Network Access Device) – see the glossary entry for *NAD*.

Global Supply Chain – The international network of retailers, distributors, transporters, storage facilities and suppliers that participate in the sale, delivery and production of goods.

HNAD (Handheld Network Access Device) – Formerly called a "Handheld Reader"; see the glossary entry for *NAD*.

ICD (Interface Control Document) – A document that describes system interfaces.

IEEE – Institute of Electrical and Electronics Engineers

IMO (International Maritime Organization) – An organization established in 1948 that aims to regulate legal, environmental, and technical matters for the maritime shipping industry with the goal of enhancing efficiency and security.

IP (Internet Protocol) – A protocol used for communicating packets of data between entities over the internet.

ISPS (International Shipping and Ports Security) – A risk management process developed by the IMO that provides a standardized method for evaluating risks and vulnerabilities associated with shipping and maritime facilities and provides measures to reduce these risks.

Manifest ID – A number issued by a shipping party that is used to identify a shipment of goods.

Mechanical Seal ID – The seal number of the Mechanical Seal used to secure the Container.

MTSA (Maritime Transportation Security Act) – U.S. law enacted in 2002 that requires shipping vessels and facilities to assess their vulnerabilities and develop security plans to mitigate risk.

NAD ID – a UUID assigned to every NAD

NAD – A *Network Access Device* (NAD) provides RF communication with any Security Device from the DHS-approved Security Device Vendors List. A NAD also can provide a network data interface for connectivity to a DCP. In the context of this document, a NAD is any appropriate combination of hardware, software, and internal interfaces that satisfy the functional requirements and user interface requirements specified for a NAD Application.

NAD Header – The header appended to the Security Device Data by the NAD before it forwards/receives data to /from DCP.

No Alarm – One of two mutually exclusive states of Alarm Status. The state of Alarm Status is valid only in the Armed Mode. *No Alarm* indicates that no Alarm Event has occurred since the Security Device was Armed.

Non-Proprietary – Not restricted by the exclusive legal rights of the inventor or maker; open-source; freely available for use by others

NTC (National Targeting Center) – CBP's facility that provides tactical targeting and analysis in support of Customs anti-terrorism efforts.

NWK – Network Protocol Layer, resides above the MAC and PHY layers

Operational Field Test – DHS field test to verify that the Security Device System meets the Security Device Requirements defined in this document while in the operational environment.

Operate – An operating regime of the Security Device, defined by external conditions, in which the Device must satisfy all technical requirements

Operating Mode – The operational state of the Security Device. Can have one of two mutually exclusive values, either *Deactivated* or *Armed*.

POA (Point of Arrival) – The U.S. maritime port through which a Security Device-equipped Container enters into the U.S.

POS (Point of Stuffing) – The shipping facility where a Container is sealed prior to initiation of transit.

Racking (of a Container) – Deformation of a container from its nominal rectangular shape.

Red Team – Red Team testing is a structured activity performed by friendly personnel who adopt the role of an attacker with malevolent intentions and attempt to circumvent or defeat the security provisions of a given system. Red team activity may begin with an initial defeat test restricted to the vulnerability/consequence path with the highest probability of success. If the defeat test does not succeed, an in-depth red team test may follow, pursuing multiple attack paths using a greater amount of time and resources. The specific tests performed during red teaming are not predetermined, but the processes for selecting and validating these tests based on the technology of the target system are well-defined. Red teaming is used to identify multiple attack paths graded by level of adversary, identify critical points of failure, and identify the strengths and weaknesses of a system. The results of red teaming allow better understanding of the risk associated with the corresponding device or system.

Restricted Commands – Security Device commands that implement security functions and are reserved for DHS-designated entities. These commands require the Security Device's Encryption Keys and authorized access to a DCP or secure NAD.

Secure Data – Security Device Data that directly or by inference may reveal: (1) the door status, (2) door status history, (3) alarm status, or (4) alarm status history. Secure Data is protected from unauthorized access, modification, or spoofing by cryptographic techniques.

Security Device Commands – Commands that are valid for a Security Device..

