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.

SECURITY DEVICE REQUIREMENTS INCLUDING ACSD AND CSD
VERSION 4.00

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

Document Number CM/CS/SNL/-/REQ/R4.0/2010/1789
December 3, 2010

<u>FOIA Exemption</u>: *This document contains sensitive information exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 522(b) (2, 4, 5). Do not release without prior approval of the Department of Homeland Security Document Point of Contact*

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

<u>Container Security Test and Evaluation Team</u>
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 derived from requirements development and 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.

Change Summary: Security Device Requirements

Date	Document Version	Summary of Primary Changes
		1. R4.0 is a rewrite with previous versions used as source material

Table of Contents

List of Figures

List of Tables

This page left blank intentionally

1 Introduction

This Department of Homeland Security (DHS) document provides system and component technical requirements for DHS Security Device Systems, primarily the Container Security Device (CSD) and the Advanced Container Security Device (ACSD), including the Hybrid Composite Container (HCC) with Breach Detection System (BDS), a specific ACSD subtype. This document also describes the process for requesting certification for trade-lane use from DHS and an overview of a process that could be used by DHS to grant certification.

The primary purpose of the Security Device is to monitor the doors of a conveyance[1] 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. In the remainder of this document, unless otherwise noted, the term “Security Device” is used to mean either a CSD or an ACSD, and the term “Security Device System” is used to mean a System incorporating either CSDs, ACSDs, or both.

The security of the global supply chain is one of the DHS’s highest priorities. The ability to secure the integrity of a conveyance as it moves through the global supply chain is vital to our nation’s security. DHS recognizes that the security requirements for conveyance shipment must take into consideration technology, people, and procedures. Any commercial vendor developing conveyance security technologies must consider impacts to existing commercial and economic global supply chain operations in considering their design choices.

DHS intends to initially deploy Security Device Systems through members of the Customs Trade Partnership Against Terrorism (C-TPAT). These C-TPAT members have assessed security risks in their own supply chain, including facilities, employees, and business partners, and have demonstrated a commitment to supporting the security measures of DHS. These trusted partners are expected to continue to follow security best-practices, and will be offered the advantages of using Security Devices.

A Security Device System includes battery-operated, conveyance-mounted Security Devices, Network Access Devices (NADs) (described in [6]), multiple network data interfaces, and DHS-designated Data Consolidation Points (DCPs).

The core elements of the requirements for a Security Device System as set forth in this document are designed to be consistent with the procedures that Customs and Border Protection (CBP) uses for CSI and C-TPAT programs, along with Port of Arrival (PoA) screening, scanning, and inspections programs. A Security Device System should integrate into the current infrastructure without impacting cargo operations. Some of the characteristics of a Security Device System are described below.

A Security Device will support the following technical capabilities:

- Detect any Door Openings, including door removals (of either door), after the conveyance on which the Device is mounted has been closed and the Device is Armed.

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

- ACSDs also detect penetration of a specified size through the doors, sides, top, or floor of the conveyance after the conveyance on which the device is mounted has been closed.
- Provide a non-proprietary, interoperable communications capability based on an open standards architecture.
- Provide an Add-on-Sensor (AoS) data bus to support scalability with future Add-on Sensors. An Add-on Sensor is a device that is internal to a conveyance and communicates directly to a Security Device via the wireless AoS bus. There can be up to five (5) AoS per ACSD/CSD (in addition to one (1) external add-on device such as an External Communications Module (ECM) or Electronic Chain of Custody (ECoC) device) as described in [4].
- Communicate with, and transfer Security Device Data through, the following four required read points, shown in Figure 1-1:
  - Exit of the C-TPAT members' Point of Stuffing (PoS)
  - Entrance Gate at the CSI Port of Departure (POD)
  - Exit gate at the Port of Arrival (PoA)
  - Entrance gate at the Point of Deconsolidation (PoDC)
- Provide a high Probability of Detection (P_d)
- Provide a low Probability of False Alarm (P_{fa})
- Provide a low Rate of Critical Failures (for the entire Security Device System)

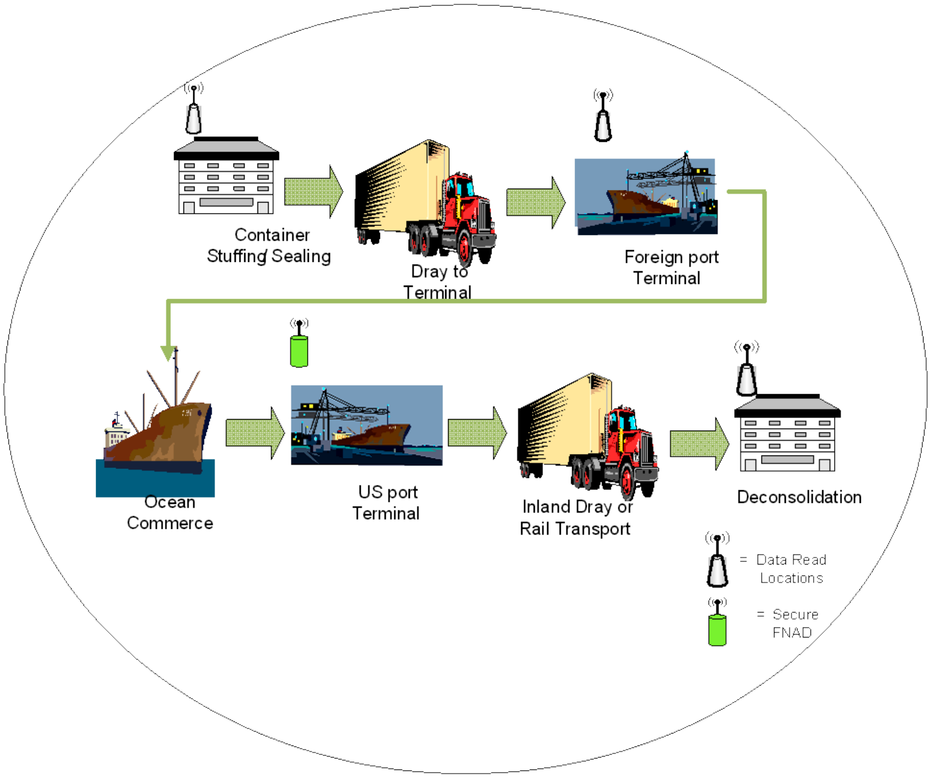


Figure 1-1: Nodes in the Supply Chain where Security Devices may be used

In this document the *Security Device* (often referred to as simply “the Device”) is a stand-alone component (which may be a combination of several integrated components) that will monitor the status of the doors—and the sides, top, and floor in the case of ACSDs—of an ISO 668 dry freight shipping Container (See *Appendix A – ISO Dry Freight Containers*) from the PoS through the U.S. PoDC. The Security Device will record the relevant event records and when in range of a NAD will transmit these event records to the NAD in the form of an event log as described herein.

Read points are locations equipped with Network Access Devices (NADs). NADs provide radio frequency (RF) communications with approved Security Devices. NADs provide network connectivity between Security Devices and Data Consolidation Points (DCPs). NADs may be used to communicate with other cargo security devices as well. Throughout this document, the term NAD is used to refer to any type of Security Device System NAD. There are two general types of NADs. These are namely a Fixed Network Access Device (FNAD) and a Handheld Network Access Device (HNAD).

A complete Security Device System will also include at least one Data Consolidation Point (DCP) and Key Management Facility (KMF). The term DCP used herein refers to a notional concept to facilitate a complete understanding of the components of a Security Device System. A DCP is a restricted-access system to be developed and deployed by the DHS and is not further defined by or addressed in this document. A KMF is a single entity that contains all of the keys in the cargo security network (see [7] for a description of System cryptographic protocols).

Appendix F – Supply Chain Certificate Application outlines a process that a prospective vendor of Security Device System components could follow to submit their product(s) to a sponsoring agency for review and approval. An example of the process appears in the appendix with DHS as the sponsoring agency. If the vendor’s component(s) satisfy all requirements described in the Appendix, the vendor’s product(s) could be placed on an Approved Security Device Vendors List, thereby making it available for Security Device Supply Chain Certification and deployment.

Commonly used terms and words in this document are defined in Section 9, *Glossary*, with the intent of providing uniform definitions and interpretation.

2 Background

During the last ten years, private industry and government agencies have investigated ways to improve security in the global supply chain in an effort to protect against criminal activity and terrorist attacks. This has included development of improved mechanical and electronic conveyance seal technology, sensor systems, and inspection agreements/processes to identify and monitor cargo movement at major ports and transit points throughout the world. The Security Device System enables DHS full compliance with the SAFE Port Act (H.R. 4954) and the Maritime Transportation Security Act (P.L. 107-295) regarding the establishment of conveyance supply chain security standards. U.S. Government policies concerning enhanced security requirements for all U.S.-bound cargo, have led various government and industry teams to investigate ways to adapt existing technologies and processes to provide monitoring of conveyances from the PoS to the PoDC. The use of Security Device Systems in the global supply chain is one component of an improved security system. A goal of the DHS S&T cargo security program is to provide requirements and open technical standards for ACSDs and CSDs that will enable commercial competition and global interoperability for international conveyance security.

This document formalizes the requirements for Security Devices consistent with DHS's security needs and operations in the context of shipping operations.

3 Scope

This document provides DHS usability, functionality, performance, and security requirements for the Security Device System components. Interface requirements for Security Device-to-NAD communications are covered in [4]. Requirements for the NADs are covered in the NAD Requirements Document [6].

The governing documents applicable to the Security Device System are the Security Device Requirements Document (this document) and [4], [5], [6], and [7]

To be compliant with this document's Security Device Requirements, a vendor must comply with all applicable documents.

Additional technical capabilities may be implemented within the Security Device component and/or NAD, provided they conform to, and do not interfere with, the requirements herein. The DCP must support the protocols defined in the relevant Interface Control Documents (ICDs). The Security Device and/or NAD functions required to support anticipated DCP functions are specified herein.

To ensure interoperability of multi-vendor Security Device Systems components, the System Interface Control Documents (ICDs), [4] and [5], may continue to evolve. While every effort has been expended to ensure compatibility, system implementers must remain cognizant of changes or refinements to this ICD, as provided by the Department of Homeland Security's Science and Technology Directorate.

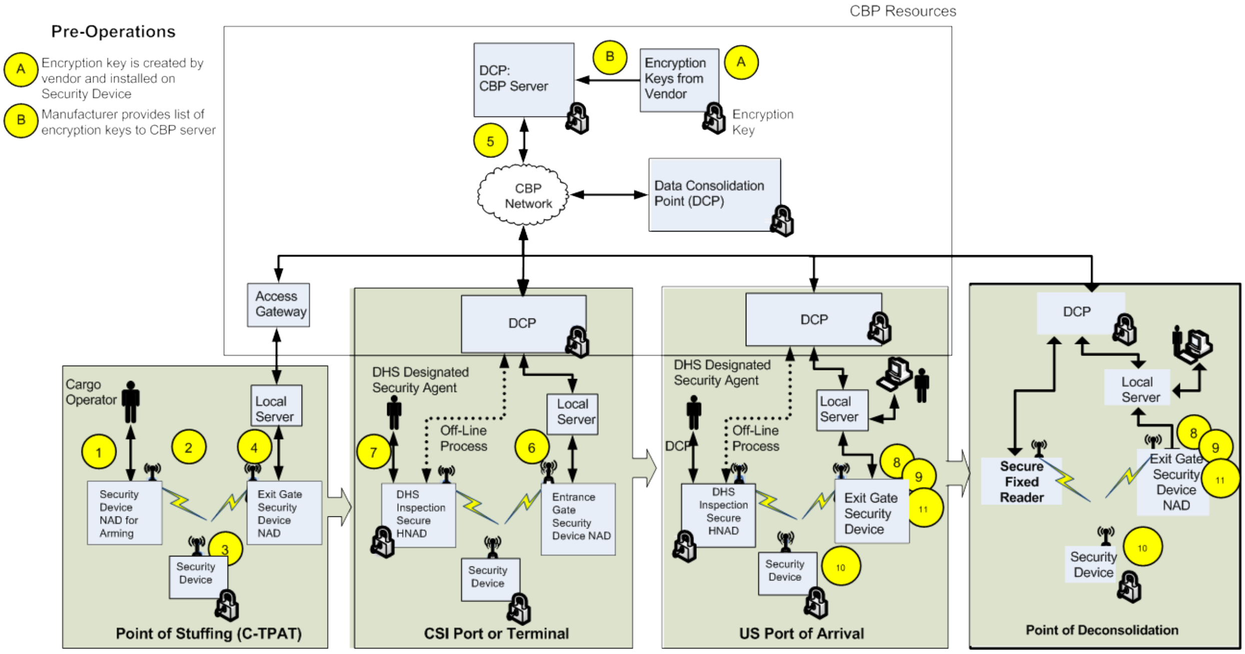
Mandatory requirements are indicated throughout this document with the use of the word "**Shall**".[2]

[2] The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in the Internet Engineering Task Force's RFC 2119.

4 Security Device System Overview and Concept of Operations

This section describes the Security Device System at a high level. A deployed System[3] may have other (e.g., commercial) capabilities; however, no commercial activity is addressed herein, except for requirements that separate commercial data and secure data (see Section 6.5.2).

The essential role of the Security Device is to collect, format, and report two kinds of data: (1) sensor data, in the form of Event Logs, and (2) data describing its own state, in the form of Status Messages. These data are collected by on-conveyance Security Devices and transferred through Network Access Devices (NADs) to a Data Consolidation Point (DCP) as shown in Figure 4-1, which depicts System data flow at a high level.


CBP Resources
Pre-Operations
A
Encryption key is created by vendor and installed on Security Device
B
Manufacturer provides list of encryption keys to CBP server
DCP: CBP Server
B
Encryption Keys from Vendor
A
Encryption Key
5
CBP Network
Data Consolidation Point (DCP)
Access Gateway
DCP
DCP
DCP
Cargo Operator
Local Server
1
2
4
Security Device NAD for Arming
Exit Gate Security Device NAD
3
Security Device
Point of Stuffing (C-TPAT)
DHS Designated Security Agent
7
Off-Line Process
6
Local Server
DHS Inspection Secure HNAD
Entrance Gate Security Device NAD
Security Device
CSI Port or Terminal
DHS Designated Security Agent
DCP
Off-Line Process
Local Server
8
9
DHS Inspection Secure HNAD
Exit Gate Security Device
11
Security Device
10
US Port of Arrival
Local Server
Secure Fixed Reader
8
9
Exit Gate Security Device NAD
11
Security Device
10
Point of Deconsolidation

1 Cargo Operator at Point of Stuffing Facility loads trip information into Security Device

2 Security Device Network Access Device (NAD) sends Arm command to Security Device

3 Security Device arms and responds with Security Device Status message

4 At exit gate, Security Device Status Message sent to DCPs via Security Device NAD Application

5 Encryption keys are provided by CBP server to appropriate DCPs for Restricted Command use and Secure data decryption

6 Security Device NAD forwards Security Device status messages to DCPs

7 DHS Designated Security Agent at CSI DCP can decrypt Secure Data and provide to officers at CBP's discretion

8 Security Device NAD forwards Security Device status message to DCP

9 Security Device Network Access Device (NAD) sends Restricted Commands to Security Device

10 Security Device is deactivated

11 Security Device NAD sends Security Device status message to DCPs

Figure 4-1: Security Device System Overview

4.1 Communication

All Security Device System on-conveyance devices communicate wirelessly with DCPs via Network Access Devices (NADs). Every on-conveyance device communicates via a

[3] Some common words are Capitalized herein to imply specialized meaning in the Security Device System context.

Communications Module (CM), including Security Devices, Electronic Chain of Custody (ECoC) Devices, and External Communication Modules (ECMs). Add-on Sensors (AoSs) are also technically on-conveyance devices, but they communicate only with CMs. Full description and requirements are found in [4] for CM-to-NAD communication and in [5] for NAD-to-DCP communication.

4.2 Security Device System Components

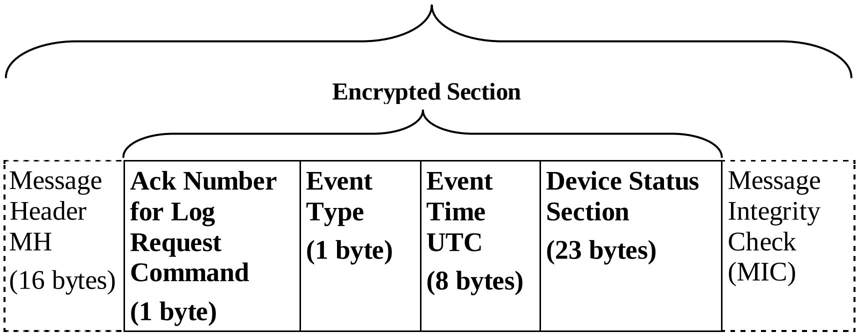
Requirements for components of the DHS *Security Device System* may include battery-operated, conveyance-mounted Security Devices (CSDs and ACSDs), Network Access Devices (NADs) [6], Electronic Chain of Custody (ECoC) Devices [8], External Communication Modules (ECMs), Add-on Sensors (AoSs), network data interfaces, and DHS-designated DCPs.

4.2.1 Security Device

A Security Device is a component of the Security Device System. The CSD type Security Device monitors the status of both Container doors. In addition, an ACSD type Security Device also monitors the container walls, ceiling, and floor Security Devices also create an Event Log containing an Event Record for every event the Device is required to sense and record since the Device was armed.

An example of the structure of an Event Record for a Security Device is shown in Figure 4-2. In case of discrepancy between this document and the Interface Control Document (ICD) [4], the ICD has precedence.

Device Event Log Record Message, Size = 16+1+1+8+23=49 bytes



Encrypted Section

Message Header MH (16 bytes)	**Ack Number for Log Request Command** **(1 byte)**	**Event Type** **(1 byte)**	**Event Time UTC** **(8 bytes)**	**Device Status Section** **(23 bytes)**	Message Integrity Check (MIC)

Figure 4-2: The structure of an Event Record

The design of the Security Device must consider door conditions and motions other than door opening, closing, and removal that may occur in the shipping environment (e.g., container racking), cargo motion within the conveyance, and interactions with other conveyances (e.g., conveyance stacking, which routinely occurs in ports and on board cargo ships).

The Security Device and the DCP bidirectionally communicate with each other through a NAD. The NAD relays information sent to it by a Security Device to its assigned DCP. The Security Device also accepts Security Device Commands from the NAD. Security Device Commands are sent to the NAD from a DCP. Additionally, the Security Device also accepts commands from the HNAD, which is not normally connected to a DCP.

4.2.2 Network Access Device (NAD)

NADs provide a bidirectional wireless RF communications interface to Security Devices, based on IEEE Standard 802.15.4-2006 physical and data link layer protocols, in accordance with [6]. The NAD is the transparent link for data and command transmission between Security Devices and the DCP.

NADs support the following tasks:

- Identify Security Devices in their RF communication range,
- Establish a wireless network connection with the Security Devices,
- Deliver Security Device Commands to the Security Device,
- Acquire Security Device Status Messages and Security Device Event Logs, and
- Communicate Security Device Status Messages and Security Device Event Logs to the assigned DCP.

NADs and their intended application are described further in [6] and the protocol for establishing a Security Device-to-NAD network connection is specified in [4]. The activities and events that govern data transfers between a Security Device and a NAD are defined in Section 6.4.

4.2.3 Data Consolidation Point (DCP)

DCPs receive Security Device Data from CMs forwarded by NADs. In an operational system, a DCP will collect data from many on-conveyance Devices, hence a DCP is literally a point of data consolidation. From an external point of view the DCP can be considered a secure server that distributes Security Device System data to other DHS-authorized information systems.

