MEDICAL DEVICES
SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

27 July 2010

Developed by DISA for DoD

UNCLASSIFIED

This page is intentionally left blank.

TABLE OF CONTENTS

SUMMARY OF CHANGES v

1. INTRODUCTION 1

1.1 Background 2
1.2 Authority 3
1.3 Scope 3
1.4 Writing Conventions 3
1.5 Vulnerability Severity Code Definitions 4
1.6 DISA IAVM 6
1.6.1 IAVM Categories 6
1.7 STIG Distribution 7
1.8 Document Revisions 7
1.9 Policy Guidance Amplification 7
1.9.1 Data Protection 7
1.9.2 DoD C&A 7

2. MEDICAL DEVICE OVERVIEW 9

2.1 Introduction 9
2.2 Medical Device Class 9
2.2.1 Class I 10
2.2.2 Class II 10
2.2.3 Class III 10

3. NETWORKED MEDICAL DEVICES 11

3.1 Introduction 12
3.2 Networked Medical Devices Life Cycle 12
3.2.1 Networked Medical Device Procurement 12
3.2.2 Inventory 12
3.2.3 Device Classification 13
3.2.4 Device Accreditation 13
3.2.5 Networked Medical Device Configuration Control 14
3.2.6 Networked Medical Device Vulnerability Management 14
3.2.7 Incident Response 17
3.2.8 Maintenance 17
3.2.9 Disposal 17

4. NETWORKED MEDICAL DEVICES IN MILITARY HEALTH TREATMENT FACILITIES 19

4.1 Networked Medical Device IAVM Types 20
4.2 Networked Medical Device VLAN Separation 21
4.2.1 Virtual Local Area Network (VLAN) 21
4.3 Networked Medical Device Security Zone 22
4.4 Screened Subnet 23
4.5 Networked Medical Device Architecture Security Settings 25
4.5.1 VLAN Security Settings 25

4.5.2 Access Control Lists (ACLs) 26
4.5.3 Networked Medical Device Intrusion Detection/Prevention System 27
4.5.4 Port Security for VLAN-Separated Medical Device Segments 27

5. NETWORKED MEDICAL DEVICE MANAGEMENT AND MAINTENANCE 29

5.1 Internally Supported Devices 29
5.1.1 Out-of-Band Management 29
5.1.2 In-Band Management 29
5.2 Externally Supported Devices 30
5.3 Authentication 31

6. NETWORKED MEDICAL DEVICE SECURITY 33

6.1 Device Configuration 33
6.1.1 Device Settings 33
6.1.2 Networked Medical Device Security Settings 34
6.2 Wireless 37

APPENDIX A. RELATED PUBLICATIONS 39

APPENDIX B. GLOSSARY OF TERMS 41

APPENDIX C. LIST OF ACRONYMS 45

APPENDIX D. MEDICAL DEVICE SPECIALITIES 49

LIST OF TABLES

Table 1-1. Vulnerability Severity Code Definitions 4
Table 4-1. Networked Medical Device IAVM Compliance Types 20

LIST OF FIGURES

Figure 4-1. MTF Networked Medical Device – VLAN Separation 22
Figure 4-2. MTF Networked Medical Device – Security Zone 23
Figure 4-3. MTF Networked Medical Device – Screened Subnet 25

SUMMARY OF CHANGES

This is a new document; therefore, there are no changes from previous releases.

This page is intentionally left blank.

1. INTRODUCTION

A core mission for the Defense Information Systems Agency (DISA) Field Security Operations (FSO) is to aide in securing Department of Defense (DoD) networks and information systems (IS). The processes and procedures outlined in this Security Technical Implementation Guide (STIG), when applied, will decrease the vulnerability of DoD sensitive information. Network security is clearly still one of the biggest concerns for our DoD customers (i.e., the warfighter).

The intent of this STIG is to include security considerations at the network level needed to provide an acceptable level of risk for information as it is transmitted throughout an enclave and, if required, throughout the DoD network.

The Medical Devices STIG has been developed to enhance the confidentiality, integrity, and availability of sensitive DoD Automated Information Systems (AISs). Network-enabled medical devices increase productivity among medical professionals; however, their implementation between sites, both military and civilian, have frequently been left to the individual enclave personnel to implement without an in-depth review of risks their use bring to the DoD network, local enclave, device, and to the Electronic Protected Health Information (ePHI), to include Protected Health Information (PHI) and Personally Identifiable Information (PII)

This STIG provides the information protection guidance necessary to implement secure IS and networks while ensuring that medical devices continue to provide healthcare without risking safety to the patient. Additionally, this STIG, in whole or in part, assists in meeting the standards and requirements for the electronic transmission of certain health information (such as, Public Law 104-191, August 21, 1996, Health Insurance Portability and Accountability Act (HIPAA) of 1996).

DoD IS must have adequate safeguards, both technical and procedural, to ensure the security of data processed. In general, DoD IS must provide maximum feasible safeguards to achieve the highest level of security possible. The actual safeguards used will commensurate with operational requirements, information sensitivity level, and consequences of exploitation of the specific DoD IS.

This document is aimed at identifying requirements, implementation efforts, and mitigating controls to aid in successfully implementing, securing, and protecting the perimeter and computing environment, medical devices, and sensitive information and achieving the objectives as identified in the DoD Directive (DoDD), “Information Assurance, 8500.1,” and the DoD Instruction (DoDI), “Information Assurance (IA) Implementation, 8500.2.”

The specific medical devices and associated systems indicated in this document are those that are regulated by the Food and Drug Administration (FDA) as well as other devices that are utilized for direct diagnostics or other treatment of patients that may not be regulated by the FDA.

1.1 Background

The FDA approval process is focused on maintaining patient safety. Approved medical devices may be located throughout the facility in varying quantities. The biomedical engineering department is focused on maintaining and repairing these devices with minimal concern over typical IA/IS issues and safeguards. Medical device manufacturers may state claims of secure devices; however, verification of these claims along with meeting our Certification and Accreditation (C&A) requirements is necessary.

IA security incidents which have occurred have revealed there are unresolved vulnerabilities within the network that put DoD Global Information Grid (GiG), Military Health Systems (MHS), and individual military service networks at risk of recurring compromises. The individual military service network IA staff located throughout the DoD community defends service-controlled assets by diligently complying with Information Assurance Vulnerability Management (IAVM) patches and fixes.

Many of the devices located at MHS commands are not IAVM compliant. These devices include, but are not limited to, environmental/facility management and monitoring systems (e.g., heating, air conditioning, humidity control, lighting, alarms, etc.), wireless, and clinical FDA-approved medical devices, as well as systems developed and supported by the MHS, other military services, or outside entities. Such devices are configured with MHS-managed public Internet Protocol (IP) addresses.

Applying IAVM patches to these devices can be problematic. In the case of FDA-approved medical devices, these devices are required to go through a validation process mandated by the FDA, insurance providers, and the manufacturer; consequently, when one of these devices has to be modified (i.e., applying a software patch), the device has to be tested by the manufacturer to ensure that its clinical functionality is unaffected. Because of this additional validation process, it is difficult to achieve IAVM compliance within the time frames specified by the DoD. In addition, several medical device vendors have indicated that some devices will never be IAVM compliant, because the vendor cannot afford to perform the required product development on these products (older models, etc.). The problem is that policy states that if the device is not IAVM compliant, it cannot remain connected to the GiG without an IAVM extension and plan of action and milestones (POA&M). For purpose of this document, the term “medical systems and their associated medical devices” refers to all IP addressable medical devices.

This document describes medical devices and presents a mitigation strategy to allow continued network connectivity of medical systems and their associated medical devices that may not be fully IAVM compliant. The Defense in Depth (DiD) methodology will provide an overarching security design solution for the enterprise that will address all IP addressable medical systems and their associated medical devices. Nothing in this document lessens requirements of the IAVM program to submit POA&M and Mitigation documentation for those medical devices unable to comply with patching requirements.

1.2 Authority

DoDD 8500.1 requires that "all IA and IA-enabled Information Technology (IT) products incorporated into DoD IS shall be configured in accordance with DoD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, National Security Agency (NSA)." This document is provided under the authority of DoDD 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category (MAC) II Sensitive level and MAC III Sensitive level containing sensitive information.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The Information Assurance Officer (IAO) will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

The United States Cyber Command (USCYBERCOM) has also established requirements (i.e., timelines) for training, verification, installation, and progress reporting. These guidelines can be found on their web site: https://www.cybercom.mil. Initially, these directives are discussed and released as Warning Orders (WARNORDs) and feedback to the USCYBERCOM is encouraged. The USCYBERCOM may then upgrade these orders to directives; they are then called Communication Tasking Orders (CTOs). It is each organization's responsibility to take action by complying with the CTOs and reporting compliance via their respective Computer Network Defense Service Provider (CNDSP).

1.3 Scope

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks which utilize medical devices. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), IAOs, Network Security Officers (NSOs), and System Administrators (SAs) with configuring and maintaining security controls.

The scope of this STIG will encompass all DoD medical facilities worldwide. The specific focus will be medical devices used for patient diagnostics or treatment which reside at the Military Treatment Facility (MTF) on the medical site's network and communicates via the Transmission Control Protocol/Internet Protocol (TCP/IP). It will not include "typical" entities/network infrastructure (such as, workstations, servers, routers, switches, etc.) making up the network and managed by the facilities IT department.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should.**" The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "will" indicates mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic

paragraph. This makes all “will” statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written.