Security Device Configuration Data – Specific information that uniquely identifies a Security Device or a Security Device System Component and may include the Manufacturer, the Hardware Version Number, and the Firmware Version Number.

Security Device Data – All data contained within and maintained and communicated by the Security Device.

Security Device ID – The UUID assigned to every Security Device that uniquely identifies it.

Security Device Status – The contents of the Security Device Status Message. Note: Security Device Status is not synonymous with Door Status or Alarm Status.

Security Device Status Message – Consists of the Time, Date, Security Device ID, and Security Device Status.

Security Device System – A system consisting of Security Devices, NADs, network data interfaces, and DHS-designated Data Consolidation Points (DCPs) that monitors the door activity of Containers while in transit, supporting container shipping from the POS, through a CSI port, and through the POA.

Shall – This word, and the terms "REQUIRED" or "MUST", mean that the definition is an

absolute requirement of the specification. (Reference: RFC 2119)

Secure NAD – A device used by DHS-designated Security Agents to initiate Restricted Commands and to view the Security Device Secure Data. A secure NAD can either be referred to as a secure Handheld Network Access Device (HNAD) or a secure Fixed Network Access Device (FNAD).

Should – Means that "there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course". (Reference: RFC 2119)

SOP (Standard Operating Procedures) – A Standard Operating Procedure (SOP) describes how the Security Device System is to be operated and maintained and provides any implementation specifics that may be unique to a shipper and/or trade-lane.

Survive – An operating regime of the Security Device, defined by external conditions, in which the Device is not required to Operate but will not change the Security Device Status or Event Log, or malfunction or fail after returning to the Operate regime.

Tamper – for the purposes of this document, an attempt to compromise the function of the Security Device through physical or cyber access and thus circumvent critical functions of the Device. Note that in this document, "Tamper" does not refer to opening the container doors.

Trip duration – Defined as 1680 hours that begins when the Security Device is placed into the Operating Mode of *Armed*.

Trip Information – Security Device Data consisting of the Container ID, Mechanical Seal ID, and Manifest ID.

Unrestricted Commands – Security Device commands that do not require access to a DCP or secure NAD (or the Security Device's Encryption Keys).

Unsecured Data – Security Device Data that is not encrypted and does not reveal (1) the door status, (2) door status history, (3) alarm status, or (4) alarm status history. Unsecured Data is not encrypted when transmitted to the NAD.

UTC/GMT – Universal Time Coordinated (UTC) is a time standard computed by adding leap seconds to International Atomic Time (TAI, from the French *Temps Atomique International*). With the added leap seconds, UTC closely tracks UT1, which is mean solar time at the Royal Observatory, Greenwich, also known as Greenwich Mean Time (GMT).

UUID (Universally Unique Identifier) – A unique identifier assigned per ISO/IEC 11578:1996 *Information technology – Open Systems Interconnection – Remote Procedure Call (RPC).*

Vendor – The entity that will build, sell, and maintain components for Security Device Systems.

Verify – To confirm that specific action has taken place.

Vulnerability – A weakness in a device or system that, if accidentally triggered or intentionally exploited by an adversary, could allow the device or system to be circumvented or defeated

13 References

[1] *Security Device Requirements R1.0*; Department of Homeland Security, Science and Technology Directorate.

[2] *Security Device (CSD/ACSD) Communications Interface Control Document (ICD) Security Device-to-Network Access Device (NAD);* Department of Homeland Security, Science and Technology Directorate.

[3] *Cargo Security Network Communications Key Management and Data Security Report;* Department of Homeland Security, Science and Technology Directorate.

[4] *Network Access Device (NAD)-to-Data Consolidation Point (DCP) Interface Control Document (ICD) (NAD-to-DCP ICD);* Department of Homeland Security, Science and Technology Directorate.

[5] *Marine Asset Tag Tracking Requirements R1*.0; Department of Homeland Security, Science and Technology Directorate.

This page left blank intentionally

This page left blank intentionally

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS “FOR OFFICIAL USE ONLY” OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.