Restricted Commands and Secure Data are protected from unauthorized access, modification, and spoofing by the use of encryption. The DCPs are able to decrypt the Secure Data from Security Devices, to generate Restricted Commands, and to transfer Encryption Keys, Security Device Event Logs, and Secure Status Messages. DCPs may exist at any or all of the CBP, CSI ports, the PoA, and the National Targeting Center (NTC) to route and collect information.

4.2.4 Additional System Components

External Communication Modules (ECMs) are designed to extend the range of Security Devices, which are mounted inside a conveyance when in operation and therefore have limited range. The ECM is fundamentally nothing more than a wireless communication relay device mounted outside the conveyance.

Electronic Chain-of-Custody Devices (ECoC Devices) [8] are designed to provide services outside the scope of this document. However, they can also perform the functions of an ECM.

Other vendor-designed features and components may be included in the Security Device System at the discretion of the vendor. For example, vendors may add functions to a Security Device to collect, maintain, and transmit commercial-purposed data that are unrelated to the Security Device requirements in this document. The vendor is responsible for determining how to maintain and transmit this data.

4.3 Authentication and Encryption

Security Device System design incorporates mechanisms to enable the DHS concept of operations while ensuring end-to-end data integrity and confidentiality. The *Cargo Security Key*

Management and Data Security document [7] specifies the authentication and encryption mathematics, cryptographic protocols, and key management processes that ensure the integrity and confidentiality of System information while providing protection against replay and spoofing attacks.

Security Devices respond to *Restricted* and *Unrestricted* Commands (Table 6-1) and transfer *Secure* and *Unsecured* Data. Restricted Commands and Secure Data are protected from unauthorized access by an encryption process implemented with Encryption Keys embedded in each Security Device and provided by the vendors. An overarching authority (namely, a Key Management Facility (KMF)) will make these encryption keys available to the DCPs. The DCP is the primary command source and consumer of System data. See [7] for details.

Operators can access Device functions and data via a NAD without a "live" DCP connection if the NAD has downloaded the relevant keys from the DCP. Unrestricted Security Device Commands and Unsecured Security Device Data can be accessed by anyone with access to a NAD or DCP. A DHS-designated Security Agent can use a Secure NAD (generally assumed to be an HNAD) to access Secure Data and issue Restricted Commands. See [7] for details.

Use of the term "authorized" implies an authentication mechanism to verify that users and equipment on opposite sides of an interface are known to each other and have permission to use the interface. The authentication process described in [7] provides only device-to-device authentication, e.g., it is possible to know whether a Secure NAD is authentic, but not whether the *user* of the HNAD is authentic. It is assumed that each site has adequate *physical* security to prevent unauthorized use of DCPs and Secure NADs, and digital authentication (preferably two-factor, although this topic area is outside the scope of these requirements) is recommended to enable NAD use by an individual.

4.4 Notional Security Device System Configurations and Utilization

4.4.1 Notional Configuration: Minimal Security Device System

Figure 4-3 depicts several components of a deployed Security Device System: a Security Device, a NAD, and a DCP. The Security Device system communicates with DHS Systems over an Internet Protocol (IP)-based interface to, e.g., notify DHS of the Security Device Status, download Security Device Event Logs, or allow Deactivation of the Security Device at the PoA. Secure Data and Restricted Commands are to be treated as authentic if properly authenticated using the appropriate encryption keys as described in [7].

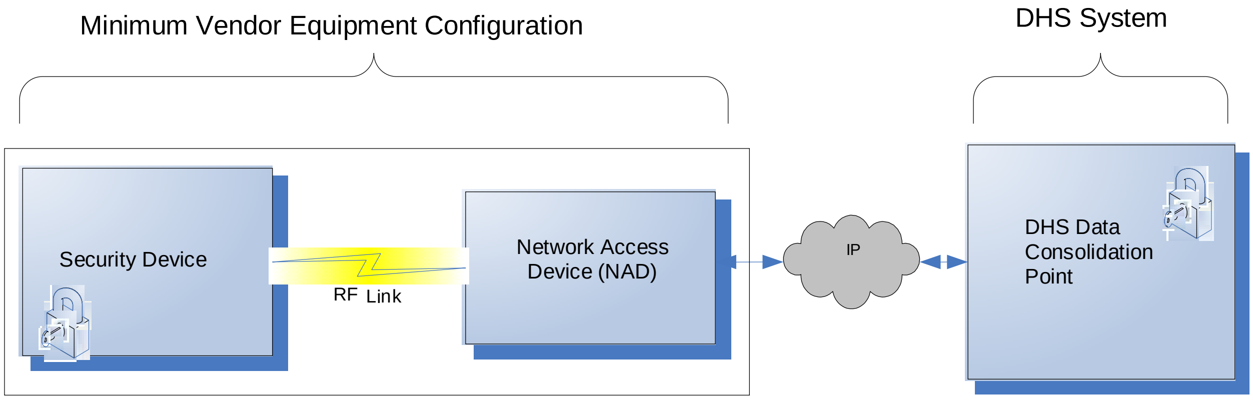

Minimum Vendor Equipment Configuration
DHS System
Security Device
RF Link
Network Access Device (NAD)
IP
DHS Data Consolidation Point

Figure 4-3: Simplified Security Device System Configuration

4.4.2 Notional Configuration: Cargo Stuffing and Security Device Arming

Figure 4-4 depicts a notional Security Device System that includes a cargo operator interface to the NAD. This diagram represents capabilities that allow a Cargo Operator to prepare and Arm a Security Device at a cargo stuffing facility. Key functional elements of the cargo support configuration include:

1. The ability to set *Trip Information* (Conveyance ID, Manifest ID, and the Mechanical Seal ID) into Security Device memory[4],
2. Provision to allow an operator to verify the *Trip Information*, and
3. Provisions to support Arming and verification of arming status prior to release for shipment.

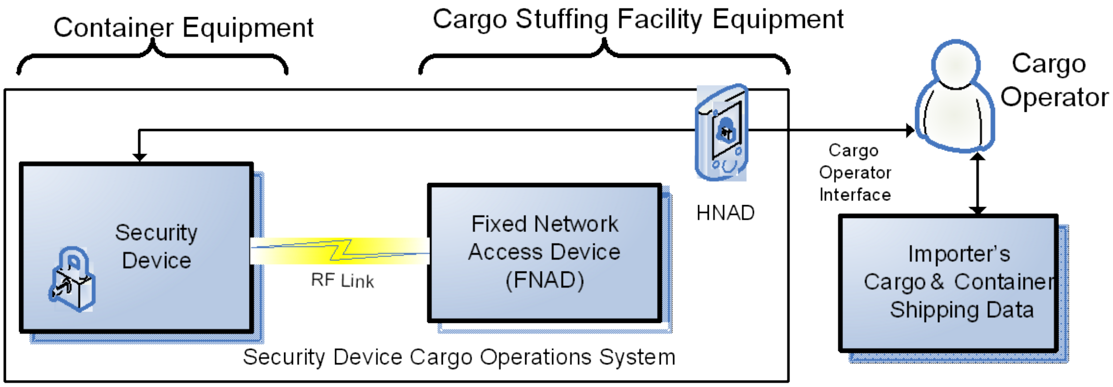

Container Equipment
Cargo Stuffing Facility Equipment
Cargo Operator
Security Device
RF Link
Fixed Network Access Device (FNAD)
HNAD
Cargo Operator Interface
Importer's Cargo & Container Shipping Data
Security Device Cargo Operations System

Figure 4-4: Notional Security Device System for Importer Stuffing and Arming Operations

The Cargo Operator Interface equipment depicted between the NAD and Cargo Operator in Figure 4-4 is implemented at the discretion of the vendor. This interface may be a Handheld NAD (HNAD) or a NAD with a network interface. NADs may use the IP network connection depicted in Figure 4-3 for the notional Security Device system. The requirements for a Cargo Operator Interface that can issue Unrestricted Commands and display Unrestricted Status are specified in [6].

4.4.3 Notional Configuration: DHS Fixed Inspection Location

Figure 4-5 depicts a Security Device System configuration to support specific DHS security screening, monitoring, and deactivation for Security Device-equipped conveyances. These security check points will be at fixed locations where a Security Device-equipped conveyance can be accessed by a FNAD to determine the alarm status of the Security Device and where the Device's Event Logs can be retrieved and reviewed.

[4] Configuration includes establishing the wireless sensor network, for sensors inside the conveyance for commercial functions.

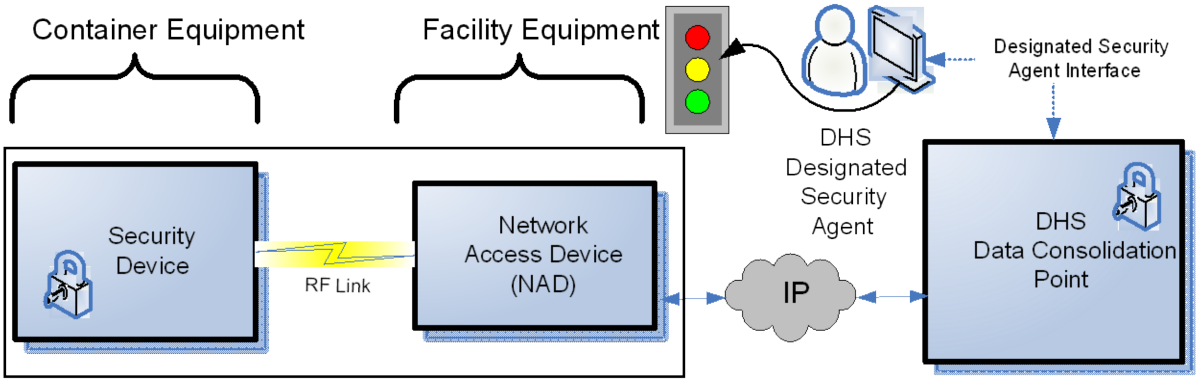

Container Equipment
Facility Equipment
Designated Security Agent Interface
Security Device
RF Link
Network Access Device (NAD)
DHS Designated Security Agent
IP
DHS Data Consolidation Point

Figure 4-5: Notional Security Device Fixed Inspection Location

4.4.4 Notional Configuration: DHS Portable Inspection System

DHS also requires a Security Device System to include a Secure Handheld Network Access Device (HNAD) to perform conveyance inspections. The Secure NAD incorporates capabilities to perform operations that can also be performed by a DHS-designated DCP with direct IP access via any NAD. A Secure NAD has the following functionality:

1. Read and display Security Device Status Messages and Event Logs, including Secure Data (similar to DCP functionality)
2. Construct and send Security Device commands, including all Restricted Commands in Table 6-1, as requested by an operator (similar to DCP functionality).

The DHS-designated Security Agent directs download of Encryption Keys from a DCP to the Secure NAD for specific Security Devices to which communication will occur prior to performing inspection activities. The DHS Secure NAD can upload Security Device Status Messages and Event Logs (if present) by communicating with a DCP.

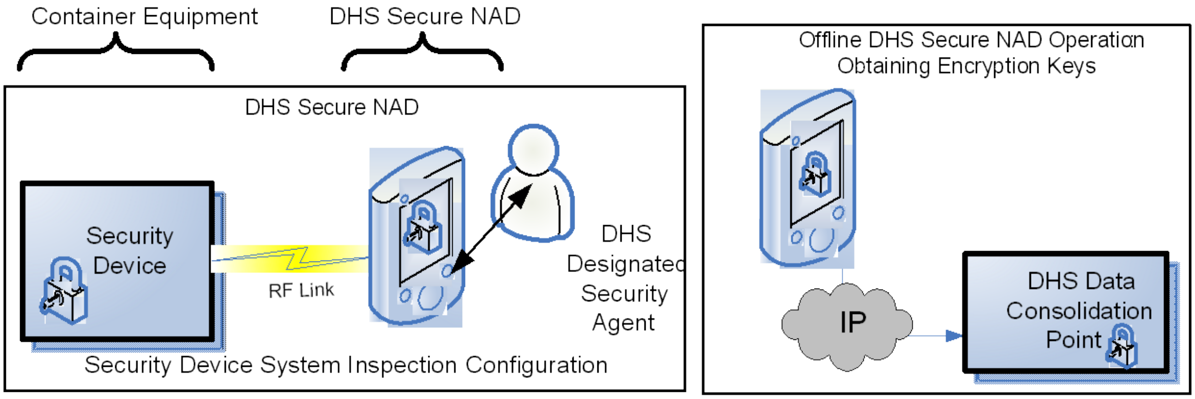

Container Equipment
DHS Secure NAD
DHS Secure NAD
Security Device
RF Link
DHS Designated Security Agent
Security Device System Inspection Configuration
Offline DHS Secure NAD Operation Obtaining Encryption Keys
IP
DHS Data Consolidation Point

Figure 4-6: DHS Secure NAD Configuration

4.5 Command and Data Categories

Security Device Commands are classified as either *Restricted* or *Unrestricted*. Security Device Data are classified as either *Secure* or *Unsecure*. A description for each is provided in the following sections.

4.5.1 Security Device Command Classes

Security Devices support two classes of commands: *Unrestricted* Commands and *Restricted* Commands. For Restricted Commands, knowledge of the Encryption Key provides the Security Device with implicit authentication that the Restricted Command was issued by a DCP or Secure NAD. The Security Device will not execute or acknowledge Restricted Commands that do not decrypt properly.

The purpose of Restricted Security Device Commands is to limit the use of certain Security Device commands only to DHS-authorized entities. Restricted Commands must satisfy the same criteria as Unrestricted Commands with an additional constraint: Restricted Commands will not be executed by the Security Device unless the Security Device receives, decrypts, and properly authenticates the Command as described in [7].

Unrestricted Commands are commands that will be executed by a Security Device when and only when all of the following are true:

1. The Security Device ID in the Command Header matches the ID of the Security Device receiving the message
2. The command/message format complies with [4]
3. The command is a valid command for the current Security Device mode and state.

4.5.2 Security Device Data Classes

Security Devices support two classes of data: Secure Data and Unsecure Data. Secure Data is encrypted by the Security Device and cannot be viewed by entities that do not possess the Security Device’s Encryption Key.

The Security Device sends a *Security Device Status Message* upon receipt of a valid command to do so. The Security Device Status Message includes only Secure Data as defined by Section 6.3. The Security Device may also communicate the *Event Log*, which is always transmitted as Secure Data.

The Message Header of the Security Device Status Message is unencrypted.

The purpose of Secure Data is to control access to Security Device Alarm Status, Door Status, and Event Log data. Access to this data is restricted in order to prevent unauthorized entities from detecting changes in Alarm Status or Door Status. Secure Data is protected from disclosure, modification, or spoofing by encryption at the Security Device Application Layer. DCPs and Secure NADs may decrypt Secure Data from a given Security Device using that Security Device’s Encryption Key.

4.5.3 Security Device Command and Data ConOps

Security Devices are nominally Armed at the PoS using commands initiated by a cargo operator. Security Devices are Deactivated by commands initiated at the DCP assigned to the PoA either at the PoA or at the PoDC. In each case a NAD transmits the commands to the Security Device and the Security Device transmits the Security Device Status Message back to the NAD in response to the command execution and to provide the current Security Device Status.

The *Arm with Trip Information* Command is Restricted and requires a secure operator interface to a DCP. Therefore the DCP or secure NAD can be used to arm the Security Device. A Security

Device Status Message is subsequently acquired by the NAD at the PoS exit gate and forwarded to a DCP.

The *Disarm from DCP or secure NAD* Command is Restricted. The Security Device deactivation process occurs only when a Security Device is in communication range of a NAD with an IP link to a DCP, or where a Secure NAD is within communication range of a Security Device. A NAD provides encrypted commands to deactivate Security Devices (see Figure 4-5).

At DHS's discretion, Security Devices may be monitored by NADs anywhere in the supply chain where an ICD-Compliant NAD is installed to provide access for transmitting Security Device data to a DCP (see Figure 4-3)

DHS may inspect conveyance Security Device status while in transit by communication with ICD-compliant NADs. By design this will result in the Security Device reporting an alarm condition if the conveyance door has been opened. The DHS-designated Security Agents may Clear Alarm, Change Trip Information, or issue any other Restricted Command that can be generated by either a DCP (Figure 4-5) or a Secure NAD (Figure 4-6).

The Security Device Encryption Key can be changed when associated with a NAD. This restricted capability allows DHS to change the Security Device Encryption Key over wireless connection as needed.

Security Device System Technical Requirements
Sections 5-8

5 Usability Requirements

Several requirements in this section are either not rigorously testable as written or technically difficult to verify; DHS understands that Security Device System operations will affect shipping operations and that Security Devices will occupy space inside the conveyance. The DHS recognizes that the terms “adversely affect”, “meaningfully decrease”, and “special” are not well-defined as used here. However, it was necessary to express the intent of these requirements in somewhat stronger terms than mere desirability, so they are stated as “Shalls” instead of “Shoulds”. The requirements in this section are intended to motivate the vendor’s design decisions towards a preferred Security Device.

A vendor seeking government acceptance of a Security Device or other system component should understand that a relatively large, heavy Device that’s difficult to install could be certified for Trade Lane Testing (see *Appendix E – Trade-Lane Pre-Deployment Test Guidelines*) but would be less desirable in a competitive setting than a smaller, lighter, easy-to-install Device.

1. The Security Device **Shall** be able to be installed and operated on an ISO 668 Dry Shipping Container (See *Appendix A – ISO Dry Freight Containers*).
2. Mounting of the Security Device **Shall Not** adversely affect the functioning of the Container’s door-to-frame environmental seal.
3. A Security Device’s door movement detection components **Shall** satisfy at least one of the following when installed:
   3.1. Physically inside the conveyance when the conveyance doors are closed
   3.2. Integrated into the structure of conveyance[5]
4. Application and use of a Security Device **Shall Not** adversely affect shipping operations or cargo loading and unloading activities.
5. Installation or removal of a Security Device **Shall Not** require special tools.
6. Installation or removal of a Security Device **Shall Not** nullify the ISO certification of the Container.
7. The Security Device **Should Not** meaningfully decrease Container cargo capacity.

[5] Significant conveyance modifications could result in a need to recertify conveyances thus modified.

6 Functional Requirements

This section describes the functional requirements for Security Devices.

6.1 Door Status Sensing Requirements

The following are the requirements for determining the Door open/closed Status. Figure 6-1 is provided to clarify these requirements, but is offered as a depiction only and not as an interpretation of these requirements. The intent of these requirements is to specify the door movement limits for Security Device sensing and reporting of Door Status, while providing the vendor design latitude to address differences in ISO-certified container construction and loading techniques in the global supply chain and still achieve the performance requirements defined in Section 7.1.

1. The Security Device **Shall** report *Door Status* as either *Door Open* or *Door Closed*.
2. The Security Device **Shall** report *Door Status* as *Door Open* if, for either of the Container's rear doors, any point on the doors' exterior surface moves 2 inches or more for longer than one second from the position of the doors when closed with both locking bars of both doors fully latched into their "closed" position.
3. While its Operating Mode is *Armed*, the Security Device **Shall** assess the positions of the doors no less often than once per second for changes in the Door Status.

Note that the removal of either or both doors satisfies the Door Open criterion.