Each policy bullet includes the STIG Identifier (STIGID) in parentheses that precedes the policy text and references the corresponding vulnerability check in the Security Readiness Review (SRR) Checklist and Vulnerability Management System (VMS). An example of this will be as follows: "(MED0111: CAT II)." If the item presently does not have a STIGID, or the STIGID is being developed, it will be not applicable (N/A) and will contain a preliminary severity code and "N/A" (i.e., "[N/A: CAT III]"). Throughout the document, accountability is directed to the IAO to “ensure” a task is carried out or monitored. These tasks may be carried out by the IAO or be delegated to someone else as a responsibility or duty.

A reference to “**should**” indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. All reasonable attempts to meet this criterion will be made.

1.5 Vulnerability Severity Code Definitions

Severity Category Code (CAT) is a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a severity code of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability. Table 1-1 provides the vulnerability severity code definitions.

Table 1-1. Vulnerability Severity Code Definitions

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability or Integrity. An ATO will not be granted while CAT I weaknesses are present. **Note**: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	Includes BUT NOT LIMITED to the following examples of direct and immediate loss: 1. May result in loss of life, loss of facilities, or equipment, which would result in mission failure. 2. Allows unauthorized access to security or administrator level resources or privileges. 3. Allows unauthorized disclosure of, or access to, classified data or materials. 4. Allows unauthorized access to classified facilities. 5. Allows denial of service or denial of access, which will result in mission failure. 6. Prevents auditing or monitoring of cyber or physical environments. 7. Operation of a system/capability which

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
		has not been approved by the appropriate Designated Accrediting Authority (DAA). 8. Unsupported software where there is no documented acceptance of DAA risk.
CAT II	Any vulnerability, the exploitation of which, has a potential to result in loss of Confidentiality, Availability or Integrity. CAT II findings that have been satisfactorily mitigated will not prevent an ATO from being granted. **Note**: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	Includes BUT NOT LIMITED to the following examples that have a potential to result in loss: 1. Allows access to information that could lead to a CAT I vulnerability. 2. Could result in personal injury, damage to facilities, or equipment which would degrade the mission. 3. Allows unauthorized access to user or application level system resources. 4. Could result in the loss or compromise of sensitive information. 5. Allows unauthorized access to Government or Contractor owned or leased facilities. 6. May result in the disruption of system or network resources that degrades the ability to perform the mission. 7. Prevents a timely recovery from an attack or system outage. 8. Provides unauthorized disclosure of or access to unclassified sensitive, personally identifiable information (PII), or other data or materials.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability or Integrity. Assigned findings that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted. **Note**: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the	Includes BUT NOT LIMITED to the following examples that provide information which could potentially result in degradation of system information assurance measures or loss of data: 1. Allows access to information that could lead to a CAT II vulnerability. 2. Has the potential to affect the accuracy or reliability of data pertaining to personnel, resources, operations, or other sensitive information. 3. Allows the running of any applications, services or protocols that do not support mission functions.

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
	device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	4. Degrades a defense in depth systems security architecture. 5. Degrades the timely recovery from an attack or system outage. 6. Indicates inadequate security administration. 7. System not documented in the sites C&A Package/System Security Plan (SSP). 8. Lack of document retention by the Information Assurance Manager (IAM) (i.e., completed user agreement forms).

1.6 DISA IAVM

The DoD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. (IAVM notifications can be accessed at the USCYBERCOM web site: https://www.cybercom.mil.)

VMS provides organizations with a tracking mechanism for IAVMs, CTOs, and other additional vulnerability compliance. VMS was developed to interface with DoD enterprise tools to assist all DoD Combatant Commands, Services, and Agencies (CC/S/A) in the identification of security vulnerabilities and in tracking the issues through the lifecycle of the vulnerabilities' existence.

All medical devices will conform to IAVM compliancy requirements or receive an approved exception via approved IAVM policy.

1.6.1 IAVM Categories

There are three (3) basic categories to define an IAVM status:

- **IAVM Compliant**: Medical systems and associated devices with all current IAVM patches applied or able to be updated either by MHS or medical device manufactures in a timely manner.

- **Non-IAVM Compliant**: Medical systems and associated devices which do not have current IAVM patches applied.

- **Unknown IAVM Compliance**: Medical systems and associated devices residing on the local area network (LAN) for which the LAN administrator does not have administrative privileges or other ability to verify IAVM compliance.

- (MED0001: CAT II) Medical devices will conform to IAVM compliancy requirements.

1.7 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The Non-Classified Internet Protocol Router Network (NIPRNet) Uniform Resource Locator (URL) for the IASE website is http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

1.9 Policy Guidance Amplification

There are numerous DoD and Federal documents and instructions that require adherence and compliance for implementation and security requirements. While a partial listing is included in Appendix A, this STIG does not intend to supersede or limit those requirements. The following requirements are not all inclusive but are those that are deemed to have significant importance.

1.9.1 Data Protection

In all cases, medical data is assumed to be non-public releasable PHI, covered by the HIPAA, For Official Use Only (FOUO), Sensitive, etc., and will always be protected to a minimum of DoDI 8500.2 standards. Ports, Protocols, and Services (PPS) usage for any medical devices attached to the network will be compliant with DoDI 8551.1.

- *(MED0002: CAT II) The IAO/NSO will ensure that the PPS' used by any medical devices connected to the MTF network are compliant with DODI 8551.1.*

1.9.2 DoD C&A

C&A is required by each service in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP). Some medical devices will require a complete C&A package while others will only require a platform IT certification (PIT). Each device will be reviewed on a case-by-case basis in accordance with (IAW) service-specific guidance for PIT determination by service and approved by the DAA.

This page is intentionally left blank.

2. MEDICAL DEVICE OVERVIEW

2.1 Introduction

Medical devices are used in all MHS facilities. These devices are used extensively in the treatment of patients to include diagnostic, therapeutic, and monitoring purposes. Delivery of patient care is, in many cases, facilitated by connecting these devices to the facilities network. The benefits of this connectivity are not without inherent risks. These risks include those imposed on the network, the devices, and, ultimately, to patient safety and confidentiality.

The purpose of this section is to define the types and classes of medical devices, as defined by the FDA, as well as to provide a basic overview of networked medical devices.

The Center for Devices and Radiological Health (CDRH) and, in specific cases, the Center for Biologics Evaluation and Research (CBER) of the FDA is responsible for regulating medical devices in the United States. The CDRH performs this function under the authority of the Federal Food Drug & Cosmetic Act (FD&C Act). The specific regulations covering medical devices is published by the FDA; these regulations are found in Title 21 Code of Federal Regulations (CFR), Parts 800-1299. The primary purpose of these regulations is to define guidelines covering the design, clinical evaluation, manufacturing, packaging, labeling, and post market surveillance of medical devices.

2.2 Medical Device Class

The CDRH groups medical devices into one of three classes: Class I, Class II, and Class III. The three classes set out to define a device's degree for potential harm to the patient, along with consideration of the device's design complexity. The FDA also defines a set of controls required to be met by the varying classes. These controls are referred to as the "General Controls". These controls are defined in the Medical Device Amendments of 1976 to the FD&C Act of 1938. The General Controls, dealing with the following identified topics, apply to all three classes of medical devices; however, they are the only level of controls that apply to Class I devices.

The General Controls include the provisions of the FD&C Act pertaining to:

1. Adulteration;
2. Misbranding;
3. Device registration and listing;
4. Pre-market notification;
5. Banned devices;
6. Notification and repair, replacement, and refund;
7. Records and reports;
8. Restricted devices; and
9. Good Manufacturing Practices.

2.2.1 Class I

Class I devices are subject to the least regulatory control and present minimal potential for harm to the user or patient. They are not intended to be used in supporting or sustaining life, in preventing impairment of human life, and they may not present an unreasonable risk of illness or injury.

Examples of Class I devices include freezers (to report temperature changes), clinical calculators, and others as identified in the Medical Device Amendments of 1976 to the FD&C Act of 1938.

2.2.2 Class II

The second class defined by the CDRH is Class II devices. These devices, if not properly managed, administered, or operated, have a greater potential to inflict harm to a patient than Class I devices. In addition, Class II devices are those for which general controls alone are insufficient to assure safety and effectiveness, and existing methods are available to provide such assurances. Class II devices are also subject to special controls, in addition to the general controls required of all devices. Special controls may include special labeling requirements, mandatory performance standards, and post-market surveillance.

Examples of Class II devices include infusion pumps, Orthopedic Computer Controlled Surgical Systems, and other devices as defined in the Medical Device Amendments of 1976 to the FD&C Act of 1938. It is likely that a significant number of Class II devices reside on the MTF network.

2.2.3 Class III

Class III is the most stringent regulatory class for medical devices. Class III devices are those for which insufficient information exists to assure the safety and effectiveness solely through general or special controls. Class III devices are usually those devices that support or sustain human life, are of substantial importance in preventing impairment of human health, or which present a potential, unreasonable risk of illness or injury.

Special controls, as defined by the Medical Device Amendments of 1976 to the FD&C Act of 1938, may be required in Class III devices. These special controls are above and beyond the required General Controls and allow the FDA to conclude that the Class III device is safe and effective for its intended use.