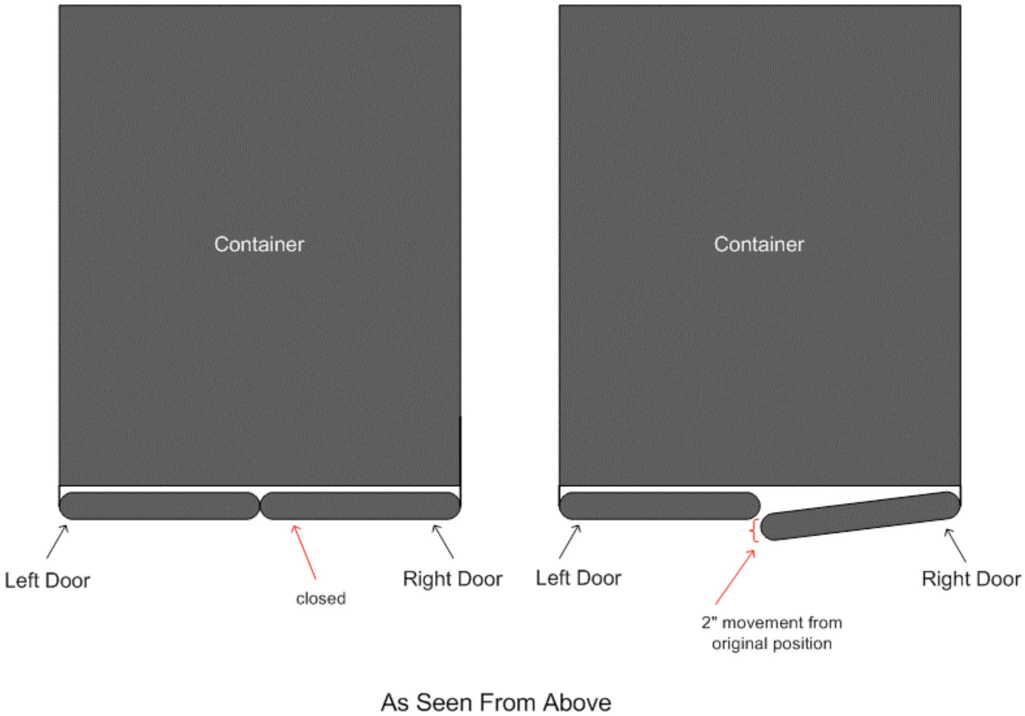


Figure 6-1: Door movement of 2 inches from a closed and latched position

6.2 Breach Status Sensing Requirements

The following are the requirements for determining a container breach. The intent of these requirements is to specify the limits for Security Device breach sensing and reporting of Breach Status, while providing the vendor design latitude to address the idiosyncrasies of the Container and the loadings imposed within the global supply chain and still achieve performance requirements per Section 7.1. These requirements apply only to ACSDs (i.e., not to CSDs).

1. The Security Device **Shall** report the Breach Status as either *Breach Detected* or *No Breach Detected*.
2. The Security Device **Shall** report the Breach Status as *Breach Detected* if, for any of the Container's sides or floor, any single penetration measuring greater than or equal to a three-inch diameter hole is present.
3. While in the Operating Mode of Armed, the Security Device **Shall** monitor for changes in the Breach Status no less often than once per second.

6.3 Security Device Status

The Security Device Status includes some data elements that are set when the Security Device is Armed and remain constant for the duration of the transit, and other data elements that change based on the requirements described below.

Detailed data formats for the Security Device Status can be found in [4]. Section 6.4 provides additional details on the commands listed in this subsection and the allowed state transitions for the Security Device.

1. The Security Device Restricted Status Message **Shall** include the Security Device time and date, Security Device UID, and the Security Device Status per [4].
2. The Security Device Status Message **Shall** include the following data elements:
   - Trip Information
   - Operating Mode (See Item 5)
   - Reserved (future use)
   - Alarm Status
   - Door Status
   - Breach Status (for ACSDs only)
3. Trip Information **Shall** consist of the following data elements (as specified in [4]):
   - Conveyance ID (16 bytes)
   - Manifest ID (16 alphanumeric characters)
   - Mechanical Seal ID (up to 15 alphanumeric characters)
4. The Trip Information data **Shall** be set upon receipt of any of the following commands:
   - A valid *Set in Trip State* Command
   - A valid *Arm with Trip Information* Command
   - A valid *Change Trip Information* Command
5. The Security Device **Shall** support two and only two Operating Modes: *Armed* and *Deactivated*
6. The Security Device Restricted Status **Shall** include a Reserved data field per [4].

7. The Security Device **Shall** support two and only two values for the *Alarm Status* parameter: *Alarmed* and *No Alarm*
8. The Security Device **Shall** support two and only two values for the *Door Status* parameter: *Door Open* and *Door Closed*
9. The Advanced Container Security Device **Shall** support two and only two values for the *Breach Status* parameter: *Breach Detected* and *No Breach Detected*.
10. The *Door Status* **Shall** be determined per the Door Status Sensing Requirements, which are described in Section 6.1.
11. ACSD *Breach Status* **Shall** be determined per the Breach Status Sensing Requirements, described in Section 6.2.
12. The state of the Security Device upon its receipt from the vendor **Shall** be consistent with the Device having executed a *Disarm from DCP or Disarm from Secure NAD* Command as its most recent valid Security Device Command per Section 6.4.
13. The Operating Mode **Shall** transition from *Deactivated* to *Armed* when and only when all three of the following conditions hold:
    - *Door Status* is *Door Closed*
    - Available Power is sufficient for a Trip[6] with the Security Device powered up and Armed
    - The Device receives a valid *Arm with Trip Information* Command
14. The Operating Mode **Shall** transition from *Armed* to *Deactivated* when and only when the Device receives a valid *Disarm from DCP or Disarm from Secure NAD* Command.
15. The *Alarm Status* **Shall** transition from *Alarmed* to *No Alarm* when and only when one of the following occurs:
    - The Device receives a valid *Disarm from DCP, Disarm from Secure NAD* Command or,
    - The Device receives a valid *Set Master Alarm = False* Command and the Event Log is not full
16. The *Alarm Status* **Shall** transition from *No Alarm* to *Alarmed* when and only when the *Operating Mode* is *Armed* and any one of the following occurs:
    - *Door Status* changes from *Door Closed* to *Door Open*
    - *ACSD Breach Status* changes from *No Breach Detected* to *Breach Detected*
    - The Device receives a valid *Set Master Alarm = True* Command
    - The Device detects other faults; e.g., the Event Log overflows regardless of cause, whether as a result of normal operation, malfunction, or malicious activity.

[6] A Trip is defined as a duration of 1680 hours (70 days) that begins when the Security Device is turned on and Armed (See Section 7.2).

6.4 Security Device Commands

The Security Device System must support both *Restricted* and *Unrestricted* command, as detailed in [4]. Table 6-1 contains all commands relevant to the DHS utilization of the Security Device. *Restricted* Commands relate to DHS security functions, and must be encrypted per [7] before being sent to a Security Device. *Unrestricted* Commands are not encrypted and can be sent to a Security Device without access to the DCP. The following requirements describe the commands. Additional details for these commands, data structure, and functions are provided in [4]. Note that when the Device Status is *Armed*, it must enter an Event Record into the Event Log for every valid command it receives, per Section 6.7.

Table 6-1: Security Device Commands, Command Types, Security Device State, and Constraints

Security Device Commands	**Device State**		**Constraints**
	Armed	**Deactivated**	
Restricted Commands	Encrypted Only		
Disarm from DCP	Valid	Not Valid	Event Log must have been downloaded and erased.
Disarm from Secure NAD	Not Valid	Not Valid	
Change Encryption Key	Valid	Valid	Must be able to change encryption key whether armed or deactivated. Device must have known key.
Change Trip Information	Valid	Not Valid	Constraints for Manifest ID and Mechanical Seal ID; Conveyance ID must be valid per STD 6346
Set Time	Valid	Not Valid	Time format per ICD.
Arm with Trip Information	Not Valid	Valid	*Door Status* must be *Door Closed*; complete Trip Information must be either already set or contained in the *Arm* Message Payload; and sufficient power for 1 Trip[7] with the Security Device powered up and Armed must be available
Set in Trip State	Valid	Not Valid	
No Operation (NOP)	Valid	Valid	Solicited status
ICD Acknowledgement (ACK)	Valid	Valid	ICD ACK is generated only by , DCP, or Secure NAD
Set Master Alarm = True	Valid	Not Valid	Alarm Status must be No Alarm
Set Master Alarm = False	Valid	Not Valid	Door status must be *Door Closed* and Alarm Status must be *Alarm*
Send Event Log Unsent	Valid	Valid	Interpreted to mean "send *all* unsent Event Records". Must follow *Send Event Log* command
Send Event Log All	Valid	Valid	Interpreted to mean "send *all* Event Records"
Erase Event Log	Valid	Valid	Must follow Event Log download
NAD Enable Sensor	Valid	Not Valid	Sensor must be disabled
NAD Disable Sensor	Valid	Not Valid	Sensor must be enabled
Configure Sensor	Valid	Not Valid	Sensor must be enabled
Read Sensor Configuration	Valid	Not Valid	Sensor may be either enabled or disabled
Sensor Pairing	Valid	Not Valid	Sensor must be enabled
Sensor Database Query	Valid	Not Valid	Sensor must be enabled
Unrestricted Commands	Encrypted or Unencrypted		
Send Unrestricted Status Message	Valid	Valid	Allowing unencrypted error message (e.g. improper or no encryption key)
Pair Command	Not Valid	Valid	ACSD/CSD deactivated/ unpaired and relay device unpaired
Pair Request Command	Not Valid	Valid	ACSD/CSD deactivated/unpaired and relay device unpaired

[7] A Trip is defined as 1680 hours (70 days) (See Section 7.2).

The Security Device will perform various functions upon receipt of valid Commands from HNADs/DCPs as shown in the State Transition Diagram, Figure 6-2. Note that every valid Security Device Command received is logged per Section 6.7, Event Log Requirements

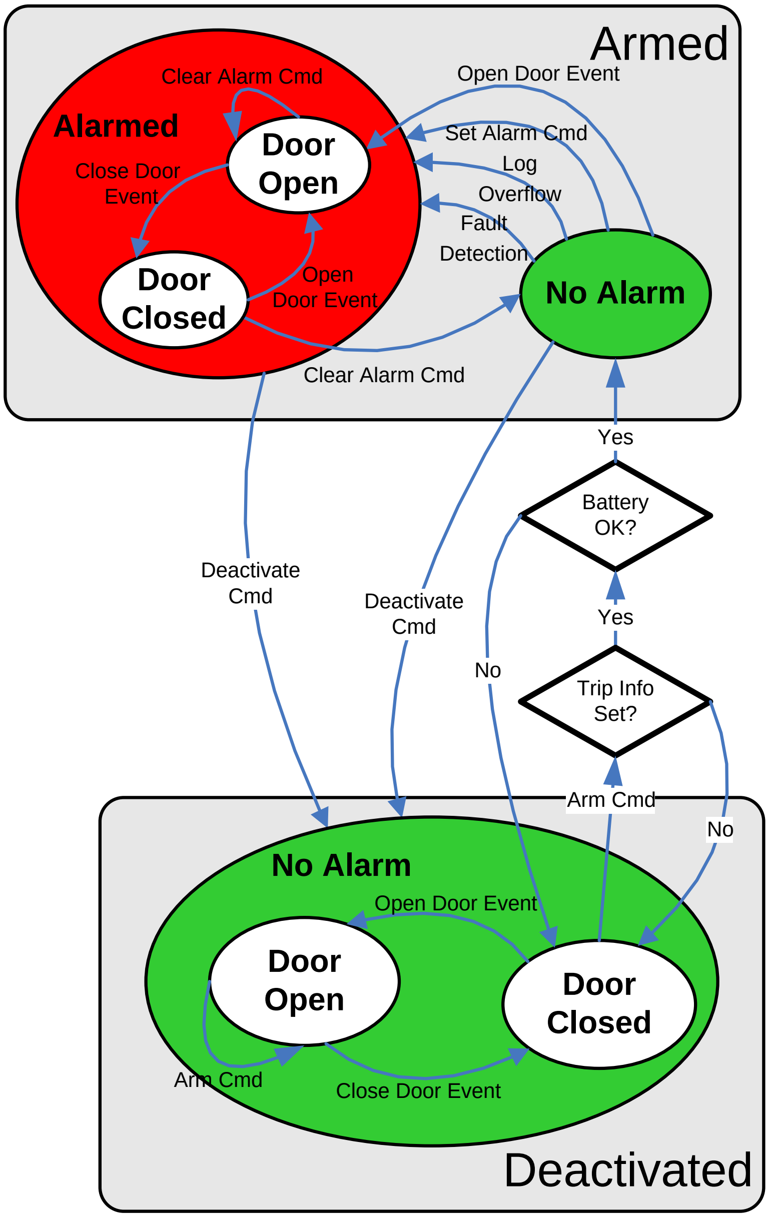


Figure 6-2: Security Device State Transition Diagram

Valid commands are listed in Table 6-1. For a Security Device to respond to a valid command it must be addressed to the Device; have a valid Command Header and Payload; have the correct number of parameters, have parameter values in valid ranges; and be appropriate for the current state of the Security Device. Restricted Commands must be encrypted per [7] and Section 6.6; Unencrypted Restricted Commands are not valid. As a rule, unless specified otherwise, the Security Device **Shall Not** respond to Commands that are not valid and **Shall Not** respond when a valid Command cannot be executed.

1. All Security Device Commands **Shall** have a Command Header and a Command Payload.
2. The Command Header of Security Device Commands **Shall** include the Unique Identifier (UID) of the message originator as specified in section 6.7 in [4].
3. The Security Device **Shall** respond to the Restricted Commands as defined in Table 6-1.
4. The Security Device **Shall** be able to determine whether a Restricted Command it receives is a valid Security Device Command for its current operating state and alarm condition.
5. A Restricted Command is a valid Security Device Command if and only if all of the following are true:
   - The Command is received as encrypted data using a valid encryption key.
   - The Command Payload is decrypted in compliance with [7]
   - The Command is listed in the Restricted Command section of Table 6-1
   - The format of the Command Payload is correct
6. The Security Device **Shall** be able to determine whether an Unrestricted Command it receives is a valid Security Device Command.
7. An Unrestricted Command is valid if and only if both of the following are true:
   - The Command is listed in the Unrestricted Command section of Table 6-1
   - The format of the Command Payload is correct
8. The Security Device **Shall** respond to the *Send Unrestricted Status* Command with an *Unrestricted Status Message*.
9. The Security Device **Shall** ignore unrestricted commands that are contained in a broadcast message.
10. The Security Device **Shall** consider an *Arm with Trip Information* Command to be valid if and only if its Operating Mode is *Deactivated*.
11. When the Security Device completes the execution of a valid Security Device Command, the Security Device **Shall** return the resulting Security Device Status Message to the sender.
12. When the Security Device receives a valid Security Device Command (see Table 6-1) while in the *Armed* Operating Mode, the Security Device **Shall** update the Event Log per Section 6.7.
13. Upon receipt of a valid *Arm with Trip Information* Command the Security Device **Shall**:
    - Set Operating Mode to *Armed* if and only if sufficient power is available for a Trip and the Door Status is *Door Closed*
    - Report power available and failure to set Operating Mode to *Armed* if remaining battery power is not sufficient for a Trip
    - Report Door Status and failure to set Operating Mode to *Armed* if Door Status is *Door Open*
14. Upon receipt of a valid *Disarm from DCP* or *Disarm from Secure NAD* command when and only when the Event Log has been downloaded and acknowledged, the Security Device **Shall**:
    - Initialize the Event Log per Section 6.7.
    - Set the Alarm Status to *No Alarm*
    - Clear the Trip Information
    - Set the Operating Mode to *Deactivated*

15. The Security Device **Shall** determine the *Change Trip Information* Command as valid if and only if the Conveyance ID conforms to ISO 6346 [9].
16. Upon receipt of a valid *Change Trip Information* Command, the Security Device **Shall** replace the existing Device Trip Information with the Trip Information values contained in the command message.
17. Upon receipt of a valid *Send Unrestricted Status Message* Command, the Security Device **Shall** transmit the current Security Device Status to the requesting entity per Section 6.8 and [4].
18. Upon receipt of a valid *Send Event Log Unsent Records* Command, the Security Device **Shall** transmit the entire contents of the Event Log to the requesting entity in reverse sequential (i.e., Last-In, First-Out (LIFO)) order per Section 7.4.
19. Upon receipt of a valid *Change Encryption Key* Command, the Security Device **Shall** replace the Encryption Key(s) with those provided in the command message.
20. Upon receipt of a valid *Set Master Alarm (False)* Command, the Security Device **Shall** change the Alarm Status from *Alarmed* to *No Alarm* only if the Door Status is *Door Closed*.
21. Upon receipt of a valid *Set Master Alarm (True)* Command, the Security Device **Shall** change the Alarm Status from *No Alarm* to *Alarmed*.
22. The Security Device **Shall** maintain Time and Date with a drift of no more than 1 second per month.
23. Upon receipt of a *Set Time* Command, the Security Device **Shall** within 1 millisecond, set its onboard time to the time contained in the Set Time Command (note the Security Device does not necessarily have access to an accurate time value).

6.5 Security Device Encryption Requirements

Security Devices implement encryption and decryption in order to control access to Restricted Commands and Secure Data.

1. All Event Records in the Event Log, **Shall** be stored as encrypted data per [7].

6.5.1 Security Device Data Classes

Two classes of data are transferred from the Security Device to a NAD: *Secure* Data and *Unsecure* Data. These classes of data are depicted and specified in [4].

1. Security Device Secure Data **Shall** be encrypted and authenticated at the application layer of the Security Device prior to processing by the 802.15.4-2006 link layer.
2. Unsecure Data **Shall** be included in a Security Device Unsecure Status Message without encryption.
3. All Security Device Data messages **Shall** contain the data content described in Sections 4, 6.1, and 6.7 of this document.
4. All Security Device Data messages **Shall** be formatted in accordance with data specifications provided in [4].

6.5.2 Commercial Security Device Data and Commands

Security Devices **May** support commercial applications unrelated to the security functions and data described in this document. This section states the requirements for separation of data used for security purposes and data used for commercial purposes. Data used for security purposes is *Secure data*, defined as data that is encrypted, which includes (but is not limited to) Device Status Data, Event Log Data, Restricted Device Command Messages, and Encryption Keys.

Commercial functionality is unlimited as long as it doesn't impact security functionality and meets the following requirements:

1. Secure Data and commercial data **Shall Not** be commingled during transmission, and while in volatile storage, non-volatile storage, or during processing within the Security Device**.**
2. Security Device Encryption Keys used to support Restricted Commands and Secure Data storage and transmission:
   2.1. **Shall Not** be used for commercial purposes.
   2.2. **Shall Not** be accessible to Security Device commercial functions.
3. Support for storage, processing and/or transmission of commercial data **Shall Not** give advantage to any entity attempting unauthorized access of Secure data or the keys that enable Secure data access.
4. The storage, processing and/or transmission of commercial data **Shall Not** give advantage to any entity attempting to access Security Device System data and **Shall Not** affect the Security Device System processing of that data.
5. Commercial data **Shall Not** be transmitted by the Security Device with the DCP as the intended recipient.
6. Secure Data **Shall Not** be duplicated to Commercial storage.
7. Secure Data **Shall Not** be derived from commercial data sources.

6.6 Security Device Encryption Key Requirements

The Encryption Key used to control access to Restricted Commands and Secure Data is embedded in the Security Device at time of manufacture and is assigned to a Security Device's UID. The Security Device keys are provided to the KMF by the vendor. See [7] for details.

1. Each Security Device **Shall** include a unique device Encryption Key used for encryption by the Security Device.
2. The vendor **Shall** implement and document a security plan to protect Security Device Encryption Keys.
3. Encryption **Shall** be implemented in accordance with Advanced Encryption Standard (AES) AES-128 [3].
4. The Security Device vendor **Shall** provide DHS with Security Device Encryption Keys and associated Security Device IDs.
5. All hardware and software employed in the Security Devices and NADs **Shall** be legally exportable.