Examples of Class III devices include medical computers and software for ophthalmic use, full field digital mammographic X-Ray system, medical image analyzer, and other devices as defined in the Medical Device Amendments of 1976 to the FD&C Act of 1938. Class III networked devices are located throughout the MTF and must be secured.

3. NETWORKED MEDICAL DEVICES

The primary mission for MHS facilities is to provide world-class medical care to service members, their families, and other beneficiaries. This world-class delivery of care is capable through use of networked medical devices and those providers that make use of them. As listed in the preceding section, there are numerous medical devices in use at any given time on an MTF network.

These devices range from Intravenous (IV) pumps on the inpatient ward to implantable devices in the human body. These devices require protection before being placed on a network with other devices, including other medical devices as well as workstations, servers, printers, and other peripherals.

This STIG sets out to provide the necessary steps to assist in protecting these devices from other resources on the network as well as to protect the network from any risk that may be present due to the devices being placed on the network.

It is essential that any information transmitted, stored, or processed by the networked devices be protected from unauthorized disclosure, unauthorized modification, and/or loss of integrity.

Network-enabled medical devices are not always able to be maintained or secured in the same manner as network-enabled end user devices, such as workstations, servers, printers, hand-held, and other wireless devices. This limitation is, in large part, due to the regulatory control of the devices and their critical patient care functions. While the network-enabled medical device itself may have information security limitations, DoD networks must still be secured and vulnerabilities and risks managed.

Wireless technology, which requires compliancy with the Wireless STIG, also introduces unique concerns related to medical device-network interaction. Examples include cardiac implantable devices (such as pacemakers and defibrillators). These devices are programmed and interrogated with the use of a stand-alone device known as a programmer. Wireless technology allows these functions in a clinical setting without the use of a programmer head or wand. Communication can be established within ranges of equal to or greater than 5 meters. Wireless synchronization then allows transfer of data to the MHS facility's network. The collected data consists of current device settings, changes made during the session, current and historical cardiac information (heart rate, rhythm history, and device therapies initiated; such as pacing or defibrillation), and information specific to the device and patient (such as, model number, implant date, etc.).

Benefits of these devices using wireless technology include less physical interference with the implanting physician during the surgical procedure, a time savings for clinical personnel, a decrease in direct patient exposure/physical interaction, and a decrease in errors that might occur during manual data entry. Concerns found with wireless technologies also manifest themselves that includes inadvertent or malicious changing of settings. Patients are at risk when a device fails to deliver needed therapy or therapy is delivered when not needed. The programmer (and the person doing the programming) now has access to the MHS network, thus, injecting IA-related security risks to the network, the device, and the patient.

Even though medical device manufacturers have been tasked with vulnerability management, they are not always able to perform the task in a manner that meets the guidelines prescribed by DoD. This STIG outlines steps to take to assist in mitigating the risk of allowing FDA-regulated medical devices and their associated systems not updated to the latest patch level on the network, while maintaining the confidentiality, integrity, and availability of MHS and DoD networks.

3.1 Introduction

For the purposes of this STIG, the assumption is that the network-enabled medical devices have been acquired IAW the procurement policies, as specified in the the following sections and in additional requirements defined in regulations covering the acquisition of medical devices. Furthermore, it is assumed that the devices acquired to be utilized on the MTF network are FDA-approved for use in the setting and manner in which they are intended.

3.2 Networked Medical Devices Life Cycle

System/device manufacturers shall be responsible for ensuring the IA process is built into the manufacturers' system development and improvement processes.

3.2.1 Networked Medical Device Procurement

Services may initiate a centralized management procurement process for procurement, whereas others will allow sites to purchase on their own.

Each service will provide detailed instruction to its sites on proper procedures for procuring medical devices.

3.2.2 Inventory

As with any IA activity, an assessment of what is being secured must first be completed prior to securing it. This is also the case with networked medical devices. Networked medical devices must be inventoried and accounted for in all MTFs.

This inventory will contain sufficient information to quickly identify the type, location, IP address, MAC level, confidentiality level, and other identifying information. This inventory will be used and shared between IA and clinical engineering staff to assist in maintaining a secure and stable MTF network. This inventory will be reviewed on a regular basis for additions, removal, or other modifications.

In addition to the device-specific identifying information, the network communication flows required for the operation and sustainment of the networked medical devices must be documented. This documentation is to include all network flows involving communication to and from any third-party vendor, communications to clinical IS, and communication to systems that support the operation of the devices.

- *(MED0010: CAT II) The IAO/NSO will maintain a current listing of all network enabled devices that includes IP Address, location, Operating System (OS), logical and physical location and Clinical Engineering POC.*

• *(MED0020: CAT II) The IAO will review all networked medical device connection requirements on a semi-annual basis to ensure the need remains current, as well as evaluate all undocumented network connections discovered during inspections.*

3.2.3 Device Classification

All networked medical devices must be classified utilizing a MAC classification; either MAC I, MAC II or MAC III together with a Confidentiality level of Classified, Sensitive, or Public. The MAC level of networked medical devices will vary based on the networked medical device type and function. Explanations of the MAC levels are defined in Table 1-1 and in Appendix B, and the confidentiality levels are explained in section 3.2.3.1.

3.2.3.1 Confidentiality Levels

The Confidentiality Levels of an IS are as follows:

- **Classified**: Systems processing classified information.
- **Sensitive**: Systems processing sensitive information, as defined in DoDD 8500.1, to include any unclassified information not cleared for public release.
- **Public**: Systems processing publicly releasable information, as defined in DoDD 8500.1 (i.e., information that has undergone a security review and has been cleared for public release).

Note: No PII (specifically, electronic protected health information processed transmitted or stored) is considered to be suitable for public release.

• *(MED0040: CAT III) The IAM will ensure all medical devices are assigned a MAC directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. (Department of Defense Instruction (DoDI) 8500.2)*

3.2.4 Device Accreditation

Accreditation is required for all DoD-owned or -controlled IS that receives, process, stores, displays, or transmits DoD information, regardless of MAC levels, classification or sensitivity levels, including but not limited to Platform IT Interconnections (such as, weapons systems, sensors, medical technologies, or utility distribution systems).

The term "Platform IT Interconnections" means a system with network access to Platform IT." Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real-time to the mission performance of special purpose systems. These systems include weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems (such as water and electric). Examples of Platform IT Interconnections that impose security

considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

Systems/devices are not exempt from this requirement and will undergo the DIACAP C&A process.

- *(MED0060: CAT II) The IAO will ensure that networked medical devices be accredited IAW DIACAP.*

- *(MED0070: CAT II) All external connections intended to be utilized for support of network enabled network devices must be listed in the site accreditation documentation.*

- *(MED0080: CAT III) The IAO will ensure the appropriate Accreditation documentation is updated to reflect the Medical Device VLAN, security zones and/or screened subnet architectures.*

3.2.5 Networked Medical Device Configuration Control

Effective configuration control policies and practices are an effective part of a strong IA program and are a key in maintaining medical device confidentiality, integrity, and availability. The purpose of this STIG is to ensure that there are effective configuration change controls for networked medical devices. The configuration change control practices requiring analysis are policies and practices concerning general information technology roles (i.e,. OS upgrades, configuration changes such as IP address reassignment, and software installs). Clinical engineering configuration changes are outside the scope of this STIG and shall be subject to the policies, guidelines, and regulations covering medical device changes, such as the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and FDA requirements.

- *(MED0090: CAT III) The IAO will ensure that configuration control policies are in use for networked medical devices.*

The FDA issues guidance to medical device manufacturers regarding software patches to devices using commercial-off-the-shelf software products. This guidance states that it is the responsibility of the device manufactures to be aware of vulnerabilities and to update the devices with patches as necessary; however, it may be necessary to inform the medical device manufacturers of vulnerabilities discovered during a scan.

3.2.6 Networked Medical Device Vulnerability Management

Networked medical devices are not to be excluded from the MHS facilities vulnerability management plan. It is essential that these devices be included in the program and assessed for vulnerabilities IAW DoDI 8500.2, just as all other networked devices are. Remediation may not be as straight forward as other networked resources within the MTF, but is equally important to identify the steps for remediation and work with those organizations responsible for remediation to ensure any vulnerability discovered or reported is mitigated.

3.2.6.1 Vulnerability Scans

All DoD IS, including networked medical devices, with an Authority to Operate (ATO) shall conduct reviews at least annually to validate the correct implementation of assigned IA Controls. A combination of independent vulnerability assessments and ongoing self assessments will be used to ensure the controls are properly maintained. The assessments will include both host-based reviews and scans or penetration tests IAW USCYBERCOM guidance.

Consequently, conducting periodic local enclave vulnerability scans, along with self-assessments, will enable sites to find and close vulnerabilities prior to exploitation. These scans need to be conducted on a monthly basis and when major network changes are implemented.

As DoD enterprise tools are evaluated and released to the community, it is the site's responsibility to deploy and configure the solution in accordance with the approved published configuration guidance.

- *(MED0100: CAT III) The IAO will ensure an annual information assurance review of all networked medical devices is conducted IAW DoDI 8510.1.*

- *(MED0110: CAT II) The IAO will properly register all networked medical devices in a vulnerability management tracking system.*

In addition to the operational and functional checks required by the JCAHO Standard EC.02.04.03, MTF IA workforce members will scan networked medical devices for vulnerabilities and weaknesses prior to being placed on the network. Vulnerabilities discovered will be reported to the vendor for remediation, and a POA&M must be submitted for remediation. For existing devices, scans must be carefully coordinated with the system owner to ensure patient care is not disrupted.

- *(MED0130: CAT II) The IAO will ensure that all networked medical devices are scanned for vulnerabilities prior to connecting to the production medical device network.*

- *(MED0140: CAT II) The IAO will ensure that all vulnerabilities discovered during scans are remediated to the extent possible by the Medical Device manufacture prior to connecting to network.*

3.2.6.1.1 Automated Scanning

USCYBERCOM CTO 08-005, Directive for Automated Scanning and Remediation of Network Vulnerabilities, requires that automated scanning and reporting be accomplished by qualified personnel who have been certified to DoDD 8570.1 Standards. The scanning is required as a part of the MTF's Vulnerability Assessment Program to sustain enclave integrity.

Because the creation of protected Virtual LANs (VLANs), security zones, and/or screened subnets are required to ensure that the networked medical systems/devices in question are protected from unauthorized access, the MTFs will be subjected to regular penetration, testing, and scanning. By testing in this fashion, the vulnerability of the systems/devices is determined

through the evaluation of the integrity of the enclave without subjecting the internal systems/devices to risks associated with vulnerability scanning.

The IAO will ensure scans are done IAW the minimal requirements to comply with current USCYBERCOM guidance.

- *(MED0150: CAT III) The IAO will ensure regular vulnerability scanning is conducted on medical device network segments.*

In the event an automated scan is not permissible or a known issue exists where patient care could be negatively affected, the IAO will document the automated scanning exception.

- *(MED0160: CAT III) The IAO will ensure automated scan exceptions are documented and reviewed regularly.*

3.2.6.1.2 Manual Assessments

It is not always possible or practical to conduct an automated vulnerability scan on networked medical devices. In these cases, the IAO must conduct the vulnerability assessment utilizing a manual methodology and ensure they are done at the same frequency as normal automated scans. This methodology requires a physical inspection, as well as a review of configuration files and interviews of the administrators and operators of the networked medical device.

- *(MED0170: CAT III) The IAO will ensure networked medical devices that cannot be scanned are manually assessed.*

3.2.6.2 Vulnerability Reporting

Vulnerabilities identified during IAVM scanning or other internal reviews must be reported to the vendor for corrective action as part of the command's VMS. Any vulnerability submitted to the vendor must be tracked.

- *(MED0180: CAT III) The IAO will ensure networked medical device vulnerabilities are reported IAW DOD 5200.1 (series).*

- *(MED0190: CAT III) The IAO will ensure networked medical device vulnerabilities are reported to the medical device manufacturer for remediation.*

3.2.6.3 Vulnerability Support

In addition to the reporting requirements identified under Vulnerability Reporting, it is imperative to ensure vendor vulnerability reports, websites, and newsletters are reviewed to determine if any of the devices are contained on the site's network.

- *(MED0200: CAT III) The IAM will ensure that vendor's vulnerability reports are monitored.*

This is to provide support to receive patches, vulnerability fixes, updates, etc.

3.2.7 Incident Response

Security and privacy incidents will be handled IAW the applicable incident response policy or regulation (e.g., DoD and service specific regulations, to include DoD 5400.11-R and 21 CFR Part 803).

Incident reporting involving networked medical devices is critical. Not reporting could negatively impact patient care and/or safety as well as patient privacy.

- *(MED0210: CAT II) The IAO will ensure that the facility incident response plan incorporates incidents involving networked medical devices.*

3.2.8 Maintenance

All medical device information assets will be protected and secured during preventative, routine, and corrective repair processes in accordance with service regulations. Care should be taken to ensure that medical device manufacturers are unable to access unauthorized sensitive information during on-site repair or update visits or in the event the device must be returned to the manufacturer for repair.

- *(MED0215: CAT II) The IAO will ensure that the local site media sanitation policy includes repair and maintenance of medical devices.*

3.2.9 Disposal

All networked medical devices will have all protected health information erased IAW DoD 5200-1R (series) prior to being disposed of. This is done to comply with Federal and DoD regulations and to protect patient confidentiality.

- *(MED0220: CAT II) The IAO will ensure that the local site media sanitation policy includes disposal of medical devices.*

This page is intentionally left blank.

4. NETWORKED MEDICAL DEVICES IN MILITARY HEALTH TREATMENT FACILITIES

MHS contains enclaves built upon a sound IA foundation of DiD utilizing:

- Demilitarized Zones (DMZs)
- VLAN separation
- IP Security (IPSec) Virtual Private Networks (VPNs)
- Security zones
- Packet filters
- Network-based and host-based intrusion protection systems (IPSs)
- Virus detection/prevention
- Server and workstation security
- Network management
- Outside Security Screening Router (OSSR)
- Firewalls
- Inside Security Screening Router (ISSR)
- Internal device security

Remote access to and maintenance of MHS systems and devices by approved personnel must be made through secure and reliable means. The proper configuration of these medical devices can assist in solving the problem of networked medical device security.

Many of the network-enabled medical devices located at MHS commands are not in compliance with IAVM or other security-related patches. Applying patches to these devices can be problematic. In the case of FDA-regulated networked medical devices, these devices are required to go through a validation process mandated by the FDA, insurance providers, and the manufacturer; consequently, when one of these devices has to be modified (i.e., applying a software patch), the device has to be tested by the manufacturer to ensure that its clinical functionality is unaffected.

Because of this additional validation process, it is difficult to achieve IAVM compliance within the time frames specified by the USCYBERCOM. In addition, several medical device vendors have indicated that some devices will never be IAVM compliant, because the vendor cannot afford to perform the required product development on these products (older models, etc.). If the vendor cannot or will not develop products to a compliant state, a POA&M should be created by the site to sunset the use of that product as soon as fiscally possible.

The DiD methodology provides for protection in network enclaves to continuously minimize community risk and ensure that the protection of one system is not undermined by the vulnerabilities of other interconnected systems. Placement of networked medical devices within the MHS enclaves is important in maintaining the DiD methodology and ultimately keeping MHS and DoD networks secure and protecting the networked medical devices.

The boundaries potentially crossed for medical devices are from the enclave at one end to the Internet on the other. DoDI 8551.1 defines and provides guidance for all boundaries controlled by DISA. (For those boundaries not owned and controlled by DISA, refer to service-specific policy for questions and permissions.)

DoDI 8551.1 and associated Vulnerability Assessments (available on the Defense Knowledge Online (DKO) website) are considered to be the guiding policy for any PPS issues.

No medical device data is considered publicly releasable; therefore, no non-secure PPS are authorized across any boundary (non-secure PPS' are those that do not encrypt the user name, password, and data such as Telnet and File Transfer Protocol (FTP)). Each of these must be encrypted to a minimum of Federal Information Processing Standards (FIPS) 140-2 requirements to cross any boundary..

Any use of PPS' not in accordance with the service-specific policy or the DoDI 8551.1 will NOT be allowed to cross the boundary until a prior exception has been received from the service for their individually owned and controlled boundaries and from the Defense Information System Network (DISN) Security Accreditation Working Group (DSAWG) (for all other boundaries).

4.1 Networked Medical Device IAVM Types

The networked medical devices are broken down into four categories within the MHS community based on their IAVM status, as shown in Table 4-1. These categories are a factor to assess in determining the proper placement within the MTF enclave.

Table 4-1. Networked Medical Device IAVM Compliance Types

IAVM Compliant	Medical systems and associated devices with all current IAVM and other security-related patches applied or able to be updated in a timely manner.
Non-IAVM Compliant	Medical systems and associated devices that do not have current IAVM patches applied.
Unknown IAVM Compliance	Medical systems and associated devices residing on the LAN for which the LAN administrator does not have administrative privileges (MHS systems usually fall into this category).
Other LAN Connected	Medical systems and associated devices with a scaled down OS that requires an IP address and connectivity to the LAN.

Note: For purpose of this document, the term "medical systems and their associated medical devices" refers to all IP addressable medical devices.

If a device is not IAVM compliant, it cannot remain connected to the GiG without an IAVM extension and a POA&M approved by the CNDSP.

In an effort to accomplish the objective of keeping the MTF network secure, the networked medical device secure, and the information transmitted, processed, or stored by the medical devices secure, this STIG provides three network architectures that define the proper network placement for medical devices on the MTF networks. The three (3) architecture options are: 1) VLAN separation; 2) Internal Security Zone, such as a Community of Interest (COI); and 3) Screened Subnet (i.e., DMZ). Implementing any or all of these options support the DiD methodology and will provide an enhanced security posture for medical systems and their associated devices that cannot be made IAVM compliant in a timely manner; thus, mitigating the risk to an acceptable level.

The first step towards implementing the DiD methodology is to determine which solution to place the medical devices and their associated systems. In order to determine placement, a thorough risk assessment will have to be conducted on each group of medical devices and their associated systems. Because there are many types of medical devices and systems performing multiple operations within MHS facilities (e.g., radiology, blood systems, wireless, voice over IP, environmental, etc.), there is a possibility that this solution would have to accommodate multiple medical devices, their associated systems, and their associated workflows.

Prior to creating the associated VLANs, Security Zones, or Screened Subnets, the following items such as the network, the number, type, location, serving communications closet, switch port, and function of each networked medical device and their associated systems that are to be connected to the enterprise data network must be fully documented.