6.6.1 Security Device Operational Command Classes

Two classes of operational commands are issued to the Security Device by/from the NAD: *Restricted* Commands and *Unrestricted* Commands. The command class for each Security Device command is specified in [4]. Restricted Commands must be encrypted to be valid, and can therefore originate only at a DCP or Secure NAD. Unrestricted Commands may or may not be encrypted and support Security Device functions for which encryption is not required per Table 6-1.

1. Restricted Commands **Shall** be processed by the Security Device if and only if it is received as encrypted data and is otherwise valid (see Section 6.4, item 5)**.**
2. Unrestricted Commands **Shall** be executed by the Security Device whether received as encrypted or unencrypted data if they are valid (see Section 6.4, item 7)**.**
3. Commands available for execution by the Security Device **Shall** be determined by the Device according to the state of the Device and its allowable state transitions, as described in Section 6.4 and shown in Figure 6-2.
4. The *Security Device Encryption Key* **Shall Not** be physically or electronically accessible from the Security Device except via the Restricted *Change Encryption Key* Command per Section 6.4.

6.7 Event Log Requirements

This section defines the requirements for the *Event Log* and the information it must contain. Reference [4] shows the message elements detailed in the requirements below and the formats for data transmission. Note that Security Device Event logs are cleared and reinitialized either prior to or upon execution of the *Disarm from DCP* or *Disarm from Secure NAD* Command, per Section 6.4, and under no other circumstances. Note that while the Security Device Status is Armed, every valid Command execution and every change in the Security Device Status Message (see Section 6.3) results in an Event Record.

1. When the Security Device Operating Mode is Armed, the Security Device **Shall** record Event Records as entries in the Event Log (See [4] for the data structure of an Event Record).

2. When the Security Device Operating Mode is Deactivated, the Security Device **Shall Not** record Event Records in the Event Log.
3. Event Log data (Event Records) **Shall** be encrypted per [4] and [7] for transmittal to the DCP or HNAD.
4. Log data entries **Shall** be encrypted when stored in the Security Device.
5. The Event Log data entries (Event Records) **Shall** be sequentially ordered by time of Event prior to encryption for transmittal to the DCP/HNAD.
6. The Event Log **Shall** be sized to accommodate a minimum of 1000 Event Records.
7. Upon Event Log overflow, the Security Device **Shall** stop updating the Event Log and leave existing Event Records unchanged.
8. The Event Records **Shall Not** be alterable by any Security Device operation, other than clearing of the Event Log when commanding the Security Device to the Deactivated state or the Restricted Command *Erase Event Log*.
9. Each Event Record **Shall** include a monotonically increasing Event Number associated with each Event entry, starting with a value = 0 for the first Event entry, per [4].
10. The Event Log **Shall** be initialized only upon receipt of a valid *Disarm from DCP* or *Disarm from Secure NAD* command, as follows:
    10.1 Event Number 0 in the Event Log **Shall** contain the Security Device UID.
    10.2 Event Number 0 in the Event Log **Shall** indicate Device Status = Armed
11. Each Event Record **Shall** include the Security Device Status Message at the time the Event occurred (See [4] and Section 6.1 for data content of Security Device Status Message).
12. Each of the following **Shall** generate an Event Record in the Event Log, as detailed in [4]:
    12.1 Any change in Security Device Status, with the Event Data field zero-filled.
        12.1.1 The Security Device Status change resulting from the *Arm with Trip Information* Command **Shall** be recorded in the Event Log as it is initialized during execution of the Command per Section 6.4.
    12.2 Successful execution of any Security Device Command (Table 6-1), with Event Data consisting of the Command Payload and Command Header from the received command, not to supersede Section 12.1.1.
        12.2.1 Successful execution of the *Arm with Trip Information* Command **Shall** be recorded in the Event Log
    12.3Successful send of Unsolicited Status Message following network discovery per [4].
13. All Security Device Commands listed in Table 6-1 **Shall** be recorded in the Event Log.
14. Prior to the Event Log overflowing the Security Device **Shall** set the *Alarm Status* to *Alarmed* and update the Event Log.

6.8 Additional Security Device Information

1. The Security Device Configuration Data and the Security Device ID **Shall Not** be altered or changed except by vendor maintenance, and only as detailed in the vendor’s Standard Operating Procedure (SOP).
2. Security Devices that record other data to support commercial supply chain functions **Shall Not** compromise or otherwise interfere with any requirements for the Event Logs.

3. Other Security Device Data to support commercial supply chain functions **Shall Not** contain any Secure Data, per [4], or allow it to be derived.
4. The Security Device **Shall** contain an Add-on-Sensor (AoS) bus with a capability for five (5) sensor inputs (in addition to one (1) external add on device such as an External Communications Module (ECM) or Electronic Chain of Custody (ECoC) device).

6.9 Communications Requirements

The Security Device system implements data communications paths that support global Security Device interoperability, Security Device monitoring, and Security Device Data recovery. Communications interfaces and requirements between Security Devices and NADs are specified in [4]; communications interfaces and requirements between NADs and the DCP are specified in [5].

General Security Device System communication requirements are as follows:

1. Security Devices and NADs **Shall** implement wireless bidirectional communications as a primary mode compliant with IEEE Standard 802.15.4-2006 and per [4].
2. Security Device Status and Command Message structure and data formats **Shall** be in accordance with [4].

7 Performance Requirements

7.1 System Performance Requirements

System performance metrics have a direct influence on operations for both DHS and for the shipping community. The following requirements define the system performance, but do not apply to any optional commercial data communications pathways or sensor systems:

1. The Security Device **Shall** provide no less than a 95% Probability of Detection (P_d), per door opening event, while the Security Device is in *Armed* Operating Mode:.
2. The Security Device **Shall** provide no more than a 0.2% for the combined Probability of False Alarm (P_{fa}) and Probability of Critical Failure, per Trip.
3. The Security Device **Shall** be able to communicate with any Fixed NAD (FNAD) positioned at a distance of 100ft (30.5m) or less from the Security Device.
4. The Security Device **Shall** be able to communicate with an Handheld NAD (HNAD) positioned at a distance of 10ft (3.05m) or less from the Security Device.
5. The Security Device and NAD **Shall** be able to initiate communications and request and transfer the Security Device Status Message while mounted in a conveyance moving at a speed anywhere in the range of 0 to 35 mi/hr (15.7 m/s), inclusive.

7.2 Power Requirements

The Power Requirements for the Security Device are specified on a per-Trip basis. A Trip is defined as 1680 hours (70 days). It is left to the vendor to decide the service lifetime for their Security Device. Therefore, the Security Device Power Requirements are as follows:

1. At the time of power-up and arming, the Security Device power source **Shall** have sufficient power to maintain all Critical Functions for the duration of a Trip. Power consumption after power-up and prior to Arming should be considered.
2. Critical Functions **Shall** be those operations necessary to sense, recognize, log, and communicate the Security Device Status and Event Log.

7.3 Security Device Environmental Requirements

The following subsection describes both the Security Device Environmental Requirements and the associated Environmental Suitability Verification for Submission. *Appendix B – Environmental Requirements Discussion* provides a discussion of this section's environmental requirements that may be beneficial during development.

Environmental requirements (of a reduced form) for both the Fixed Network Access Devices (FNADs) and Handheld Network Access Devices (HNADs) are addressed in [14] and [15] respectively.

There are two kinds of environmental requirement: those in which the Security Device must continue to *Operate* and those that the Security Device must *Survive*. Some environmental conditions only have *Survive* requirements, as detailed below.

7.3.1 General “Operate” and “Survive” environmental requirements

1. In environmental conditions identified as “Operate”, the Security Device **Shall** satisfy all technical requirements found in Sections 5 through 8 of this document.
2. As a result of exposure to the Survive environments, the Security Device **Shall not**:

   2.1 Incorrectly change or report Security Device Status data

   2.2 Add erroneous event data to the Event Log

   2.3 Modify, delete or otherwise compromise the integrity of the Event Log

   2.4 Malfunction or fail after returning to the Operate environment.
3. As a result of exposure to the global shipping environment, the Security Device **Shall** continue to Operate.

7.3.2 Temperature and Humidity Requirements

4. Temperature: The Security Device **Shall** Operate in the temperature range as occurs in the global shipping environment, such as the -40°C to +70°C, from IEC 60721-3-2 Table 1, Classification of climatic conditions, Class 2K4. Temperatures outside of this range are governed by Requirement 7.3.5, below.
5. Temperature: The Security Device **Shall** Survive in the temperature ranges consistent with the global shipping environment, such as the -50°C to -40°C and +70°C to +85°C, from IEC 60721-3-2 as above, and IEC 60721-3-2 Class 2K5 (modified low end to -50°C).
6. Thermal Shock: The Security Device **Shall** Operate when subjected to the rapid temperature changes consistent with the global shipping environment, such as the following temperature changes from IEC 60721-3-2, Table 1 – Classification of climatic conditions, Class 2K4:
   - from 20°C to -40°C over a time interval of no more than 4 minutes
   - from -40°C to 20°C over a time interval of no more than 4 minutes
   - from 20°C to 70°C over a time interval of no more than 4 minutes
   - from 70°C to 20°C over a time interval of no more than 4 minutes
7. Humidity: The Security Device **Shall** Operate at humidity levels consistent with the global shipping environment, such as 95% humidity over the temperature range from -40° C to +70° C from IEC 60721-3-2, Table 1, Classification of climatic conditions, Relative humidity, Class 2K4.

7.3.3 Structural Vibration and Mechanical Shock Environmental Requirements

8. Shock:

   8.1 The Security Device **Shall** remain attached and Operate during and after shock events consistent with the global shipping environment, such as that equivalent to a ten-foot empty Container drop and a five-foot fully-loaded Container drop, from IEC 60721-1, Table 1, Item No. 6.1.3. *Non-stationary vibration, including shock,* Spectrum Type III, where the spectrum is the shock response spectrum.

   8.2 The Security Device **Shall** Survive a handling shock drop of 1 meter onto a hard surface (concrete or asphalt) as a bare unit (i.e., not mounted in a conveyance) on any side.

9. Vibration: The Security Device **Shall** Operate when exposed to vibrations consistent with the global shipping environment, such as stationary random vibration equivalent to the following levels from IEC 60721-3-2, Table 5 – Classification of mechanical conditions, *Stationary vibration, random,* Class 2M3:

   9.1 3 m^2/s^3 from 10-200 Hz

   9.2 1 m^2/s^3 from 250-2000 Hz

7.3.4 Precipitation Environmental Requirements

10. Salt Mist: The Security Device **Shall** Operate when exposed to salt mist as it occurs in the global shipping environment, such as that specified in IEC 60721-1, Table 1, *Chemically active substances, Sea salt* (conditions of air) which lists 0.3 g/m^3.

11. Rain: The Security Device **Shall** Operate when the conveyance is exposed to rain as it occurs in the global shipping environment, such as at a rate of 15 mm/min for 10 minutes from IEC 60721-3-6, Table I, *Classification of climatic conditions, Precipitation, rain,* Class 6K5.

12. Impacting Water/Water from sources other than rain: The Security Device **Shall** Operate after the parts of the Security Device that are affixed and external to the Container are exposed to salt water as it occurs in the global shipping environment, such as water from wheel spray or breaking seas with a concentration of sea salts of 30 kg/m^3 at the rate of 10 m/s for the Security Device once installed from IEC 60721-3-6, Table I, *Classification of climatic conditions, Water from sources other than rain,* Class 6K5, and Table III, *Classification of chemically active substances, Substances in water, Sea salts,* Class 6C3. The Composite Security Container subtype of ACSD **Shall** Operate after the walls and floor are subjected to 30psi direct pressure water without leakage per the watertight designation.

13. Frost/Ice: The Security Device **Shall** Operate when exposed to frost and ice in the global shipping environment, as described in IEC 60721-1, Table 1, *Formation of ice and frost.*

14. Sand and Dust: The Security Device **Shall** Operate when exposed to sand and dust as it occurs in the global shipping environment, such as 10 g/m3 sand and 3 mg/(m2 x h) dust from IEC 60721-3-6, Table IV, Classification of mechanically active substances, Sand in air and Dust sedimentation, Class 6S2 and 6S3.

15. Fungus – the Security Device **Shall** Operate in an environments where conveyance is exposed to conditions which are conducive to fungus growth as it occurs in the global shipping environment, such as from IEC 60721-3-6, Table II, *Classification of biological conditions, Flora,* Class 6B2, as, for example: in a fungal environment created in 95% relative humidity, at 30°C (+/- 1), using a mixed spore suspension.

7.3.5 Radiation and Electromagnetic Environmental Requirements

16. Radiated Emissions:

    16.1 The Security Device radiated emissions **Shall not** exceed the limits given in *47 CFR Part 15 (FCC Rules on radio frequency devices)*.

    16.2 The Security Device radiated emissions **Shall not** exceed the Emission limits for enclosure port type (see *Appendix B – Environmental Requirements Discussion* 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. Measured at a distance of 3 meters.

Note that the radiated emissions requirements in this table do not pertain to the 802.15.4b frequency band used for communications and are applicable only to non-communications sources of emissions from the Security Devices.

Emissions Limits – Non-Communications

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

16.3 The Security Device radiated emissions for both communications and sensors **Shall not** exceed the Maximum Allowable Environment (MAE) for radiated emission as defined in NAVSEA OP 3565/NAVAIR 16-1-529 VOLUME 2, Sixteenth Revision, *Technical manual, Electromagnetic Radiation Hazards (Hazards to Ordnance)*

16.4 The Security Device radiated emissions for both communications and sensors **Shall not** exceed the field strength or power density limits for human exposure (HERP) for mobile devices (ANSI/IEEE C95.1-1992, *IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields*).

17. Radiated Susceptibility: The Security Device **Shall** Operate when exposed to radiated emissions consistent with the global shipping environment, such as power-frequency magnetic fields and radio-frequency magnetic fields as detailed below.

17.1 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, with frequencies adjusted to fit application).

17.2 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 and B, and IEC 61000-4-3 Section 5 and Annex E, adjusted values to fit application).

18. Static Electricity: the Security Device **Shall** Operate after being subjected to electrostatic contact discharge as it occurs in the global shipping environment, such as of ± 8kV contact discharge, ±15kv air discharge, from IEC 61000-6-2, Table 1, *Immunity – Enclosure ports,* subsection 1.5, *Electrostatic discharge*.

19. Lightning: the Security Device **Shall** Operate after experiencing a nearby lightning strike as it occurs in the global shipping environment, such as at 100m with a peak current amplitude of 30kA having a transient magnetic field with a peak amplitude of 50 A/m.

20. Radiation exposure: The Security Device **Shall** operate after accumulating a total radiation exposure of up to 82 rad (Si).

21. X-ray exposure: The Security Device **Shall** operate without malfunction or false signal as a result of exposure to a pulse of X-rays at a dose rate of no less than 5 x 10^4 rad (Si)/s

22. SOLAS (Safety of Life at Sea): for Security Devices installed in ISO 668 Containers, the Security Device **Shall** fulfill the requirements of SOLAS regulation II-2/19.3.2, *Sources of Ignition* (electrical equipment fitted in enclosed cargo spaces must be of a certified safe type for use in the dangerous environments to which it may be exposed unless it is possible to completely isolate the electrical system.

7.3.6 Environmental Suitability Verification for Submission

This section describes the environmental verification requirements for a Security Device**.** In order to submit a Security Device for DHS consideration, the vendor must provide verification that the Security Device satisfies a subset of the more general environmental conditions of Section 7.3. The following vendor verification does not constitute compliance with all of the requirements of Section 7.3, but rather represents a suitability and readiness for a more general DHS test and evaluation process. The vendor must document the verification results per Section 17 of this document.

7.3.6.1 Verification for Submission by Testing

1. For all required testing, verification **Shall** be accomplished by successfully demonstrating that the Security Device either Operates or Survives, as required, using a minimum of 5 Security Devices per test, each of unique serial number from the Security Device Type and Configuration under consideration under the test conditions prescribed.

2. Indication of compliance with the Temperature Range **Shall** be demonstrated by the following:
   - 2.1 The Security Device **Shall** be tested per the Operate requirement using testing that conforms to IEC 60068-2-1 and 60068-2-2 (Tests A (cold) and B (dry heat), respectively), using procedures consistent with Method Ae (for a heat dissipating device, powered throughout, under a gradual heat change) with an end temperature of -40°C for 16 hours, and Method Bb (for a non-heat dissipating device under a gradual temperature change) with an end temperature of +70°C for 16 hours. Additionally, The Security Device is to be tested with a diurnal temperature cycling, conforming to IEC 60068-2-14 (Change of temperature), using procedures consistent with Method Nb (Change of temperature with specified rate of change), with the low temperature being -40°C, the high temperature being +70°C, the rate of change being 1 +/- 0.2°C/min, the exposure time at each extreme being 2 hours, and the number of cycles being 4.
   - 2.2 The Security Device **Shall** be tested per the Survive requirement using testing that conforms to IEC 60068-2-1 and 60068-2-2 (see Section 10.1.2.1), using procedures consistent with Method Ae with an end temperature of -50°C for 16 hours, and Method Bb with an end temperature of +85°C for 2 hours.

3. Indication of compliance with the Temperature Shock **Shall** be demonstrated by Security Device testing that conforms to IEC 60068-2-14, Test N (Change of Temperature), using procedures consistent with Method Na (Rapid change of temperature with prescribed time of transition), and the temperatures and transition times as listed above for the nominal five cycles.

4. Compliance with the Temperature & Humidity requirements **Shall** be demonstrated by the Security Device being tested in a manner conforming to IEC 60068-2-38, Test Z/AD

(Composite temperature/humidity cyclic test), using stipulations and procedures consistent with those in Test Z/AD, with the 24h cycle going between the temperatures listed above.

7.3.6.2 Verification for Submission by Testing or Analysis

1. Indication of compliance with the Shock Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-27 (Shock), using procedures and stipulations consistent with Ea and a final-peak saw-tooth pulse shape with a peak acceleration of 35809 m/s^2 and duration of 0.43ms.
2. Indication of compliance with the Vibration Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-64 (Vibration – broadband random).
3. Indication of compliance with the Salt Mist Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-11 (Salt Mist), using stipulations from subsection 4 on the salt solution and air supply, for a duration of 96 hours.
4. Indication of compliance with the Rain Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-18 (Water), using stipulations and procedures from Method Ra 1 (Falling drops: Artificial rain) and the following severities: drop falling height of 2m, tilt angle of 0 and 45, a duration of 60 minutes, and the intensity as listed above.
5. Indication of compliance with the Impacting Water/ Water from sources other than rain Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-18 (Water), using stipulations and procedures from Method Rb 2 (Impacting Water: Water jet).
6. Indication of compliance with the Frost/Ice Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-39, using stipulations and procedures from Method Z/AMD (Sequential Cold, Low Pressure, and Damp Heat) with a low pressure value of 30kPa, a low temperature of -40°C, using a total of 4 cycles.
7. Indication of compliance with the Sand and Dust Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-68 (Dust and Sand), using stipulations and procedures from Method Lb (Free settling dust), for a duration of 3 days using a particle size of 75μm, and from Method Lc (Blown dust and sand) with a particle size distribution as indicated for all three variants (fine dust, course dust, and sand) in part 6.1.4.1, a dust concentration of 10 g/m^3, and air velocity of 25 m/s, for a duration of 4 hours.
8. Indication of compliance with the Fungus Environment (The Security Device **Shall** be designed and implemented to avoid materials that are conducive to the growth of fungus. Fungus in the environment proximate to the Security Device **Shall** not impact the operation of the Security Device.) This **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 60068-2-10 (Mould Growth), using stipulations and procedures from Method J, variant 2 (including choosing the fungi to which the materials used in the Security Device are susceptible, from Table 1), for a total incubation of 28 days.
9. Indication of compliance with the Radiated Emissions Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 61967-3 (Measurement of radiated emissions), using stipulations and procedures from the test method and over the frequency ranges indicated in 47 CFR Part 15 applicable to the device type of the specific

Security Device, assuring that measured emissions levels fall within the limits of 47 CFR Part 15 and conforming to ANSI C63.4 or CISPR 22.