- *(MED0240: CAT II) The IAO/NSO will ensure a risk assessment has been completed in an effort to ensure that the proper amount and VLAN types are created and used within the network.*

4.2 Networked Medical Device VLAN Separation

The first networked medical device architecture is to provide a layer of protection through the use of VLAN separation. This solution is applicable for medical devices and their associated systems that need to communicate inside the trusted enclave and/or need to communicate across DoD boundaries and service specific firewall policy compliant PPS to a .mil domain. An example of a VLAN separation solution is depicted in section 4.2.1. In addition to the communication restrictions, only those networked-medical devices in the IAVM compliant category may utilize the VLAN separation option.

- *(MED0245: CAT II) The IAO/NSO will ensure only IAVM compliant networked-medical devices are allowed on the VLAN.*

4.2.1 Virtual Local Area Network (VLAN)

A VLAN, in a switched network, is a logical collection of devices and their associated systems which are grouped together to form a common broadcast domain. Both port and IP-based VLANs ultimately appear as a subnet on the LAN. Information security is one of the common reasons VLANs are used to control network traffic.

Because a VLAN is considered by Layer 3 devices (i.e., routers) to be a separate network segment, traffic between VLANs must be controlled by a routing function in the network. This routing enables the network administrator to control the traffic into and out of selected VLANs in the enterprise switching architecture, as shown in Figure 4-1.

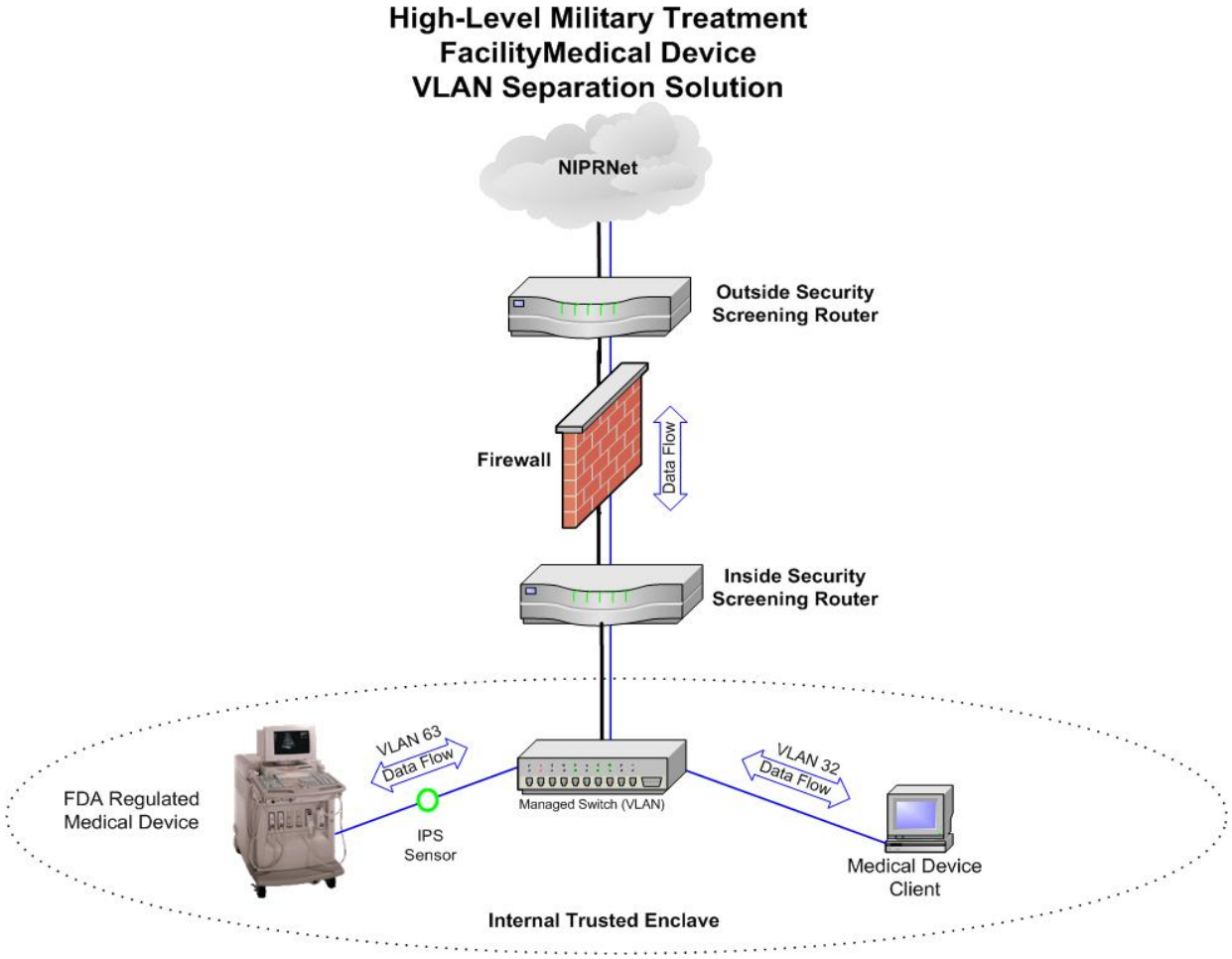

Figure 4-1. MTF Networked Medical Device – VLAN Separation

4.3 Networked Medical Device Security Zone

The second solution is to establish a Security Zone, which is also referred to as a COI. Like the VLAN separation solution, this solution is applicable for medical devices and their associated systems that need to communicate inside the trusted enclave and/or need to communicate across DoD boundaries and service specific firewall policy compliant PPS to a .mil domain. A notational example of a Security Zone solution is depicted in Figure 4-2. The networked medical devices in the Non-IAVM compliance, Unknown IAVM compliance, and other LAN-connected categories will be placed in the Security Zone architecture.

Security Zones add another layer of security by isolating the medical devices and their associated systems behind a firewall inside the internal trusted enclave, as shown in Figure 4-2. In addition, the firewall rule set is written using the “deny by default” IA best practices. The firewall rule set

is further enhanced by ensuring that inbound and outbound communications are to a specific source and destination IP address, using only the required PPS necessary for the operation of the medical devices and their associated systems. As these systems are FDA-regulated, and host-based Intrusion Detection/Protection System (IDPS) may not be a viable solution for the detection of any anomalies on the devices and systems located in the Security Zone, an IDPS sensor will be utilized IAW the IDS/IPS Network STIG, Version 8, policies to report any anomalies that may be detected.

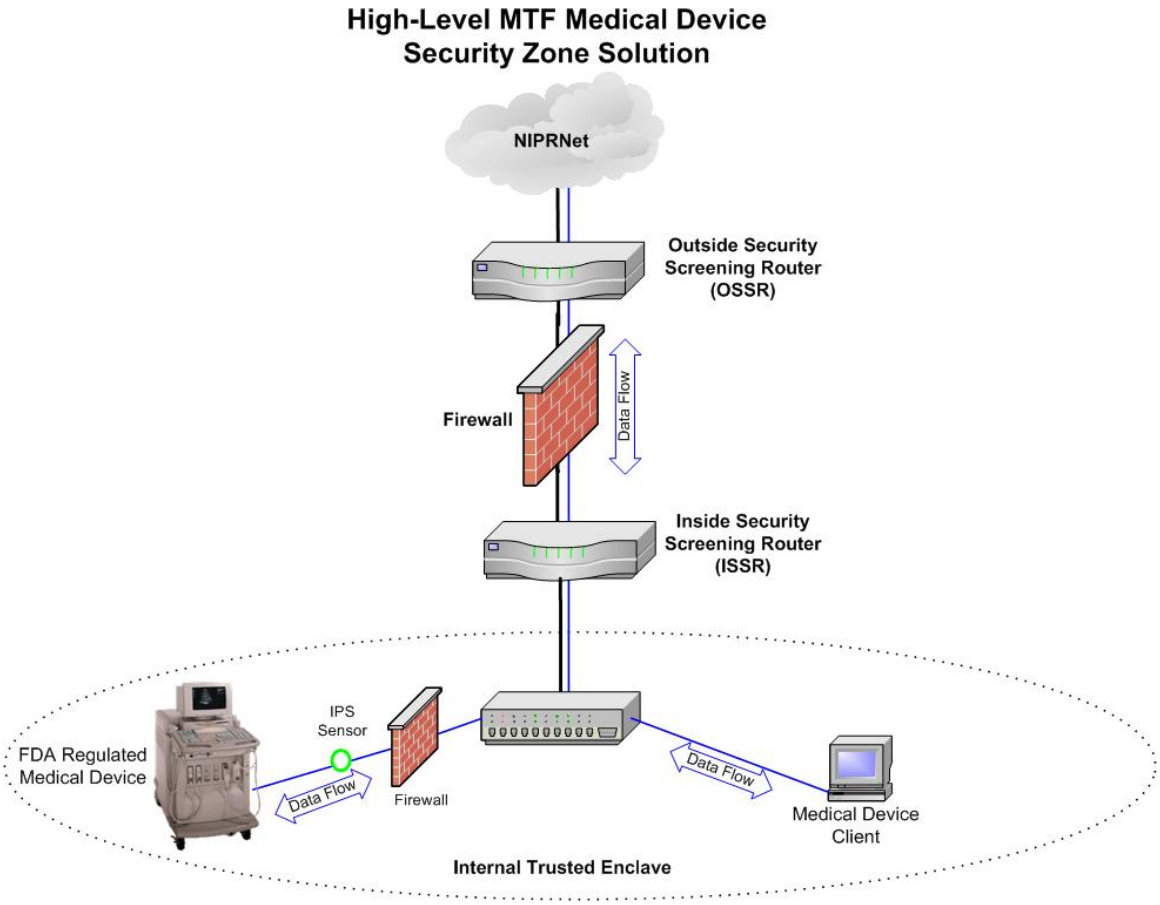

Figure 4-2. MTF Networked Medical Device – Security Zone

4.4 Screened Subnet

The first two solutions discussed addressed medical devices and their associated systems that are compliant with DoDI 8551.1 and service firewall policies, and communicate inside the trusted enclave, and/or outside the boundary to a .mil domain. However, there are medical devices and their associated systems that are not compliant with DoDI 8551.1 and service firewall policies that need to communicate across the boundary to either a .mil domain or a non-mil domain. The security issues with these devices can be mitigated by placing them in a Screened Subnet, which is sometimes referred to as a DMZ. However, there are distinct differences between a traditional DMZ architecture and the use of a Screened Subnet DMZ solution. The networked medical devices in the Non-IAVM compliance, Unknown IAVM compliance, and other LAN-connected

categories requiring communication not IAW the service-specific firewall policies will be placed in the Screened Subnet architecture.

A traditional DMZ architecture uses only the access control list (ACL) provided by the OSSR for access to systems in the DMZ and for access out of the traditional DMZ architecture to the NIPRNet. The OSSR ACL can be configured to use source and destination IP addresses, so that only IP addresses listed in the OSSR ACL have access to systems located in the traditional DMZ architecture. A Screened Subnet, on the other hand, uses the DiD methodology in that access to medical devices and their associated systems are controlled by the OSSR and ISSR ACLs and by the firewall rule set. In addition, logging can be enabled on the OSSR, ISSR, and firewall so that all access to the systems residing in the Screened Subnet is logged. This logged data can, then, be reviewed for auditing purposes. The OSSR and ISSR ACLs would still use source and destination IP addresses, as well as specific PPS. In addition, the firewall rule set would be configured to use source and destination IP addresses, as well as specific PPS. Access to the medical devices and associated systems located in the Screened Subnet is strictly controlled and logged for incident response/forensic activities, if needed. Refer to the Network Infrastructure STIG for more details on specific network requirements. An example of a Screened Subnet solution is depicted in Figure 4-3.

In addition, an IPS sensor should be placed inside the Screened Subnet to provide an additional layer of security and to alert the appropriate personnel in the case of an anomaly.

From a policy perspective, the connection between the NIPRNet and the Enclave DMZ/Screened Subnet would require compliance with the DoDI 8551.1 and the associated documentation for boundaries 9/10. Additionally, the connection between the Enclave DMZ/Screened Subnet and the Enclave would require compliancy with the service-specific perimeter protection plan for boundaries 11/12.

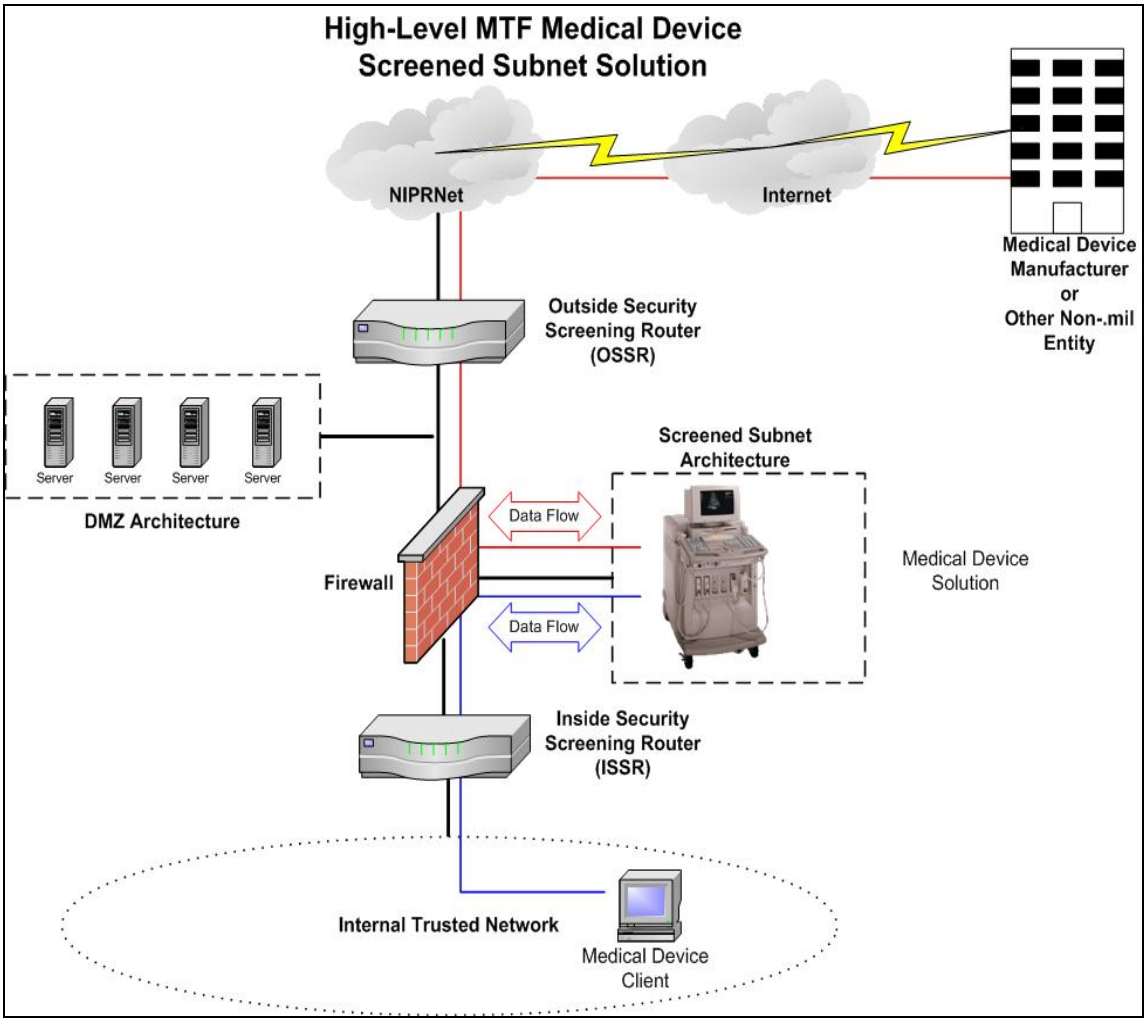

Figure 4-3. MTF Networked Medical Device – Screened Subnet

4.5 Networked Medical Device Architecture Security Settings

4.5.1 VLAN Security Settings

The VLAN security settings defined in this STIG are specific to networked medical devices. Many of these same settings are defined in the Network Infrastructure STIG. This STIG is not meant to replace the requirements on the Network, Enclave, or any other STIG that applies to MTF enclaves.

In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to transport Layer-2 control plane traffic. This traffic is all untagged traffic. This results in VLAN1 possibly spanning the entire network, if not appropriately pruned. If the scope of coverage for the VLAN is too large, the risk of compromise can increase significantly. The risk is even greater if VLAN1 is also used for user VLANs or the management VLANs. In addition, it is unwise to mix management traffic with user traffic, making the management VLAN an

easier target for exploitation. See the Network Infrastructure STIG for additional details/requirements.

• *(MED0250: CAT II) The IAO/NSO will ensure VLAN1 is not used for the medical device VLANs IAW the Network Infrastructure STIG.*

• *(MED0260: CAT II) The IAO/NSO will ensure trunking is disabled on all medical device VLAN access ports (do not configure trunk on, desirable, non-negotiate, or auto—only off) IAW the Network Infrastructure STIG.*

4.5.2 Access Control Lists (ACLs)

An ACL is a group of statements allowing or denying traffic on the network. Each statement defines a specific IP address relationship between systems and devices that have a need to communicate with each other to satisfy required communications between MHS commands and those who support them. As each data packet comes through the switch or router via an interface with an associated ACL, the switch scans the ACL from top to bottom for IP addresses that match the incoming packet. If the ACL has a rule matching the address, that rule determines the path for the data packet within the network. If the ACL has no rule matching the address, the data packet is discarded.

This capability provides for the configuration of a flexible access control capability for data packets that traverse MHS networks, represented by the following rules:

- ✓ Separate ACLs for each protected VLAN, Security Zone, and Screened Subnet.
- ✓ The ACLs will be developed with a philosophy of deny by default, permit by exception. This forces the ACL to be configured to permit only the communications necessary to support clinical and operational functionality.
- ✓ The ACLs, whether large in scope and/or complex in nature, should not reduce performance.
- ✓ Core Switch ACLs will allow communication with other devices located on the same VLAN or within the Security Zone. External clients (operating on the MHS data network) will not be allowed to access FDA-regulated medical devices within the protected VLAN or Security Zone without traversing an ACL, and being compliant with the DoDI 8551.1, associated policy documentation, and service-specific firewall policy.
- ✓ FDA-regulated medical devices that have communication requirements with external clients (not operating on MHS networks) will be placed in the Screened Subnet, and the ACLs and Firewall ruleset will be written with the deny by default, permit by exception DiD philosophy.