10. Indication of compliance with the Radiated Susceptibility Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 61000-4-3 (Radiated, radio-frequency, electromagnetic field immunity), using stipulations and procedures from the test method and frequencies and levels as indicated above; and to IEC 61000-4-8 (Power frequency magnetic field immunity test), using stipulations and procedures from the test method and frequencies and levels as indicated above.
11. Indication of compliance with the Static Electricity Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 61000-4-2 (Electrostatic discharge immunity), using stipulations and procedures from Method 1a (Contact discharge), at a test level of 2 (±8kV) from Table 1 – Test levels.
12. Indication of compliance with the Lightning Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to IEC 61000-4-9 (Pulse Magnetic Field Immunity), using stipulations and procedures from the test method and at the levels indicated above.
13. Indication of compliance with the Radiation Environment **Shall** be demonstrated by either Analysis or Test.
    - 13.1 Total Dose verification **Shall** be in a manner conforming with exposure to either Co-60 gamma rays or 9-MeV electrons at a dose rate of 0.1 rads/sec, or an electron scanning system, where each scanned area is exposed to a total dose of 82 rads.
    - 13.2 Dose rate verification **Shall** be in a manner conforming with exposure to a dose rate of no greater than 5 x 10^4 rad (Si)/s, where the pulse width of the electron pulse is 1 µs or, using an electron scanning system, each scanned area is exposed to the specified dose rate.
14. Indication of compliance with the SOLAS Environment **Shall** be demonstrated by either Analysis or Test, in a manner conforming to SOLAS II-2/19.3.2 for Sources of Ignition.

7.4 Failure Modes

An objective of these requirements is to ensure that an application or device either fails safe or fails-soft [1] (continues to function, possibly in a degraded mode) even when certain components have been intentionally damaged or destroyed. Although these requirements are important to consider during the design of a system, they are difficult to test and verify compliance. Therefore, these requirements are written as recommendations rather than absolute requirements. They will be taken into consideration during vulnerability testing and analysis.

1. The Security Device **Should** fail safe, such that systems that fail or lose power do so in such a way as to protect assets.
2. The Security Device **Should** fail-soft, i.e., the Device should continue to operate, perhaps in a reduced capacity, during a failure of some element in the system.

8 Security Requirements

8.1 Cyber Anti-Tamper

1. The Security Device **Shall** ensure that Security Device program code cannot be modified, replaced, or deleted except by the manufacturer.

8.2 Physical Protection / Physical Anti-Tamper

Tamper-evident coatings or seals are used so that the coating or seal must be broken to attain physical access to the interior of the Security Device. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

1. The Security Device design and implementation **Shall** provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the module is attempted.
2. The Security Device design and implementation **Should** be tamper resistant to physical attacks.
3. The tamper-evident coating or tamper-evident enclosure **Should** be opaque within the visible spectrum.
4. The Security Device **Should** include design features to mitigate a potential adversary from avoiding or circumventing the sensor's detection capability.

8.3 Security Device Component Interfaces

To the extent that a Security Device System is composed of multiple elements or components that communicate on an interface or interfaces that are accessible external to its sealed components, those interfaces and data transmitted on those interfaces must adhere to the following requirements:

1. A Security Device of multiple elements/components with interfaces (physical, RF, or other) external to the Security Device housing **Shall Not** reveal the Security Device Restricted Status data or any sensor data used to monitor the Door Status.
2. A Security Device of multiple elements/components with interfaces (physical, RF, or other) **Shall** be protected from modification, alteration, creation, or other interference by any entity other than the specific element of interface component associated with that Security Device.

9 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*, per 7.1.16.

Application Layer – 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 with Trip Information Command – A 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 Section 6.

Authorized User – a User designated by the appropriate authorizing agency as allowed to receive and read data and issue commands. An Authorized User can be authorized at two levels: (1) for Restricted Commands and Secure Data or (2) for Unrestricted Commands and Unsecured Data. The authority of an Authorized User will be authenticated by the CSD/ACSD System through the use of a password or other technique.

Breach Detected – One of two possible values for Breach Status that must be detected by the ACSD per Section 6.2, and which indicates a Breach has occurred.

Breach Not Detected – The Breach Status that indicates no Breach has occurred.

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

Cargo Operator – A Cargo Security System commercial user authorized to use the System to read certain data and issue certain commands.

Change Trip Information Command – A Restricted Command, on receipt of which a Security Device replaces its Trip Information with the values from the command message per Section 6.4.

Clear Alarm Command – A Restricted Command, on receipt of which the Security Device changes the Alarm Status from *Alarmed* to *No Alarm*, per Section 6.1.15.

Command Payload – The command operation code and associated parameters, per Section 6.4

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

Container – An ISO 668 Dry Shipping Container per Appendix A

Conveyance – an ISO 668 Dry Shipping Container, motor carrier trailer, or comparable rail enclosure

Conveyance ID – Identification marked on the conveyance (per ISO 6346 [9] for ISO 668 containers).

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

Critical Functions – Those operations necessary to sense, recognize, log, and communicate the Security Device Status and Event Log, per Section 6.7.2.

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 and maintain Security Device Data forwarded by NADs. The DCPs are able to decrypt 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). 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.

***Disarm* Command** (*from DCP or Secure NAD)* – A Restricted Security Device Command directing the Security Device to transition the Operating Mode from *Armed* to *Deactivated* and in doing so to complete the functions described in Section 6.4.

Deactivated – One of two possible Operating Modes in which the Security Device functions per Sections 6. A *Deactivated* Security Device does not generate Alarm Events.

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 Unsecured Data and issue Restricted and Unrestricted commands.

Door Closed/Door Open – The two possible values for Door Status that must be detected by the Security Device per Section 6.1.

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

Encryption Key – A "secret" symmetric key associated with a Security Device's UID 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, per [4].

Event Number – a monotonically increasing entry associated with every Event, and begins with a value of 1, per Section 6.7.

Event Record – Data structure recorded by the Security Device consisting of the Event #, Event Type, Event Data, and the Security Device Status Message, per [4].

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 (up to 16 alphanumeric characters).

Message Header – The header appended to the Security Device Command, which includes the NAD ID, the NAD time, and the Security Device ID, per [4].

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

NAD ID – a Unique Identifier (UID) 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 and user interface requirements specified for NAD Application, Section 4.2.2.

NAD Header – The header appended to Security Device Data by a NAD before it forwards data to or receives data from a DCP, per [4].

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*.

P_d (Probability of Detection) – The likelihood that the Security Device will properly alarm when in the Armed Mode and the door(s) are moved such that the conditions for Door Open are satisfied (per Section 6.1).

P_{fa} (Probability of False Alarm) – The likelihood that a Security Device in the Armed Mode will alarm improperly due to environmental conditions or conditions other than opening or removing the door(s).

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 conveyance) – Deformation of a conveyance from its nominal rectangular shape.

Red Team – Red Team testing is a structured activity performed by friendly personnel who adopt the role of a malevolent attacker 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 more 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 target system technology are well-defined. Red teaming is used to identify multiple attack paths graded by level of adversary, identify critical points of failure, and identify a system's strengths and weaknesses. Red teaming results allow better understanding of the risk associated with a device or system.

Restricted Commands – Security Device commands that implement security functions and are reserved for DHS-designated entities (Section 6.4). These commands require the Security Device's Encryption Keys and authorized access to a DCP or Secure NAD, per Section 7.4.

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, per Section 6.4, items 4 and 6.

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, per [4].

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

Security Device Status – The contents of the Security Device Status Message per [4]. 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, per [4].

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 conveyance shipping from the PoS, through a CSI port, and through the PoA.

Send Security Device Status Message Command – An Unrestricted command on receipt of which the Security Device communicates the current Security Device Status, per Section 7.4 and [4] per Section 6.4

Send Event Log Command – A Restricted Command on receipt of which the Security Device communicates the current entire contents of the Event Log, per Section 7.4, in reverse sequential order, per Section 6.4

Set Alarm Command – A Restricted Command that, on receipt of which, the Security Device changes the Alarm Status from *No Alarm* to *Alarmed*, per Section 6.4.

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.

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.

Supply Chain Certificate – Certification that the vendor's SOP conforms to CBP requirements per Section 17. Awarded by CBP and required for each trade-lane to be supported by Security Device Container monitoring.

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 conveyance doors.

Trade-Lane Pre-Deployment Test – Vendor/shipper field test to verify that the Security Device System meets the Security Device Requirements within the context of the proposed Trade-Lane environment, per Sections 16 and 17.

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 Conveyance 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. (See [4])

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

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).

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

10 References

[1] Garcia, M.L., *The Design and Evaluation of Physical Protection Systems,* ISBM 0-7506-7367-2, Elsevier Science, 2001.

[2] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* May 25,2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] FIPS PUBS 197, *Specification for the Advanced Encryption Standard (AES),* November 26, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] *Security Device (CSD/ACSD) Communications Interface Control Document (ICD) Security Device-to-Network Access Device (NAD), Final Draft*; Version 8.0; November, 2010

[5] *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.

[6] *Cargo Security Network Access Device Requirements*; Department of Homeland Security, Science and Technology Directorate; September, 2010.

[7] *Cargo Security Network Communications Key Management and Data Security Report*; Department of Homeland Security, Science and Technology Directorate; March, 2010.

[8] *Marine Asset Tag Tracking System (MATTS) Requirements Document*; Department of Homeland Security, Science and Technology Directorate.

[9] ISO/IEC 6346:1995 *Freight Containers – Coding, Identification, and Marking*

[10] *International Standard of Classification of environmental conditions (IEC 60721-2-1): Environmental conditions appearing in nature – Temperature and humidity,* International Electrotechnical Commission (IEC), edition 1.1, October 2002.

[11] *International Standard of Classification of environmental conditions Part 3: Classification of groups of environmental parameters and their severities, Section 2: Transportation (IEC60721-3-2)*, International Electrotechnical Commission (IEC), Second edition, March 1993.

[12] *International Standard of Classification of environmental conditions Part 3: Classification of groups of environmental parameters and their severities, Section 6: Ship environment (IEC60721-3-6)*; International Electrotechnical Commission (IEC); First edition, Amendment 2; November 1996.

[13] Utah Climate Center, http://climate.usurf.usu.edu/products/data.php

[14] *Fixed Reader Reduced Environmental Requirements Document*, 2010

[15] *Handheld Reduced Environmental Requirements Document*, 2010

11 Acronyms

ACSD	Advanced Container Security Device
AES	Advanced Encryption Standard
CBP	Customs and Border Protection
CM	Communications Module
CSD	Container Security Device
CSI	Container Security Initiative
CSTE	Cargo Security Test and Evaluation
C-TPAT	Customs-Trade Partnership Against Terrorism
DCP	DHS-designated Data Consolidation Points
DHS	Department of Homeland Security
DNS	Domain Name Services
EMI	Electromagnetic Interference
EMR	Electromagnetic Radiation
FIPS	Federal Information Processing Standard
FFD	Full Function Device
GTS	Guaranteed Time Slots
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to Personnel
HNAD	Handheld Network Access Device
ICD	Interface Control Document
ID	Identification
IDART	Information Design Assurance Red Team
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMO	International Maritime Organization
IP	Internet Protocol
ISO	International Organization for Standardization
ISPS	International Shipping and Ports Security
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LAN	Local Area Network
LS	Locking Seal
MAC	Medium Access Control Layer
MTSA	Maritime Transportation Security Act
NAD	Network Access Device
NTC	National Targeting Center
OSI	Open System Interconnection
P_d	Probability of Detection
P_{fa}	Probability of False Alarm
PHY	Physical Protocol Layer

PoA	Port of Arrival
PoS	Point of Stuffing
RF	Radio Frequency
RFD	Reduced Function Device
RFID	Radio Frequency Identification
S&T	Science and Technology Directorate
SOP	Standard Operating Procedure
SVA	Security Vulnerability Assessment
UTC/GMT	Coordinated Universal Time
UID	Unique Identifier
WAN	Wide Area Network

12 Appendix A – ISO Dry Freight Containers

A specified subset of ISO 668 series 1 freight containers (Reference ISO 668:1995(E)) with the dimensions described below:

- Series 1A:
  - External dimension: 8 ft (height) x 8 ft (width) x 40 ft (length)
  - Minimum internal dimensions: 7.2 ft (height) x 7.6 ft (width) x 39.4 ft (length)
- Series 1AA:
  - External dimension: 8.5 ft (height) x 8 ft (width) x 40 ft (length)
  - Minimum internal dimensions: 7.2 ft (height) x 7.6 ft (width) x 39.4 ft (length)
- Series 1CC:
  - External dimension: 8.5 ft (height) x 8 ft (width) x 20 ft (length)
  - Minimum internal dimensions: 7.2 (height) x 7.6 ft (width) x 19.2 ft (length)
- Series 1C:
  - External dimension: 8 ft (height) x 8 ft (width) x 20 ft (length)
  - Minimum internal dimensions: 7.2 (height) x 7.6 ft (width) x 19.2 ft (length)
- Series 1AAA (40 ft high cube):
  - External dimension: 9.5 ft (height) x 8 ft (width) x 40 ft (length)
  - Minimum internal dimensions: 8.7 ft (height) x 7.6 ft (width) x 39.4 ft (length)
- Series 1BBB (30 ft high cube):
  - External dimension: 9.5 ft (height) x 8 ft (width) x 30 ft (length)
  - Minimum internal dimensions: 8.7 ft (height) x 7.6 ft (width) x 29.3 ft (length)

13 Appendix B – Environmental Requirements Discussion

To determine Security Device environmental requirements, subject matter experts and reference material were consulted to establish realistic levels for climate and operational conditions known to be problematic for electronic sensing and communication devices in the global shipping environment. Care was taken to ensure that a Security Device that survived and functioned in the prescribed conditions would survive and function in the environment intended for use. To establish a relationship between Security Device performance and internationally recognized climactic conditions, the IEC climate classes from [10], [11], and [12] that encompass the climactic conditions expected to be experienced by these devices were used to establish the levels listed for the environmental requirements. This appendix is an explanation of the reasoning behind the environmental requirements and their levels, with the intent of showing that a sound and reasoned approach was used in their determination, and that all are needed to ensure that a compliant Security Device will operate in all conditions likely to be encountered.

The environmental conditions to which a Security Device may be subjected can be extremely harsh and difficult to characterize. In addition to the requirements detailed in Section 7.3, this appendix provides further information about the environmental characteristics and supporting information for why the specified values were chosen for the Security Device environmental requirements. The relevant Specifications referenced within Section 10 and Appendix B are from the International Electrotechnical Commission (IEC). Security Devices within the global supply chain will encounter many of these and failure to operate and/or survive will affect the performance assessment of the Security Device.

Security Device Temperature Range, Thermal Shock, and Humidity:

Temperature:

The temperature ranges were selected based on global climatograms, which indicated the most representative category for defining the climatological extremes. The coldest climate encountered in the global shipping environment is classified in a climate category referred to as "Cold". The following ports have Cold climates: Qasigiannquit, Greenland; Dikson, Russia; Tiksi, Russia; Pevek, Russia; and Kotzebue, Alaska. The warmest climates encountered in the global shipping environment are in the "Extremely Warm Dry" IEC climate category. The following ports have Extremely Warm Dry climates: Benito, Equatorial Guinea, Africa; Port Gentil, Gabon, Africa; Port of Santana, Brazil, South America; Port of Cayenne, French Guiana, South America; Port of Sitra, Bahrain; and Port of Shuwaikh, Kuwait. IEC 60721-2-1 Table 3 indicates that the absolute extreme low temperature for a Cold climate is -60°C and that the absolute extreme high temperature for an Extremely Warm Dry climate is +60°C. This base range of temperatures was modified for the existing requirements to account for solar heating and partial-to-full enclosure of the devices. In warmer weather the extreme temperature could be as much as 30 degrees warmer (hence the +70°C for Operate and +85°C for Survive requirements respectively), and in cold weather, containment and general insulation from the elements, due to conveyance frame and cargo, provided the basis for modifications to the cold temperatures (hence the -40°C for Operate and -50°C for Survive requirements respectively). Additionally, while actual temperatures in the operational environment can occasionally be lower than the stipulated low end, -40°C was chosen as the lowest required operational temperature due to the lack of commercially available rugged batteries that can perform below that temperature.

Overall, the listed conditions equate to the climatic classes of 5K3 and 5K4 from IEC 60721-3-5, which are equivalent to classes 2K4 and 2K5 in IEC 60721-3-2, as listed in the requirements.

From *IEC 60721-3-2, Table 2 – Classification of climatic conditions*, the two most relevant climatic classes are 2K4 and 2K5, which cover transportation in weather-protected and non-weather-protected conditions with temperatures as low as -65°C (which is lower than the Security Device's -50°C "survive" temperature), and as high as +85°C, with relative humidity of 95%. It is an expert opinion that temperatures as low as -65°C and as high as 85°C will rarely, if ever, be experienced by Security Devices. Therefore, environment 2K4 is used as a guideline for the operational range of the Security Device 2K5 and is referenced for the upper bound on the survive range (85°C). The lower bound (-50°C) for the survive range is based to some extent on input from subject matter experts (SMEs). IEC 60068-2-14 and SME input were used to determine the time durations for both cyclic temperature testing and thermal shock.

Thermal Shock:

The intent of the Security Device thermal shock requirement is to ensure Security Device operation as the conveyance and onboard Security Device is moved back and forth between indoors, at an assumed "room temperature" of 20°C, and outdoors, at either the high or the low specified extreme operational temperature. This is the primary and most severe thermal shock likely to be seen while in use, and is likely to occur when a conveyance is moved either before or after stuffing or unstuffing at a temperature-controlled warehouse-type facility, or when a hot conveyance is splashed with cold water. Failures accelerated or caused by thermal shock include cracking and rupturing, delamination of coatings, and degradation of thermal and vacuum seals.

Humidity:

The intent of the Security Device humidity requirement is to ensure Security Device operation in the presence of high humidity, such as at the Port of Singapore, Singapore, and Southeast Asia, where the relative humidity can reach 100%. Water will almost certainly cause problems—e.g., lowered resistance between circuit board traces and component leads, metal and electronic corrosion, shorted leads—if it reaches device electronics. Although humid air will not necessarily cause the same problems as liquid water, air at the specified 95% relative humidity carries sufficient water to cause problems with water-sensitive components and will penetrate some barriers that stop liquid water. Such water-saturated air is at the dew point; i.e., liquid water will condense given the slightest reduction in temperature. This would happen if, for example, such air were to come in contact with interior Security Device surfaces a degree or two cooler than ambient temperatures. Condensation on optical sensor lenses or optical viewing ports could impede proper operation of the sensor. The entire operational temperature range is specified in the humidity requirement because air can be water-saturated to 95% of its capacity at any given temperature.

Structural Vibration and Mechanical Shock Environments:

Shock:

The intent of the Security Device shock requirement is to ensure Security Device operation in case of shock to the conveyance or the device itself, either prior to or during installation. Shock is essentially sudden and rapid acceleration or deceleration, and can be caused, for example, by impact or explosion. Examples of high-impact scenarios apt to be seen by the devices include handling drops of the device onto a hard surface and accidental drops of the entire conveyance after the device has been installed. Container drops may include scenarios where a conveyance is accidentally dropped from a partially raised crane, as well as the more likely scenario where a conveyance is more-or-less purposely dropped onto the top of another conveyance or onto the ground while being moved. The conveyance may be full or it may be empty. Specified drop heights and conditions are based on likely handling drop heights (which may occur, e.g., when the Security Device is being installed) and on conveyance drop tests that determined empirical limits on the shock a conveyance can endure and still be certified as fit for use. The peak acceleration and duration of these drop scenarios were calculated from finite element models and verified with actual conveyance drop tests. The resultant impact damage to the device can cause various forms of physical damage, including electrical subsystem damage (e.g., solder failure of board-level components; power connections loosening or unplugging, or breaking) and mechanical damage (e.g., breakage or dislocation of the device housing, sensors, antenna, or other components).

From IEC 60721-1 Table 1, Subpart 6 – Mechanical conditions, 6.1.3 *Non-stationary vibration, including shock*, the Spectrum type III for shocks with short duration and high peak acceleration is an example of the same type of shock as the drop shock. The shock testing guidelines were obtained from data gathered during actual conveyance drop tests.

Vibration:

The intent of the Security Device vibration requirement is to ensure device operation when subjected to the vibration regime encountered during transport, including scenarios where trucks carrying conveyances with devices on them are driven over rural, non well-developed roads, such as may be seen on the way to such ports as those in Brazil getting cargo from the Amazon. This requirement also addresses vibration conditions that occur on rail lines and potential shipboard vibration levels where conveyances may experience vibration stimulus from engine rooms or other mechanical sources. Possible damage incurred as the result of vibration includes mechanical damage of electrical subsystems (the same as for shock, listed above), the loosening of housing closures or loosening of the attachment of the device to the conveyance. As it is highly likely a device will experience various levels of vibration throughout its usage, the total of which would exceed the duration of the test, the requirement, as stated, constitutes accelerated conditions, so as to accomplish the assessment in less time.

IEC 60721-3-2, Table 5 – Classification of mechanical conditions, *Stationary vibration, random,* class 2M3, covers mechanical loading, transportation in aircraft, various lorries, trucks and trailers (both in areas with and without well-developed roads), and transportation by trains and ships, and gives acceleration spectral density of $3m^2/s^3$ over the frequency range of 10 to 200 Hz, and $1m^2/s^3$ over the frequency range 200 to 2000Hz.

Precipitation Environments:

Salt Mist:

The intent of the Security Device salt mist requirement is to ensure Security Device operation when subjected to corrosive environments encountered in the global shipping environment, primarily salt-saturated, humid sea air and salt-water spray. Salt mist is conducive to corrosion and is commonly used as a general stand-in for corrosive environments of all types. Experience has shown that devices able to function in salt mist do well in all corrosive conditions. Salt mist is especially injurious to electrical and electro-mechanical components and can cause short circuits more readily than water vapor without salt. The concentration of salt in the specified salt mist exceeds concentrations likely to be encountered in normal oceanic conditions, but this provides some assurance that the Security Device will function not only in even the most severe oceanic conditions but also in other corrosive environments that may be encountered in industrial settings. Typical storage and transport conditions can often lead to racking conditions where conveyance doors and/or frames are slightly bowed, providing open space where salt mist or salt spray (or other corrosives) may enter the conveyance, not to mention the already present vapors from conveyance cleaning.

From IEC 60721-1 Table 1, Subpart 3 – Chemically active substances, 3.1, *Sea Salt,* the general value given for the concentration in air is 0.3 g/m^3.

Rain:

The intent of the Security Device rain requirement is to ensure Security Device operation in the presence of rain as it will be encountered in the global shipping environment. Rain is a threat because water penetrating the device will damage electronics and electro-mechanics and because water droplets on the Security Device exterior could prevent device function (e.g., liquid water might block sensing or communication apertures). Specified rainfall rates equal or exceed maximum global rainfall rates, which, similar to the vibration requirement above, constitute an accelerated test for this condition, as a device is likely to experience a total accumulated exposure to rain during usage greater than what is likely for any single rain event.

From IEC 60721-3-6 Table 1 – Classification of climatic conditions, for the 6K5 climate class (which encompasses 2K5 from IEC 60721-3-2 mentioned above), the value for rain precipitation is 15 mm/min.

Impacting Water:

The intent of the Security Device impacting-water requirement is to ensure Security Device operation in the presence of high-velocity water, such as waves and cleaning jets. High-velocity water can penetrate barriers not penetrated under simple exposure conditions, and a high-pressure stream can cause mechanical damage, such as knocking components from the device or knocking the device loose from the conveyance.

From IEC 60721-3-6 Table I – Classification of climatic conditions, for the established 6K5 climate class, the value for water from sources other than rain is 10 m/s, and from Table III – Classification of chemically active substances, Substances in water, *Sea salt,* for the class 6C3, which covers both weather-protected and non-weather-protected installations on ships, has a concentration value of 30kg/m^3.

Frost/Ice:

The intent of the Security Device frost and ice requirement is to ensure Security Device operation under frost formation conditions. The requirement specifies conditions under which ice or frost may form on or in the device. Frost inside the device could mechanically or electrically interfere with device function and cause moisture problems when it thaws. Exterior frost could impair the operation of sensors and antennae.

From IEC 60721-1 Table 1, Subpart 1.10, *Formation of ice and frost,* ice and frost formation is due to influences from external sources.

Sand and Dust:

The intent of the Security Device sand and dust requirement is to ensure Security Device operation in the presence of airborne sand and dust, which is found in dust storms, industrial operations such as insulation manufacturing and furniture making, and ground travel over unpaved roads. Particulate matter inside the device could mechanically interfere with the function of internal components and could block sensors, vents, and antennae. Specified dust levels, although high compared to dust sources named above, are consistent with levels specified elsewhere that have proven successful in terms of device lifetime performance assessments.

IEC 60721-3-6 Table IV – Classification of mechanically active substances, class 6S3 encompasses 6S2 and additionally covers weather-protected and non-weather-protected installations, including those on ships operating close to sand deserts, which encompasses the expected environment, and gives 10 g/m^3 for sand in air and 3.0 mg/(m^2 h) for dust sedimentation.

Fungus:

The intent of the Security Device fungus requirement is to ensure Security Device operation under conditions where fungus can form. The fungus requirement describes two conditions conducive to fungus growth: first, where spores are provided and any fungal medium that may be present will subsequently grow fungus; second, where both spores and medium are provided such that fungal growth will almost certainly occur. The first condition is to test whether the device itself provides a function-threatening medium and the second is to test whether fungus growth inhibits device function. Fungus growth, like moisture and dust particles, may interfere with the function of internal components and with communications or sensing capabilities even if fungus does not grow inside the device. It is virtually impossible to guarantee function under all conditions of fungus growth because of the large variety of fungal types, but this requirement attempts to cover those most likely to occur.

IEC 60721-3-6 Table II – Classification of biological conditions, class 6B2 covers installations in ships, both protected and non-protected, operating in areas where mold growth may occur, so the presence of mold or fungus is to be assessed. The fungal environment given in section 10 is provided as an example.

Radiation and Electromagnetic Environments:

IEC 61000-6-2 Table 1 – Immunity – Enclosure ports; covers electromagnetic compatibility (EMC) immunity requirements for apparatus in an industrial environment, of which ships and shipping ports can reasonably be characterized as members. Because Security Devices are battery operated standalone units, and are specified to be completely enclosed, they can reasonably be classified as a special type of enclosure port (IEC 61000-6-2, Section 3.2) for EMC testing purposes, where enclosure port is defined as the physical boundary of the apparatus which electromagnetic fields may radiate through or impinge on. As such, the values in Table 1 are applicable to expected usage conditions and have also been, where indicated below and in Section 10, expanded or modified for specific aspects of the anticipated environment not covered by Table 1.

Radiated Emissions:

The intent of the Security Device radiated emissions requirement is to ensure Security Device radio operations comply with all radio bandwidth, frequency, and power restrictions globally.

Radio emissions can interfere with other radio frequency-dependant processes and some electronics, depending on the frequency and power of the emissions. The Security Device must not exceed legal limits imposed by all governments (see, for example, 47 CFR Part 15, the U.S. FCC ruling on radio frequency emissions limitations) and other authoritative agencies (international radio frequency emission limits to avoid interference with ship operations). The specified limits permit Security Device operation in all radio environments found globally.

The intent of the Security Device HERO compatibility requirement is to assess if Security Device radio emissions in areas where certain types of ordnance may be present pose a danger, because radio emissions at certain frequencies and power levels can affect susceptible ordnance.

47 CFR Part 15 contains details of the FCC Rules covering radio frequency devices, which Security Devices will be subject to, so the applicable limits contained therein are considered as part of the global supply chain environment in which Security Devices will be expected to operate. IEC 60533 specifically addresses equipment in use or installed on ships, and as Security Devices will effectively be such equipment once deployed and while in transit for a shipment, the emission limits detailed in Tables 2 and 3 (covering the locations in the bridge and deck zone, and the general power distribution zone) are applicable. IEC 61967-3 covers measurement of radiated emissions by the surface scan method, and can be used to determine if a Security Device meets the applicable requirements.

Radiated Susceptibility:

The intent of the Security Device radiated susceptibility requirement is to ensure Security Device operation where radio energy not emitted by the Security Device is likely to be present. Device electronics not designed to operate in the presence of the radio emissions found in the global environment could easily malfunction, especially while communicating, since significant power is emitted at certain frequencies and locations.

IEC 61000-6-2 Table 1, Subparts 1.1 – 1.4, specify requirements and performance criteria for power-frequency magnetic field immunity and radio-frequency (RF) electromagnetic field immunity. As stated under the Remarks column, Subpart 1.1, the test frequency should be appropriate to the power supply frequency anticipated on ships and in shipping ports. As given in IEC 61000-4-8, Section 5 and Annex C, power-frequency magnetic field immunity test levels for Security Devices nominally fall under Class 4 and 5. The frequency range for RF field immunity is expanded as necessary to cover that anticipated in ports. As given in IEC 61000-4-3, Section 5 and Annex E, Section E.2, test levels for Security Devices nominally fall under Class 3 and 4. Also as noted in Section E.4, test levels are expanded as necessary to account for high power fixed transmitters on ships and in port environments. Additional justification for field test levels is given in IEC 61000-2-5, Annex A, Section A.5 (ships and ports can reasonably be characterized as a “Location class type 5”), then using guidance from Table A.5, HF-radiated oscillatory emissions (being representative of radio-frequency EM fields), to get the disturbance degrees for this type of location, and applying it to Annex B, Table B.1, the associated field levels can be obtained.

Static Electricity:

The intent of the Security Device static electricity requirement is to ensure Security Device operation in the presence of electrostatic discharge. Surprisingly low levels of electrostatic discharge can harm electronics not designed to withstand it. The specified values cover conditions that may be encountered throughout the global shipping environment as individuals and other objects with a net static charge create a discharge on or around a device.

IEC 61000-6-2 Table 1, Subpart 1.5 (contact discharge) specifies requirements and performance criteria for electrostatic discharge (ESD) immunity. IEC 61000-4-2 outlines stipulations and procedures for the preferred contact discharge test method.

Lightning:

The intent of the Security Device lightning requirement is to ensure Security Device operation in the presence of nearby lightning strikes. A lightning strike causes a transient electromagnetic field, which can harm device electronics not designed to withstand such fields. It is nearly impossible to design electronics that can withstand a direct or very close lightning strike because power levels and field strengths are very high; however such an event is unlikely.

IEC 61000-4-9 specifies pulse magnetic field immunity test requirements and gives recommended levels for industrial installations and power plants as well as for medium and high voltage sub-stations. Subject Matter Experts(SMEs) have calculated the peak amplitude current and resulting transient magnetic field of a typical lightning strike at a distance of 100m, which levels have been designated for this test. Additional background information and justification can be obtained from IEC 61000-2-7, Section 4, Natural phenomena.

Total Radiation Exposure:

The intent of the Security Device total radiation exposure requirement is to ensure Security Device operation as it is exposed over its operational life to radiation from radiation-based detection equipment used around and on conveyances. Radiation-induced problems include rapid deterioration, communication dropouts, spurious signals, processor failure, permanent processor flaws, and complete loss of function. The specified total dose is consistent with detection equipment likely to be encountered and the number of exposures implied by the Security Device’s design lifetime and concept of operations.

Radiation Dose Rate:

The intent of the Security Device dose rate requirement is to ensure Security Device operation subjected to radiation at dose rates consistent with individual scans from radiation-based detection equipment (such as X-ray scanners used at shipping ports) used around and on conveyances in the shipping environment. The requirement is consistent with and similar to the preceding cumulative dose rate requirement, except that the specified value here refers to a single dose rather than a cumulative dose.

SOLAS:

The intent of the Security Device SOLAS requirement is to ensure that the Security Device will not ignite any flammable vapors or aerosolized solids that may be present inside ISO 668 container due to cargo out gassing or handling, or on shipboard environments. Essentially, during the process of operation the Security Device will not produce sparks or point heat sources sufficient to cause ignition, or open flames.

14 Appendix C – Red Team Vulnerability Assessment

14.1 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 an application to DHS for approval. If the application is accepted, then DHS will need devices/systems as specified in Section 17 to perform vulnerability tests. DHS vulnerability tests will include red team assessments, which are described in more detail in this section.

14.2 Background

The DHS Container Security Test and Evaluation (CSTE) Team routinely performs red team assessments for Security 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, which takes place during the first two steps of red teaming. 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, is allowed a greater amount of time and resources. Although the specific tests performed during red teaming are not predetermined and are based upon the technologies involved, there are defined processes for selection and validation of these 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 system. The results of these tests allow for a better understanding of the risks associated with using the corresponding device or system 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.

14.3 Objectives

The purpose of defeat testing is to determine whether a Security Device can be defeated by an adversary with limited resources. The information obtained will be helpful in identifying how difficult it is to defeat the Security Device, the capabilities an adversary needs to defeat the Security Device, and the amount of time and effort required to defeat the Security Device. Defeat testing is the first step in the Red Team process and 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:

- Explore potential vulnerabilities
- Determine whether a security device can be defeated by an adversary with minimal resources
- Identify a high consequence vulnerability that can be exploited by a low to medium level adversary
- 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 Security 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:

- Identify multiple attack paths graded by level of adversary
- Identify critical points of failure
- Identify the strengths and weaknesses of a system
- Determine whether a security device can be defeated by a program-specified level of adversary

14.4 Red Team Methodology

According to the Information Design Assurance Red Team (IDART) TM methodology[8], 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.

14.4.1 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 system under evaluation, and understand what goals an adversary might attempt.

14.4.2 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 system architecture. Open-source information and customer/vendor provided information are used to gain system understanding. Defeat testing is done during this step as well.

Defeat testing is a subset of red teaming and 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. It is designed to find simple attacks that will circumvent a critical component or function of the system. 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

Defeat testing provides data collection, introductory views, and system understanding for the 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,

[8] http://www.sandia.gov/idart/method.html

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.

14.4.3 Characterization

The system 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.

14.4.4 Analysis

The team analyzes the viewpoints and the system 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 Security Device System from a security perspective are an essential part of the design. If it does not fulfill the fundamental security requirements, the Security Device System does not fulfill its mission. In general, an adversary may have the following high-level goals when attacking the Security Device System:

1. Affect the integrity of the system by generating false alarms
2. Prevent Security Device sensors from sensing any door opening or removal
3. Prevent Security Device sensor algorithms from determining an alarm condition exists
4. Erase an alarm in the Security Device log before the next communication opportunity
5. Prevent the Security Device from communicating its alarm state to DHS
6. Tamper with or delete the alarm message during its transmission from the Security Device to DHS systems or users

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

14.4.5 Report

The analysis results are recorded in a report that will include details on the techniques used against the system. This includes the contents of the attack graph. DHS will use this report as a decision aid to determine if further testing is required, one or more attacks may be implemented to verify their effectiveness, and the results of these tests will be added to the report as well. This report will not be released to the applicant.

14.4.6 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 system 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.

DHS reserves the right to disclose a summary of the test results via an oral debrief to the applicant. Written reports that provide detailed test procedures and results will not be released.

15 Appendix D – Risk Assessment of the Deployed Security Device

15.1 Introduction

DHS will assess the potential vulnerabilities of vendor devices offered for use in the Trade Lanes. That said, both the vendor and the government benefit if the vendor seeks to identify and address vulnerabilities prior to delivering a device for test and evaluation.

Vendors are encouraged to assess the potential vulnerabilities of their designs at every stage of the development lifecycle: concept, design, prototyping, production, operations, and disposal. Almost without fail, fixing a consequential vulnerability after a design is operational will cost much more than if the vulnerability had been identified before manufacturing began.

Although a vendor may use any approach to assess potential vulnerabilities, we suggest an approach that is *structured*, to ensure the evaluation process is consistent, and *documented*. A team using an approach that is not structured and documented is likely to revisit some issues repeatedly and overlook others.

Few development teams can pursue potential vulnerabilities indefinitely. Just the process of selecting an approach to analyzing vulnerabilities can upset budget and schedule. The approach below provides a general structure that addresses the primary issues of interest yet can be adapted to fit a wide variety of situations.

15.2 Analyze and Address the Device's Vulnerabilities

The approach we discuss here has four main steps:

- identify possible attacks,
- characterize each attack,
- assess the relative risk of each attack, and
- estimate the amount of effort required to address the attacks that offer the greatest risk.

Figure 1 summarizes the approach graphically. The dark squares represent the main steps, the lighter squares represent secondary steps, and the text items represent inputs and outputs. The goal of this process, of course, is to address the most worrisome and easily fixed attacks first.

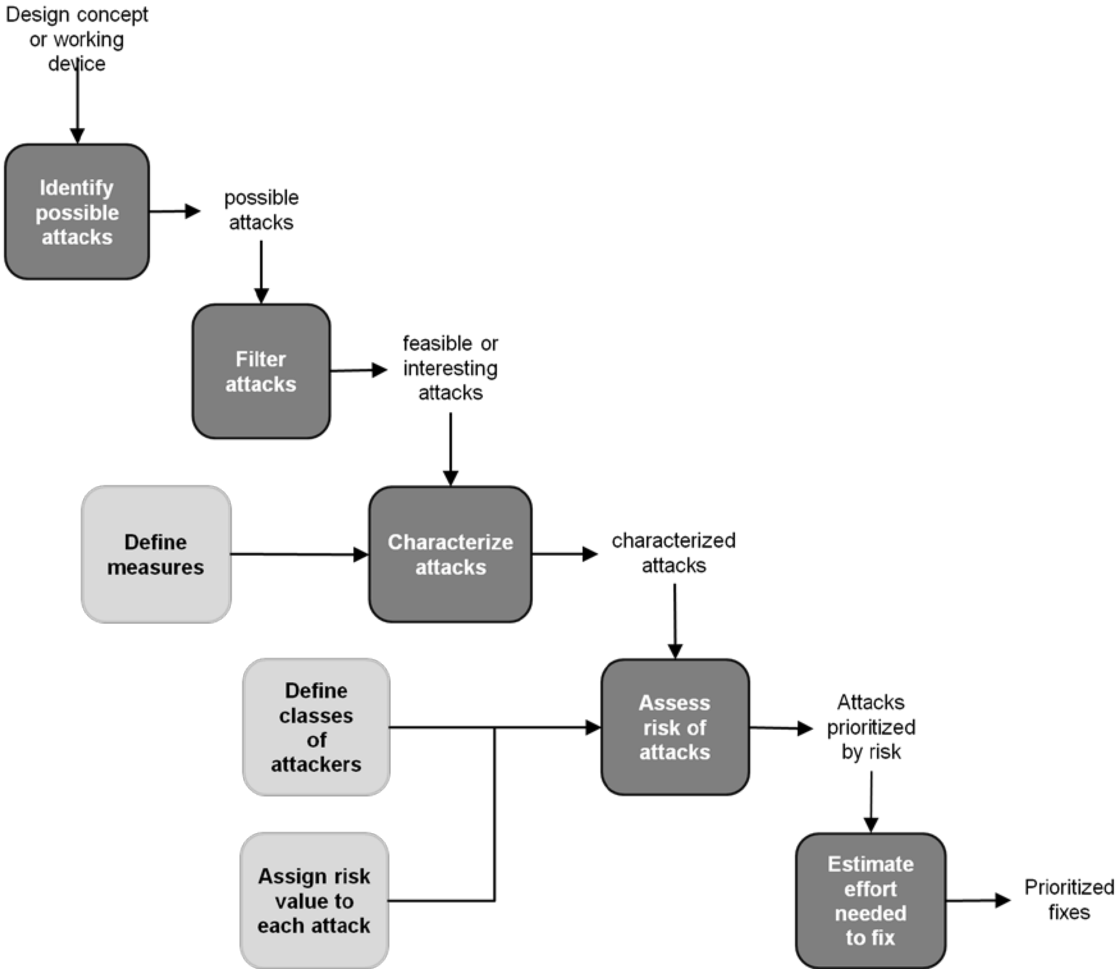

Design concept or working device
Identify possible attacks
possible attacks
Filter attacks
feasible or interesting attacks
Define measures
Characterize attacks
characterized attacks
Define classes of attackers
Assess risk of attacks
Attacks prioritized by risk
Assign risk value to each attack
Estimate effort needed to fix
Prioritized fixes

Figure 15-1: A general risk analysis process

15.2.1 Identify Possible Attacks

The first step is to brainstorm possible attacks against the device. This activity differs fundamentally from any safety and reliability analyses the team might undertake. Here, the team seeks to identify ways an *attacker* might negate, undermine, circumvent, or misuse the device. The attacker might exploit a safety or reliability issue, but the attacker's primary intent is not merely to produce an unsafe condition, but to deny completion of the device mission.