• *(MED0270: CAT II) Each medical device VLAN, security zone and screened subnet will have an Access Control List for both ingress and egress.*

- *(MED0280: CAT II) The IAO will ensure the Medical Device VLANs, security zones and screened subnets are protected via deny by default and permit by exception policy that only allows the necessary PPS for successful operation and maintenance of the networked medical devices.*

- *(MED0290: CAT II) The IAO will ensure that ACLs put in place to protect medical devices will not affect performance.*

- *(MED0300: CAT III) The IAO/NSO will ensure there is a review on a daily basis, of the Medical Device ACL log data by the Firewall Administrator (FA), or other qualified personnel, to determine if attacks or inappropriate activity has occurred.*

4.5.3 Networked Medical Device Intrusion Detection/Prevention System

All DoD locations will install, maintain, and operate a network IDPS inside of their network enclaves. The Enclave IDPS will monitor internal network traffic and provide near real-time alarms for network-based attacks. A Host Intrusion Detection (HIDS) application is not required on an OS-based Network Intrusion Detection System (NIDS).

The site may establish a support agreement with the CNDSP for monitoring. The local staff is responsible for initial response to real-time alarms.

If monitoring is being performed using a switch SPAN port, it is recommended that the IDPS is configured in Stealth Mode; the Network Interface Card (NIC) connected to the SPAN port would not have any network protocol stacks bound to it. A second NIC would then be connected to an Out-of-Band (OOB) network. Stealth Mode will eliminate the risk of the Intrusion Detection System (IDS) itself being attacked. Stealth Mode would not be applicable if the IDS is monitoring from a network tap solution.

- *(MED0310: CAT II) The IAO or Network IDS administrator will ensure a Network IDS is installed and operational in promiscuous mode for all medical device segments being monitored.*

- *(MED0320: CAT II) The IAO/NSO will ensure authorized reviewers of Network IDS data are identified in writing by the site's IAM and have completed HIPAA awareness training.*

- *(MED0330: CAT III) The Network IDS administrator will subscribe to the vendor's vulnerability mailing list.*

4.5.4 Port Security for VLAN-Separated Medical Device Segments

The port security feature provided by most switch vendors can be used to block input to the access port when the MAC address of the station attempting to access the port does not match any of the MAC addresses specified for that port—that is, those addresses statically configured or auto-configured (i.e., "learned"). The maximum number of MAC addresses that can be configured or learned (or combination of both) is also configurable.

In the event of a security violation, the Link Light Emitting Diode (LED) for that port turns orange. Configure the port to shut down permanently, shut down for a specified time interval, or

drop incoming packets from the unsecured host if a violation occurs. If either of the first two methods is used, a link-down trap is also sent to the Simple Network Management Protocol (SNMP) manager.

If port security is implemented, every switch at the access layer must have port security enabled on every access port that is in use—that is, a switch port configured as enabled and as an access port. Furthermore, the MAC addresses must be statically configured for each port.

5. NETWORKED MEDICAL DEVICE MANAGEMENT AND MAINTENANCE

This section defines the various means in which the networked medical devices are managed and maintained, by both internal and external sources. In- and out- of band management security is discussed and explained and settings to ensure secure management are defined.

- *(MED0380: CAT III) The IAO/NSO will ensure a record is maintained of all logons and transactions processed by the networked medical device or device used to manage the medical device.*

5.1 Internally Supported Devices

These settings are for devices that will allow for local administration and modifications by on-site administrators or clinicians.

Internally supported devices are those that are maintained by local staff only and require no communications across the DoD boundaries. Any local support that crosses only local service boundaries will require traffic to be compliant IAW the service-specific boundary policy. If it also crosses DoD boundaries, traffic is required to be compliant with DoDI 8551.1.

Internally supported devices that are maintained by vendor personnel who perform technical administration or maintenance activities in the MTF are considered to be providing internal support, provided they do not cross the DoD boundaries for any reason.

5.1.1 Out-of-Band Management

OOB Management is the preferred method for administering networked medical devices. By administering the devices utilizing an OOB method, the risk of exposure or disclosure to unauthorized parties of authentication, administration, and other sensitive data is less likely. OOB also provides a mechanism to administer a device when in-band management solutions, such as the production network, are unavailable. OOB management addresses this limitation by employing a management channel that is physically isolated from the data channel.

- *(MED0390: CAT I) The IAO/NSO will ensure all out-of-band management connections to the device require passwords.*

- *(MED0400: CAT II) The medical device administrator will ensure out-of-band management access to the device is secured using FIPS 140-2 compliant encryption modules.*

- *(MED0410: CAT II) The medical device administrator will ensure the timeout for out-of-band management access is set for no longer than 10 minutes.*

5.1.2 In-Band Management

In-band management refers to management of networked medical devices utilizing the same path as the data channel. This is often the only choice to administer networked medical devices. However, OOB management should be used when possible. The following guidelines focus on securing/limiting the connections for in-band administrative access.

- *(MED00420: CAT II) The IAO/NSO will ensure the device only allows in-band management sessions from authorized IP addresses from the internal network or DAA approved and documented external connections. The ACLs that allow this communication will be enforced on either the device or the firewall protecting the device segment.*

- *(MED00430: CAT II) The IAO/NSO will ensure that networked medical devices are not configured or able to initiate connections to external resources unless approved by the DAA and included in networked medical device inventory.*

- *(MED0440: CAT II) The medical device administrator will limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. The IAO/NSO will approve the use of in-band management on a case-by-case documented basis.*

- *(MED0450: CAT I) The IAO/NSO will ensure all in-band management connections to the device require passwords.*

- *(MED0460: CAT II) The medical device administrator will ensure in-band management access to the device is secured using FIPS 140-2 certified encryption methods.*

- *(MED0470: CAT II) The medical device administrator will ensure the timeout for in-band management access is set for no longer than 10 minutes.*

5.2 Externally Supported Devices

Externally supported devices are those that are maintained by staff external to the local enclave and require access across DoD boundaries. In cases where the support is external to the DoD network (e.g., the Internet), this would require transiting the DISA or service-approved Business to Business (B2B) gateway. Except in the most extreme cases, external support to and from the Internet is not to be used. External connections need to be recorded, maintained, and reviewed. Any support provided across DoD boundaries will be fully compliant with DoDI 8551.1, FIPS 140-2, and DoD Public Key Infrastructure (PKI) requirements, as well as any other DoD and service-specific policies that govern these connections.

- *(MED0480: CAT I) The IAO will ensure all privileged user access to a MHS networked medical device or system uses FIPS 140-2 compliant encryption to secure the data traversing the network.*

The access control functionality of DiD must be able to allow or disallow connections to support remote maintenance access to specific systems/devices on the MTF network. The MTF network perimeter must provide secure remote access to those medical systems/devices requiring approved remote maintenance. This access is instrumental in ensuring the maximum up-time possible for clinical operations and minimizing the high cost of maintaining medical systems/devices.

Medical systems/devices must be maintained in a secure fashion in order to prevent unauthorized system administration access. The MTF network must be configured to support the following secure administration:

- ✓ Alert event selection capability.
- ✓ Full session administration security and audit capability.
- ✓ Hardware and/or software features that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the product.
- ✓ Data protection with capability to prevent unauthorized disclosure, modification, and unauthorized input of data.
- ✓ Vendors must comply with DoD IA standards for computers that access the MTF on-site and from remote locations. This includes implementation of applicable security patches and all IAVM alerts.
- ✓ Additionally, anti-virus software with updated signatures must be active on the remote access workstation. Vendor's computers will be subject to random checks by the MTF to ensure compliance.
- ✓ Vendors must comply with the DoD PKI policy and obtain a Common Access Card (CAC), Alternate Tokens, or External Certificate Authority (ECA) certificate.
- ✓ Password policy with capability to enforce minimum length in accordance with the established site security policy and applicable DoD regulations.

- *(MED0500: CAT II) The IAO will ensure that Hardware and/or software features that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the product are available and used.*

- *(MED0510: CAT II)The IAO will ensure data protection (e.g. back-up, access control permissions, etc.) capabilities to prevent unauthorized disclosure; modification and unauthorized input of data are in place to when remote administration is used.*

- *(MED0520: CAT II)The IAO will ensure that vendors comply with DoD IA standards for computers that access the MTF on-site and from remote locations.*

- *(MED0530: CAT II) The IAO will ensure vendors must comply with the DoD Public Key Infrastructure policy and obtain (an approved DoD PKI Certificate) via a Common Access Card (CAC), External Certificate Authority (ECA) or DoD issued Alternate Token certificate.*

- *(MED0540: CAT II) The IAO will ensure that a password policy with capability to enforce minimum length in accordance with the established site security policy and applicable DoD regulations, including Joint Task Force CTO's and INFOCON guidance, for remote administration of networked medical devices.*

5.3 Authentication

A registry of vendor-partners that require protected access to specific systems and devices must be developed to ensure that access to systems and devices is granted only to appropriate entities and agents. Access to systems and devices must be accomplished IAW the Secure Remote Computing STIG. The system or device program manager will be responsible for development

of the registry when any new system or device is deployed. The operation and maintenance activity will be responsible for maintaining the registry thereafter.