Should the same team that developed the device also assess its vulnerabilities? While this is a matter of preference and circumstance, the management team should consider two principles:

- the development team understands the device better than anyone else, and
- the development team will tend to favor the device it developed.

The tension between these principles can be partly alleviated by staffing the vulnerability assessment team with members of the development team and "outsiders" (informed technologists or operators who did not help develop the device).

Teams assigned the task of identifying vulnerabilities may be tempted to pursue this task informally. We recommend against this. Even minimal process structure will provide results that are more complete and consistent. Foremost, the vulnerability team should consider whether its work will help the development and management teams analyze the tradeoffs and manage the decisions that are certain to follow the vulnerability assessment. Simply poking random holes in the device might expose some weaknesses in the device but won't necessarily lead to informed decisions.

Accordingly, the team should begin by brainstorming possible attacks against the device using a structured technique. A technique that is either diagrammatic or supported by diagrammatic tools—e.g., attack trees, fishbone diagrams, or concept maps—is recommended. Regardless of which technique the team chooses, the aim should be to document all of its efforts. Group settings in which a facilitator maintains the diagram, document, or model can be very productive.

Brainstorming rules apply at this stage. The team should not seek to criticize or filter the ideas until the next step, and team members should feel free to propose ideas without fear of censure or criticism. Diagrammatic models help team members associate ideas with one another and develop the notional space of solutions.

15.2.2 Filter Attacks

The team should it filter its attack ideas only when the initial brainstorm has been completed. Ad hoc, informal filtering is quick, but it can lead to inconsistent decisions. A simple table in which each attack is roughly and rapidly assessed for feasibility is often sufficient to balance speed and consistency. If the group generates an unwieldy number of possible attacks, the team may wish to undertake two rounds of filtering: an initial, informal round in which clearly infeasible attacks are simply removed from the list, and a second, somewhat more structured round in which the attacks are tabulated and assessed by some common measure of feasibility.

15.2.3 Characterize Attacks

At this point the team has generated a list of possible attacks that has been reduced to a manageable size based on a rough measure of feasibility. Here, the team looks at each of the remaining attacks in greater detail. The team should identify a few observable measures of performance that it will use to separate worthwhile attacks from insignificant ones.

Example measures include the estimated cost of the attack, its relative chance of success, and its effect. The team may then assign the following values to *attack A and attack B* using these measures, as shown in the following table.

	Cost to develop and implement	*Success rate*	*Effect*
Attack A	$1,000	0.4	Completely disable device without leaving a trace
Attack B	$400	0.6	Temporarily disable device.

Table 15-1: Example of characterized attacks

This is undeniably a modest method. Teams wishing to engage in more refined analysis may choose to generate the values based on explicit observations. Allowing for uncertainty in the estimates would further refine the approach. This takes time, however, and it may be necessary to forego refinement for efficiency.

In the interest of both efficiency and effectiveness, we encourage teams to focus their assessment efforts on the most consequential attacks—attacks that could render the device inoperative or ineffective. Teams should remember that the overarching goal is to identify and address the most consequential attacks during the design phase; the cost to remediate flaws only grows if the flaws remain unidentified and unaddressed. To be effective, teams must think in terms of both technical and operational functions. They must consider how the device is likely to be employed and how attackers might exploit that setting. They must also do their best to shed the designer's perspective and approach the device as an attacker would.

15.2.4 Assess Risk of Attacks

At this point the team will have a list of the most consequential attacks characterized by estimated values for the attack performance measures. The team can either simply review the table and order the attacks subjectively or perform a more formal decision analysis. A variety of decision analysis techniques exist that will not be detailed here.

A common decision analysis strategy is to weight each measure and score each alternative (the attacks in this case) based on the sum of the weighted values. Using the measures above, for example, the team may decide to assign *cost* a relative weight of two, *success rate* a relative weight of one, and *effect* a relative weight of three. This approach is limited, however, and teams may again choose to adopt a more refined approach.

Teams may also wish to consider different classes of attackers. A wealthy attacker might not balk at an attack costing $1 million while a petty thief certainly would. A petty thief, on the other hand, might be willing to undertake attacks with a much lower success rate. As a general rule, teams should focus on attacks that can be executed by low- to mid-range attackers, because they are the most likely to be attempted in the real world, especially if they appear to be effective. Costly, technically complex attacks requiring deep knowledge, time commitment, and costly development are less likely to be attempted, in large part because fewer attackers can afford to pursue them, but even a sophisticated, wealthy attacker will prefer a cheap, easy attack to one that's costly and complicated.

15.2.5 Estimate Effort Needed to Fix

The team now has an ordered list of attacks. Some of the vulnerabilities associated with these attacks will be easier to fix than others. The design team must therefore review the vulnerabilities and estimate the amount of effort required to eliminate them. A table such as the one shown here can help the team associate the vulnerabilities, attacks, and fixes.

Vulnerability	Attacks	Fix	Ease of fix
1	A		Hard
2	B		Easy
3	C		Hard
4	D		Easy

Table 15-2: Structure for prioritizing vulnerability fixes

One method of prioritizing the fixes is to map them relative to the relative risk of the attack. What the team would be looking for are the immediate fixes: high risk attacks that are easy to address. Figure 2 illustrates this approach diagrammatically. The vertical axis represents the estimated ease of fix (*easy* to *hard*). The horizontal axis represents the risk associated with the attack (*low* to *high*). Four attacks are shown. Attack A is characterized as *low risk*, *hard fix*, attack B as *low risk*, *easy fix*, attack C as *high risk*, *hard fix*, and attack D as *high risk*, *easy fix*. Of these four attacks, attack A arguably represents the least immediate priority. Attack D is arguably the most immediate. Attack C is hard to fix, but it also has high consequence. The team may need to address this vulnerability by reconsidering the device's basic design.

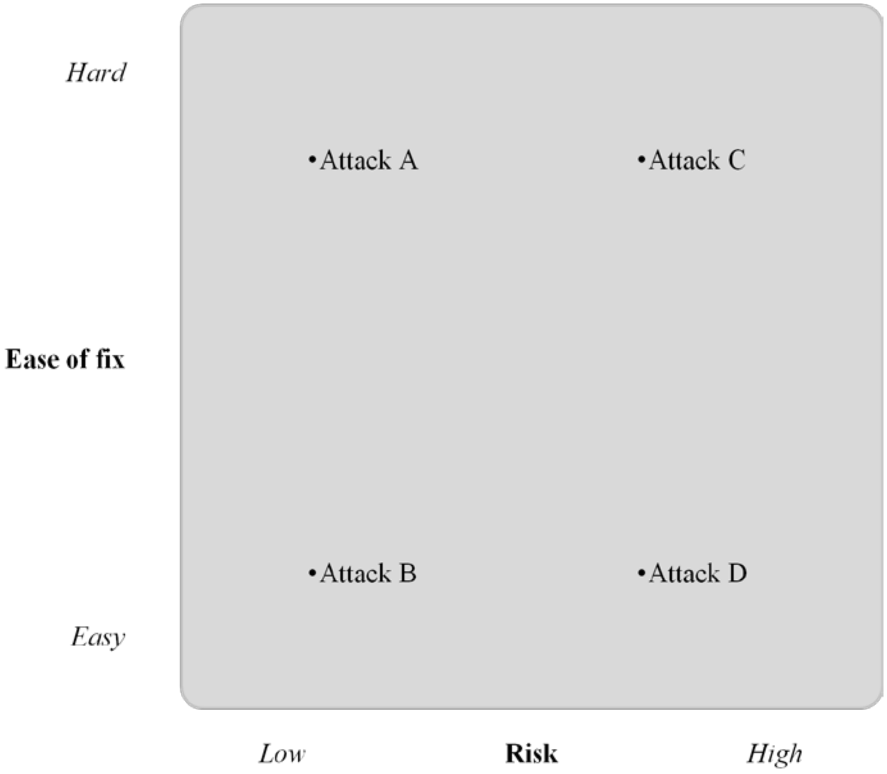


Figure 15-2: Risk vs. Ease-of-fix

Of course, real life is rarely this simple. Multiple attacks may be associated with the same vulnerability, or a single attack may be associated with several vulnerabilities. The team should look for opportunities to address multiple vulnerabilities with single fixes.

15.3 Summary

The purpose of analyzing potential vulnerabilities during the design phase is twofold: it saves time and money in the long run, and it decreases the likelihood that a device with significant vulnerabilities is fielded. Moreover, devices that have been subjected to internal vulnerability review are likely to fare better during independent test and evaluation, especially if it involves Red Team analysis, as Trade-Lane Pre-Deployment Testing (Section 16) very well might.

The process outlined here is meant to guide teams toward a practical, structured, and documented approach that balances efficiency and effectiveness. This approach is offered as general guidance, leaving teams to adopt it whole, adapt it as circumstances warrant, or undertake another approach that meets the same ends.

16 Appendix E – Trade-Lane Pre-Deployment Test Guidelines

16.1 Trade-Lane Pre-Deployment Test Overview

This appendix contains DHS guidance to vendors regarding the Trade-Lane Pre-Deployment Test to be conducted by the vendor and/or shipper in order to obtain a Supply Chain Certificate.

16.1.1 Purpose

The purpose of the Trade-Lane Pre-Deployment Test is to verify that a vendor's Security Device System meets Security Device Requirements in the context of the proposed Trade-Lane environment. The test must specifically demonstrate the following capabilities:

- Network connectivity and data exchange with DHS-designated DCP(s) at all required CSI read points (PoS and PoA).
- Successfully integrate Security Device operations and equipment into importer's stuffing facilities and operations, per vendor SOP

16.1.2 Scope

This section describes the test objectives for the vendor Trade-Lane Pre-Deployment Test. This test applies only to Security Device Systems currently on the DHS-Approved Security Device Vendor List.

16.1.3 The Objective of the Trade-Lane Pre-Deployment Test

The overall objective of the Trade-Lane Pre-Deployment Test is to demonstrate Security Device System and shipper readiness, Supply Chain SOP implementation in the designated supply chain, and Security Device System compatibility with DHS data systems and interfaces.

16.1.4 Test Sizing and Number of Test Devices

To demonstrate Security Device System functionality in a Trade Lane, the vendor must document several armed Security Device transits that originate at a C-TPAT PoS and conclude at a designated PoA.

16.1.5 Test Scoring

To score a trip as successful or failed, it **Shall** be compared to a reference measure of acceptable performance that cover aspects unique to the Supply Chain SOP, its implementation, and the shipper, such as proper input and use of Trip Information, proper Arming of the Security Device, and the successful transmittal of Arming information from the point of stuffing (PoS).

Rigorous record-keeping at the PoS and destination is recommended so test observers can ascertain whether Security Device Data and shipment data are stored and identified as required.

The number of planned test trips (test sample size) should be set by the vendor to ensure sufficient insight into the Security Device's ability to integrate into the system within the test Trade Lane.

16.2 Roles and Responsibilities

The responsibility for determining successful demonstration resides with DHS. The vendor is responsible for all other aspects of the test planning, execution, and reporting.

16.2.1 Vendor/Shipper testing responsibilities

The vendor and/or shipper provide or arrange for the personnel and resources to support the implementation of their SOP. The vendor and/or shipper's responsibilities include the following:

- Implement all required aspects of the SOP
- Develop a test plan that addresses DHS objectives
- Develop & document test processes and test procedures to implement the test activities
- Provide the test articles and all necessary support equipment
- Comply with export control regulations as applicable to the Security Device system components, software, and documentation
- Identification, selection, and agreement-of-cooperation of the supply chain participant to comply with the vendor/shipper SOP.
- Install, or arrange and coordinate use of existing, equipment at field sites (PoS, CSI, PoA), as required
- Provide any necessary training to supply chain participants for the test as required
- Provide DHS with a comprehensive test participant list and participant roles and responsibilities
- Provide DHS with a detailed list containing Points of Contacts and contact information for each portion of each shipping route.
- Document and report test results, assessments, conclusions for DHS for review.

16.2.2 DHS testing responsibilities

DHS/CBP is the final authority to determine the results of the test. Specific DHS/CBP responsibilities include:

- Review the vendor application for approval, including the vendor Test Plan and Results
- Authorize vendor to execute the Test Plan
- Provide DCP test interfaces to support the test operations.
- Determine final results

16.3 Test Documentation

1. Test Plan

The vendor's Test Plan should be developed to satisfy DHS test objectives. DHS test objectives should be the basis for defining the necessary number of test articles, test trips, and data capture requirements. The Test Plan shall be submitted to DHS for review prior to execution of the test.

2. Standard Operating Procedures

The vendor should submit to DHS, with the Test Plan, the SOP for the Security Device system.

3. Test Plan and Procedures

The vendor's test plan, test processes, and test procedures should be based on and consistent with the Supply Chain SOP.

Test procedures should include sufficient structure and content to ensure that the verification process is reliable and repeatable.

4. Anomalies, Problems, and Failures

The vendor should implement a system for capturing, tracking, and documenting problems and issues that arise during the execution of the Trade-Lane Pre-Deployment Test.

The vendor should implement a failure-reporting system to document test article, procedural, or implementation deficiencies.

5. Risk Assessment

The vendor should submit a Risk Assessment of the device or system being tested consistent with the objectives and process described in *Appendix D – Risk Assessment of the Deployed Security Device*.

6. Inventory

Prior to the commencement of testing, the vendor should establish an inventory of specific test articles allocated to the Test. The traceability, test history, and dispositioning for every test article should be maintained in the inventory history and reported to DHS in the test report to be completed at the conclusion of the test.

7. Test Report

At the conclusion of the Trade-Lane Pre-Deployment Test, the vendor should generate and submit to DHS a test report to summarize the qualitative and quantitative results from test operations and the evaluation of the data. The test report should include:

- test logistics and organization
- test process and procedure
- A description of any specialized test or support equipment not covered in the SOP
- equipment configurations
- data collection activities
- data analysis and evaluation

8. Test Data & Results

The following data should be provided in the test report:

a. Test Article Inventory

   Test Article inventory history should trace all test articles from introduction to the test process through completion of test.

b. Summary of Test Anomalies and Failures

   The vendor should provide a summary of all test anomalies, failures, and operational problems including operator errors.

c. Critical Data

   - Number of Security Devices Tested
   - Total number of test trips and counts of how many were completed and successful
   - Security Device or Security Device System Functional Failures, with assessments of each
   - Procedural Failures with assessments of each
   - Summary of Communications at DCP Reader Interface Points

17 Appendix F – Supply Chain Certificate Application

The following sections provide an example of how a sponsoring agency could write an SOP, an application process, an approval process, and submittal guidelines for vendors who developed products using these requirements. The process/steps mentioned in this section may differ for various devices and the Security Device system is used only as an example. In these sections, DHS is used as the sponsoring agency. This is provided to aid agencies who might wish to use these requirements, as they are transitioned from use in Research and Development to use by government agencies and industry.

17.1 Standard Operating Procedures

All application submittals and requests for new Supply Chain Certificates will include SOP documents in accordance with Section 17.3. An SOP collects and details how the Security Device System is to be operated and maintained, and any implementation specifics that may be unique to a shipper and/or trade-lane.

DHS recognizes that SOP documents may be subject to some modifications and amendments, based on specific supply chain operations. Therefore, vendors included on an Approved Security Device Vendors List will also be required to submit an SOP for each C-TPAT member and their specific supply chain route(s) prior to commencing with authorized Security Device-equipped cargo movement operations, in accordance with Section 17.2.

1. Each Security Device System SOP **Shall** include the vendor company name and specific identification of the Security Device System and components (make, and model number, version, etc) for which the SOP is applicable.

   The SOP and Security Device equipped trade-lane operations are valid for only the identified Security Device and vendor system components, which must be on the DHS Approved Security Device Vendors List.
2. The Supply Chain SOP **Shall** indicate trade-lane specific operations, the C-TPAT member name, and the specific supply-chain route for which the SOP applies.
3. The Supply Chain SOP **Shall** indicate the specific differences from the Security Device System SOP.
4. SOPs **Shall** identify and show compliance with all applicable licenses, permits and contract agreements required to deploy, install, and operate the Security Device System throughout the applicable supply chain route.
5. The SOPs **Shall** include the operating and validation procedures to be used when arming a Security Device.
6. The SOPs **Shall** specify how all required information is entered into the Security Device during the arming process.
7. Any activation, deactivation, or operational procedures that are trade-lane specific **Shall** include documentation of testing that verifies the proposed changes will have no impact to any DHS requirement identified in this document.
8. The SOPs **Shall** provide the operational procedures that establish and verify that the communications pathways and interface capabilities necessary for the communication functions are operational.
9. The SOPs **Shall** include contingencies for non-nominal operating scenarios.

10. The SOPs **Shall** provide installation, maintenance, servicing, technical, and operational process and procedures, as well as logistic support for a Security Device System and all of its supporting components.
11. The SOPs **Shall** provide the procedures and processes that ensure the integrity and security of all data collected during, and at completion of, a trip remains secure.
12. The SOPs **Shall** provide the procedures and processes that clearly state how all data needed to meet the requirements in this document will be reinitialized for use if a Security Device is improperly armed, or found to be already improperly armed, at the shippers stuffing or deconsolidation location.
13. The SOPs **Shall** provide specific training requirements for installing, arming, deactivation, and removal of a Security Device System.
14. The vendor **Shall** provide, prior to initiating a specific supply chain route, a Trade-Lane Pre-Deployment Test to validate the functional performance of their Security Device System through all node-points of the specific trade-lane. If required, this demonstration must occur prior to commencing authorized Security Device-equipped cargo movement operations.
15. Prior to the Trade-Lane Pre-Deployment Test for each trade-lane, DHS **Shall** be notified. At DHS's option, DHS personnel may conduct on-site verification exams of Trade-Lane Pre-Deployment Testing to ensure compliance with the test plan and the supply chain SOP.
16. The Trade-Lane Pre-Deployment Tests **Shall Not** use any DHS message routing information. Only after successfully completing any Trade-Lane Pre-Deployment Testing and the trade-lane specific SOP has been approved will DHS provide the Supply Chain Certificate and the IP addresses for security related data message to be transmitted to CBP.

17.2 Vendor Application and DHS Approval Process

The approval and application process for a Security Device System and/or Component(s) requires the applying-vendor to verify and document compliance with this document for the candidate Security Device System and/or Components prior to submitting an application for approval to DHS.

The process to approve a Security Device System Component for operational use consists of two steps:

- DHS approval for the Security Device System Component(s) to be included on an Approved Security Device Vendors List, once the agency has validated the components, operability, and interfaces.
- Trade-lane specific review that confirms that the operational process, procedures, and interfaces can be satisfactorily implemented by a particular importer in the specific trade-lane. Successful completion of these reviews may result in a Supply Chain Certificate.

17.2.1 Application and Approval Process Overview

The application and approval process is summarized in Figure 17-1. The key process interactions between Security Device System vendors and DHS are:

1. The DHS releases the Security Device Requirements Document and the Device-to-Network Access Device Interface Control Document [4] to a vendor.
2. The vendor designs, develops, and conducts System Verification and Testing. The vendor submits the calculation and analysis of the system's Probability of Detection (P_d), Probability of False Alarm (P_{fa}), and Probability of Critical Failure (P_{cf}). Supporting documentation, including laboratory and field test results and analysis, should be included with all other documentation submitted in accordance with Section 17.3 of this document.
3. Vendor submits application to DHS for review and approval in accordance with Section 17.3 of this document. Sample devices of the Security Device System or Components are submitted to DHS with the application.
4. The DHS reviews the application and notifies the vendor of application status. The DHS will request additional information, as may be required.
5. The DHS reviews the vendor application data for satisfactory demonstration of compliance with technical requirements. DHS may request additional information or verification testing.
6. The DHS procures and/or accepts sufficient component hardware for testing, then conducts a Vulnerability Assessment and Compliance Verification testing.
7. The DHS conducts an Operational Field Test.
8. Upon DHS request, the applicant vendor may be required to assist DHS Operational Field Testing with any required logistics, technical expertise, information, or support.
9. The DHS performs an assessment based on the vendor's compliance data and DHS test results.
10. The DHS approves or disapproves the vendor's Security Device System or Components and notifies the vendor. Approved Security Device Systems or Components are placed on the "DHS Approved Security Device Vendors List".
11. The vendor/importer applies to DHS/CBP for Security Device System or Component use in specific trade-lanes.
12. The DHS reviews application and, upon DHS's direction, the vendor/importer **Shall** perform a Trade-Lane Pre-Deployment Tests associated with each SOP. DHS will review the trade-lane specific SOP for C-TPAT compliance and vendor/shipper implementations per the DHS-Approved Security Device Vendor Certificate. The approved vendor/importer receives a "Security Device Supply Chain Certification" for specific trade-lane.
13. The vendor/importer may commence secure cargo operations with the specific SOP approved for the specific trade-lane upon receipt of a "Security Device Supply Chain Certification"

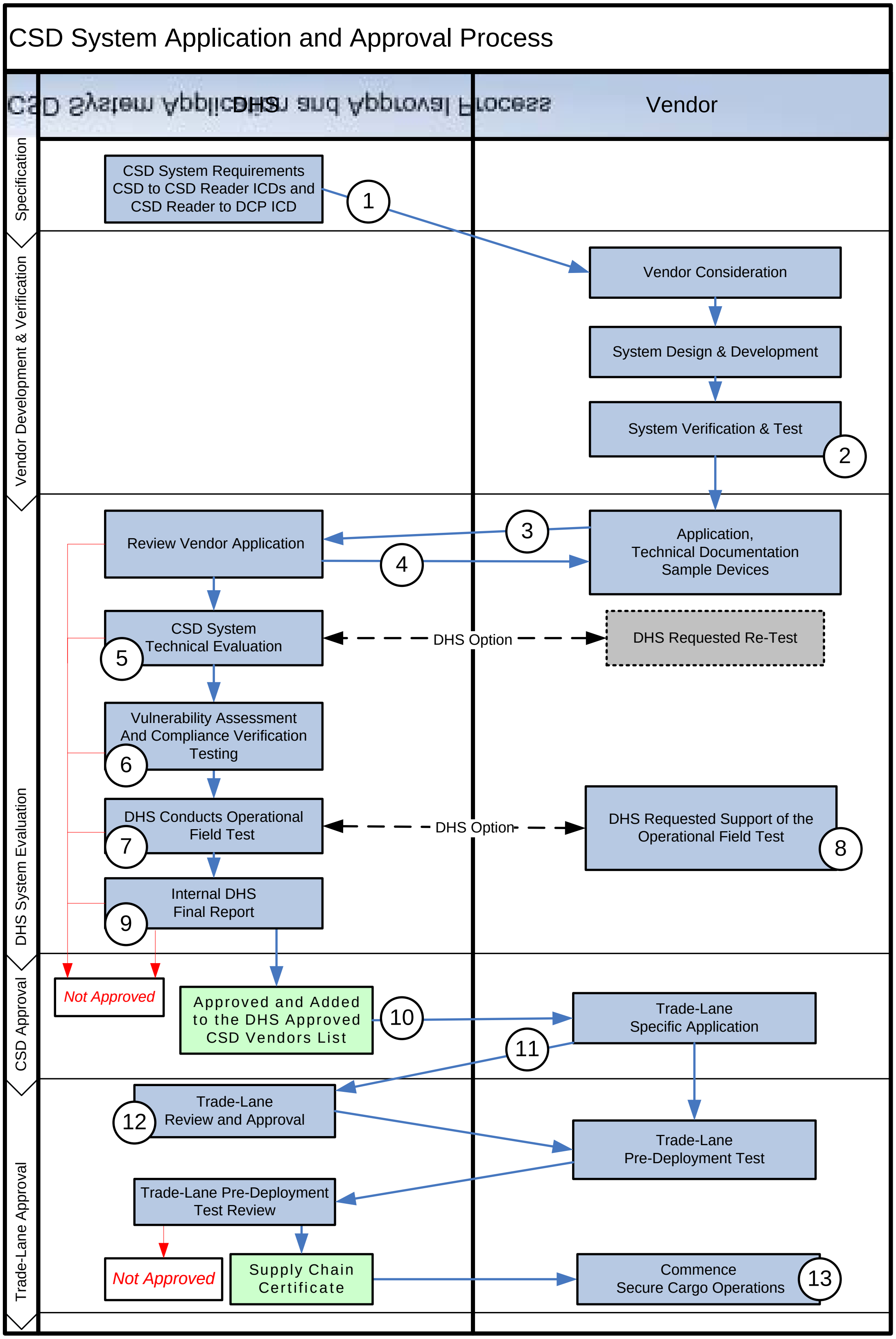


Figure 17-1: Security Device System Application & Approval Process

17.2.2 Approved Security Device Vendors List and Approved Security Device Supply Chain Certification

An applicant vendor may be issued a DHS Approved Security Device Vendor Certificate only after the sponsoring agency certifies that their entire system satisfies all Security Device requirements listed in this document.

Prior to receiving authorization to commence secure cargo operations using the vendor's Security Device System, the vendor and importer:

1. **Shall** provide proof of C-TPAT status of importer and the specific supply chain route for which a Security Device System is to be used.
2. **Shall** provide documented proof of all licenses and permits and contract agreements to deploy, install, and operate a Security Device System throughout the applicable supply chain route.
3. **Shall** provide current version of SOPs to be implemented by Security Device System users in the specific trade lanes, per the Section 17.1
4. Approved vendors **Shall** submit an updated SOP for each C-TPAT member, and supply chain routes for which an approved Security Device System is applied, prior to actual commencement of supply chain Security Device operations.

The DHS has the option to require a Trade-Lane Pre-Deployment Test by the vendor and importer as specified in Section 16.

Only after DHS receives, reviews, and approves trade-lane specific SOPs and any required Trade-Lane Pre-Deployment Test data will a vendor be issued a Security Device Supply Chain Certification. The Security Device Supply Chain Certification authorizes the shipper to commence cargo movements with Security Device-enabled Containers. Security Device-enabled cargo-movement operations are restricted to those trade-lanes as described in the Supply Chain Certification as identified in the vendor's trade-lane specific SOP.

To avoid costly duplication of fixed reader infrastructure at stuffing/consolidation facilities and foreign/US marine terminals, vendors/shippers are required to share infrastructure to the extent possible. Therefore:

5. All vendors/shippers with authorized Supply Chain Certificates **Shall** allow, where applicable, any other Approved Security Device Vendor with a Supply Chain Certificate access and use of infrastructure at all required read points.

A Security Device System Status website will list and identify all of the approved Security Device System vendors and the approved Security Device System components. This website will also contain the list of approved and active Supply Chain Certificates. DHS reserves the right to remove an approved Security Device System or Component from the list if an unacceptable degradation in Security Device System, or Component(s), performance is observed when used in a trade-lane. The Security Device System Status website will be publicly accessible.

17.3 Submittals and Administrative Information

Application package submittals must be in compliance with all sections of this document. In addition, only one submittal per Security Device System hardware configuration and firmware version number will be accepted. All documents are to be provided on company letterhead and limited to a total package size of no more than one hundred pages. All documentation submittals are to be in English in MS Word in 12-point Times New Roman. All data received marked or designated as business confidential or proprietary will be fully protected and maintained within the DHS evaluation team. All packages submitted electronically or by electronic media must be free of any computer virus. If a virus is found, the package will be destroyed. Submittals are to be entered at a DHS website. Within three business days of submittals being posted, applicants will receive an email confirming that DHS has received and successfully opened the package, and that the reviewing process has commenced.

Questions regarding submissions can be sent by email to the designated point-of-contact.

A complete vendor submission package **Shall** include:

(1) A **cover page** that includes the company name and address, with business and technical contact information, including e-mail, fax, telephone, and web page (if applicable).

(2) Identification of **any existing or former (past 5 years) federal government contracts** released in conjunction with the Security Device and/or components to be considered, including agency, agency point of contact, and contract / purchase order number.

(3) Identification (if applicable) of any company or companies whose components, software/firmware or support make up a Security Device system. All contractual agreements which state that the submitter is the authorized representative with regards to this submittal **Shall** be in place and signed prior to an application submittal.

(4) A **detailed system description,** which provides a well-developed description of the entire vendor solution. This description should include:

   a. What the system is and how it works (what technologies are used).

   b. A description of how the system meets all requirements set forth by DHS (Security Device Requirements Document).

   c. A complete system overview that includes and itemizes all components, their interactions, part numbers with revision number, and firmware and/or software with revision numbers.

   d. An operational and logical data flow for the system. The operational data flow should describe, at a high level, how the data flows through the entire system. The logical data flow should be a more detailed description of the implementation of the operational data flow.

   e. A complete listing of all the functional capabilities.

   f. Reference to applicable specifications for all functional capabilities.

   g. Level and definition of the adversary that was assumed in designing this version of the system.

   h. An SOP plan that meets the requirements in Section 17.1 of this document.

(5) The following documentation:

   a. A **Testing Report** that documents:

      i. A description of all laboratory and field tests/usage to date.

      ii. Customer references.

      iii. Number of devices involved in tests.

iv. Issues found in previous tests to include failure rates and modes.
v. Duration of tests/usage experiences.
vi. Date of actual testing verifying that testing data was obtained not more than 12 months prior to the submittal.

b. Acceptable test and analysis submittals **Shall** comply with the following requirements. Analysis documentation will only be accepted where testing is not explicitly required.
i. Documentation **Shall** contain a description of actual test or analysis conducted.
ii. Documentation **Shall** be in accordance with International and U.S. recognized institutions and standards.
iii. Testing and analysis documents **Shall** be submitted, stamped and certified by DHS accepted independent standards institutions/bodies or a third party Professional Engineer.
iv. Detailed testing and analysis reports are not required at time of submission, however they are required during the package review process.
v. Depending on the level of detail and accuracy of submitted documentation, DHS Cargo Security Test and Evaluation (CSTE) team may require verification testing at submitter’s cost.
vi. Testing and analysis performed at submitter facilities is permissible, however the results are subject to verification by DHS CSTE team.

c. A **System User’s Manual** that documents:
i. How to install the system.
ii. How to use and operate the system, including detailed standard operating procedures.
iii. How to maintain the system.

(6) **Items required to support laboratory and field testing of the Security Device systems.** The contents and quantities of these lists are subject to change, but will nominally include:

a. Vulnerability Assessment and Compliance Verification Testing
i. 20 Security Devices of the Hardware Version Number and Firmware Version Number being reviewed
ii. Two of each type of Reader offered by vendor
iii. Cabling, Software, Manuals, and all other components necessary to operate the Security Device System in a laboratory setting

b. Operational Field Test
i. Pricing and availability for the proposed equipment configuration (Security Devices, and Readers) necessary to support a large scale Operational Field Test
ii. Complete listing and copies of all documentation and training materials covering installation, training, and use of Security Devices in an operational setting
iii. Specifications for any computers and infrastructure requirements necessary to support testing

iv. Cabling, Software, and all other components necessary to operate Security Device System in an operational setting

(7) **An itemized list of costs** for:

a. The Security Device and associated system components.

b. Items required for testing.

c. Documentation.

d. Required third party services.

(8) **Deployment Capabilities**

The documentation of the deployment strategy **Should** account for the global nature of the shipping and freight handling community, including any reliance on technologies that may be restricted by US or foreign regulation.

(9) **Technical capability**

a. The vendor **Shall** document their technical capability to support all aspects of product deployment, validation, manufacturing, distribution, operations support, and maintenance. This **Shall** include the ability to document and modify the Security Device and support equipment.

b. The vendor **Shall** document their capability to provide technical support worldwide, including, as applicable, but not limited to, implementation and access to any necessary global information network, data storage, and information distribution capabilities.

17.3.1 Submittal Requirements for Auxiliary Sensors

The system in its entirety (inclusive of any auxiliaries) will be evaluated, and if it passes all tests, it will be considered approved as a whole system. Removal or deactivation of auxiliary sensors after a Security Device has been approved will not be permitted unless the initial evaluation included that option, and the Security Device was tested in those configurations and received acceptance.

Note: DHS will not be responsible for evaluating or certifying the performance or functionality of any auxiliary sensors; this is the sole responsibility of the vendor.

1. All data from any non-security auxiliary sensors will be considered to be “commercial data”.
2. Vendors **Shall** submit, in the initial application, all such auxiliary sensors or add-ons, including the specifications for their operational and performance characteristics, and any impact, positive or negative, that they have on Security Device Requirements.
3. Vendors **Shall** submit documentation, including test records, demonstrating that any auxiliary sensors do not negatively affect the ability of the Security Device System to meet DHS Security Device Requirements.

18 Appendix G - Measurement Assurance Plan (Worksheet)

Project: Security Device Operational Test and Evaluation (OT&E)

Q1 – What measurements are important?

Q2 – How good do the measurements have to be?

Q3 – How do you know they are good enough?

Measurement	Quantity measured	Required tolerance	Equipment used	Equipment accuracy	Test Accuracy Ratio >=	Calibrate Y/N?
P1A – Size (length, width, height)	Inches	+/- 1/8 inch	Standard metal ruler	+/- 1/32 inch	4	No
Weight	Pounds	+/- 0.1 pound	Scale	+/- 0.01 pound	10	No
P1B – Comms range	Feet	+/- 1 foot	Tape measure	+/- ¼ inch	48	No
Shock (container and device drop)	Feet	+/- 3 inches	Tape measure	+/- ¼ inch	12	No
Vibration magnitude	Meters/second^2	+/- 0.1 m/s^2	Accelerometer	+/- 0.001 m/s^2	100	Yes
Vibration frequency	Hz	+/- 10 Hz	Accelerometer and Data acquisition system	+/- 5 Hz	2	Yes
Shock (device drop)	"g"	+/- 0.01 g	Accelerometer	+/- 0.0001 g	100	Yes
Radiation	Rad (si)	+/- 1rad	Thermoluminescent Detector (TLD)	+/- 0.1 rad	10	Yes
Temperature	Degrees C	+/- 0.1^{o}C	Temperature Gauge	+/- 0.001 ^{o}C	10	Yes
Time	Hours	+/- 1 hr	Digital Clock Timer	+/-1 min	60	Yes
Humidity	Relative Humidity (RH)	+/- 1%	Relative Humidity Sensor	+/- 0.1%	10	Yes
Water pressure	Pounds/in^2 (psi)	+/- 2.5 psi	Pressure gauge	+/- 1 psi	2.5	No
Electrostatic Discharge	Voltage	+/- 100V	Digital voltmeter	+/- 10V	10	Yes
Electrostatic Discharge	Current	+/- 0.1 A	Digital current meter	+/- 0.01A	10	Yes
Nearby Lightning	Magnetic Field	+/- 1 A/m	Injection current sensor	+/- 0.1 A/m	10	Yes
Radiated Emissions	Field strength	+/- 1 dBuV/m	Antenna, amplifier, electronics	+/-0.01 dBuV/m	100	Yes
Radiated Susceptibility	Field strength	+/- 0.1 V/m	Antenna, amplifier, electronics, signal generator	+/- 0.01	10	Yes
Magnetic Susceptibility	Field strength	+/- 10mV	B dot probe	+/- 1 mV	10	Yes

EM Tests	Frequency	+/- 1 Hz	Digital Spectrum Analyzer	+/-0.01 Hz	100	Yes
EM Tests	Voltage	+/- 10mV	Digital Spectrum Analyzer	+/- 1mV	10	Yes
Comms speed	Seconds	+/- ½ second	Stop watch	+/- 1/10 second	5	No
Interference – frequency range	Hz	+/- 1 Hz	RF Spectrum Analyzer	+/- 0.01 Hz	100	Yes
Interference – frequency modulation	Hz	+/- 1 Hz	RF Spectrum Analyzer	+/- 0.01 Hz	100	Yes
Interference – signal strength	mW	+/- 1 mW	RF Spectrum Analyzer	+/- 0.01 mW	100	Yes
Comms frequency	Hz.	+/- 0.1 Hz	Frequency meter	+/- 0.001 Hz	100	Yes
Comms read distance	Feet	+/- 1 foot	Tape measure	+/- ¼ inch	48	No
Comms orientation	Degrees	+/- 5 degrees	Protractor	+/- 2.5 degrees	2	No
Security Device measurement range	Feet	+/- 1 foot	Tape measure	+/- ¼ inch	48	No
Data log clock accuracy (time drift)	Seconds	+/- 1 second	Stop watch	+/- 1/10 second	10	No
Alarm report delay time	Seconds	+/- 1 second	Stop watch	+/- 1/10 second	10	No
Data upload/ download time	Seconds	+/- 1 second	Stop watch	+/- 1/10 second	10	No
Power usage in hibernation (avg)	mW	+/- 1 mW	DVM	+/- 0.1 mW	10	Yes
Power usage in detection mode	mW	+/- 1 mW	DVM	+/- 0.1 mW	10	Yes
Power usage in communicating	mW	+/- 1 mW	DVM	+/- 0.1 mW	10	Yes
Door Opening distance	Inches	+/- ¼ inch	Metal ruler - Caliper -	+/- 1/32 inch +/- 1/100 inch	8 25	No Yes
Side Penetration hole size	Sq Inches	+/- 1 sq inch	Metal ruler - Caliper -	+/- 1/32 inch +/- 1/100 inch	8 25	No Yes

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.