• *(MED0550: CAT II) The IAO will ensure a registry of vendor-partners that require protected access to specific systems and devices is created and maintained.*

• *(MED0560: CAT II) The IAO/NSO will ensure that all remote/external or vendor connections utilized to manage, maintain or support network enabled network devices are accomplished IAW the Secure Remote Computing STIG, DODI 8551.1, Service Specific Firewall Policy and appropriate network and OS STIGS.*

In addition to complying with this STIG and HIPAA regulations, all vendors are required to complete an either a Tricare Management Activity or component level Business Associate Agreement (BAA) for remote access for administering and managing networked medical devices.

The following requirements must be included in the BAA:

a. Physical location of each person requesting access

b. Full name and Social Security Number or Foreign National Identifier

c. Trust level or Clearance level

d. IP address of computer managing devices

e. Signed by the Chief Executive Officer (CEO) or security representative of company, including address and phone number

f. Signed by the MTF's Chief Information Officer (CIO)

• *(MED0570: CAT I) The IAO/NSO will ensure that all external vendor connections have an up-to-date BAA.*

6. NETWORKED MEDICAL DEVICE SECURITY

The systems' and devices' functional proponent will be responsible for working with the medical device manufacturers to apply NSA, DoD IA control, and DISA STIG OS hardening guidance to all medical systems/devices. By applying these guidelines, the device manufacturers will turn off or disable all unnecessary communications PPS.

Security features of OSs will be configured in a standardized manner to provide maximum feasible safeguards with the highest level of security possible. These configurations will be periodically checked via an automated mechanism and reapplied, as required. For specific details on OS security configurations, refer to the appropriate OS STIG (e.g., Windows, UNIX, OS/390, etc.).

The IAO must ensure host OSs are configured according to the latest applicable STIG, when possible, as so not to affect patient care or take away from the mission of the MHS. STIGs provide configuration guidance to achieve a minimum baseline level of security. Operational requirements may prevent implementation of all STIG requirements. If a requirement cannot be met, a POA&M is required as part of the accreditation documentation and must be approved by the appropriate DAA.

The settings defined in this STIG are guidelines that the IAO and site IA staff will seek to implement to the extent possible. Any exception to the requirement must be documented, and the staff will strive to work with the device manufacturer to implement changes to satisfy the IA requirement.

6.1 Device Configuration

6.1.1 Device Settings

The following settings are required, when achievable, without affecting patient care or device functionality as determined by the service program manager or functional manager.

- *(MED0590: CAT II) The IAO will ensure if the networked medical devices run on an OS platform, then the host must be STIG compliant prior to the installation of the networked medical device, or exceptions must be submitted to the DAA for approval.*

6.1.1.1 Auxiliary Port

The auxiliary port (AUX) is often used for administration activities or to connect remote administration devices. These ports have been known to be used by individuals to gain unauthorized access to devices for malicious means.

- *(MED0600: CAT III) The medical device administrator will ensure the device auxiliary port is disabled; if a secured modem providing encryption and authentication is not connected.*

6.1.1.2 Modem

Dial-up connections are infrequently used in the DoD community; however, if a dial-up connection is the only method available to administer a networked medical device, precautions must be taken to ensure device security. All modem use must be approved by the appropriate component DAA. See the Secure Remote Computing STIG for details and requirements.

- *(MED0610: CAT III) The IAO/NSO will ensure modems connected to networked management devices are disabled or disconnected when not in use.*

- *(MED0620: CAT II) The IAO/NSO will ensure modems are not connected to the networked medical device.*

6.1.1.3 Other Peripherals

Printers, faxes, bar code scanners, and other peripherals are often tied to networked medical devices. These devices must be handled with the same level of care and caution as the networked medical device so as not to introduce an unacceptable level of risk to the networked medical device and to the network itself.

- *(MED0630: CAT II) The IAO/NSO will ensure peripherals used or connected to the networked medical device do not introduce risk to the device.*

6.1.1.4 Internet Protocol Version 6 (IPv6)

Networked medical devices must be IPv6-compliant prior to implementation on the network IAW DoD IPv6 Transition Office (DITO) IA Guidance for Milestone Objectives 3 (MO3). There is guidance requiring all networked devices on DoD networks to be IPv6 compliant or capable. New devices must be compliant upon purchase; existing systems must comply IAW the instruction. Networked medical devices must be able to support Internet Protocol Version 4 (IPv4) until DoD IPv6 is fully implemented.

- *(MED0640: CAT III) The IAO/NSO will ensure that all networked medical devices are capable of supporting IPv6 now or submit a PO&AM for those not meeting this requirement.*

6.1.2 Networked Medical Device Security Settings

As with all nodes on a network, there are settings that, when properly implemented, reduce the likelihood of an attack or of a vulnerability being exploited by an unauthorized user. In implementing the settings outlined in the following sections, when possible, the overall device security will be enhanced.

6.1.2.1 Default Passwords

Since applications are delivered containing userids and accounts that have well-known default passwords, malicious users can make use of these accounts and userids unless action is taken prior to deployment. Vendor-supplied passwords will be changed to non-trivial passwords that are in compliance with DoD standards for strong passwords prior to testing and deployment of the product.

- *(MED0650: CAT I) The IAO/NSO will ensure that default passwords are changed.*

6.1.2.2 Extraneous Services

Many applications are received from vendors with extraneous services (such as modem ports, network connections, etc.) which are not desired or needed in the medical facility and which open the device and network up to unnecessary risks. These extraneous services/devices will be disabled prior to deployment.

- *(MED0660: CAT II) The IAO will ensure the networked medical devices do not utilize any services or capabilities other than what is required to perform its intended clinical function (e.g. Domain Name Service (DNS), Electronic Mail (E-Mail), FTP services, Telnet). If these services exist on the device they will be disabled or uninstalled if possible.*

6.1.2.3 Remote Administration

Data contained on medical devices is sensitive and requires special considerations with handling, storing, and administration. Secure services shall be used to remotely and securely administer networked medical devices. DoDI 8551.1 compliancy is required for any services used for remote administration.

- *(MED0670: CAT II) The medical device administrator will ensure any services used for remote administration are fully compliant with all conditions of use IAW DoDI 8551.1.*

6.1.2.4 Password Protection

Accounts must be protected from being accessed by unauthorized users. When an account is created for a user, that user must be given a temporary password. The IAO will brief the user on implementation of password protection. The IAO will verify that the DoD password policy contained in USCYBERCOM CTO 07-15 is followed for all user accounts. If users are unable to comply with the DoD password policy, the IAO will set the passwords to the highest level (length and character parameters) that the system will allow and generate a POA&M indicating when DoD password policy can be followed.

- *(MED0700: CAT I) The IAO/NSO will ensure all network enabled medical devices are password protected.*

- *(MED0710: CAT II) The IAO/NSO will record the locally configured passwords used on communications devices and store them in a secured manner.*

• *(MED0710: CAT II) The IAO/NSO will ensure that any passwords used are compliant with USCYBERCOM CTO 07-15 guidelines.*

6.1.2.5 Accounts

Applications are delivered containing userids and accounts that may not be required in an operational setting. The IAO will remove all unnecessary accounts prior to deployment, and all created accounts will be assigned at the lowest permission level possible that will allow users to perform their jobs.

• *(MED0720: CAT II) The IAO/NSO will ensure only those accounts necessary for the operation of the medical-device and for access logging are documented and maintained.*

• *(MED0730: CAT II) The IAO/NSO will ensure all accounts are assigned the lowest privilege level of access/rights necessary to perform their jobs.*

6.1.2.6 Device Auditing

Audit reviews are conducted to ensure no one is attempting to gain unauthorized access and that any unauthorized transaction attempts are mistakes and not malicious attacks. Auditing will be configured and implemented on all systems. Auditing can result in a great deal of information being collected on device/system activities. There should be a determination made of critical events/data to audit to allow enough granularity to allow for the monitoring of intrusive activity.

Controls should be in place to ensure audit log data is not deliberately or accidentally disabled or deleted. If the logging capability is not configured correctly, there is a risk that logging would not be complete and an attack could remain undetected.

Documentation is a key component to consistent security measures being applied across an environment or an enterprise. Roles, responsibilities, and security access authorizations will be clearly documented. Each user group should be aware of their specific roles and their responsibilities to protect data. Auditing will be enabled for all user accounts to ensure data integrity.

Controls will be in place to ensure audit log data is protected from corruption or deletion. This control is necessary to ensure audit log data is protected. Without protection, the data could be changed or deleted intentionally or unintentionally, rendering the data inaccurate or unavailable for investigative purposes.

Controls should be in place to obtain a list of the “administrative user” userids, and then ensure the appropriate logging of these userids is taking place. Monitoring for evidence of misuse helps to protect the integrity and availability of the system.

The security audit log will be reviewed on a regular basis. Failure to monitor the system to detect unauthorized activities and reconciliation of abnormalities could result in unauthorized disclosure, modification, or destruction of sensitive data.

The IAO will conduct security audit reviews on all production systems and document the results. The IAO should become familiar with HIPAA audit requirements in order to monitor and review activity to ensure users are set up appropriately to satisfy these requirements IAW DoD 8500.2.

- *(MED0740: CAT III) The IAO/NSO will ensure the medical device audit log data is backed up weekly.*

- *(MED0750: CAT II) The IAO/NSO will ensure audit logs are protected from deletion.*

- *(MED0760: CAT III) The IAO/NSO will ensure the audit trail events are stamped with accurate date and time.*

- *(MED0770: CAT III) The IAO/NSO will ensure the audit trail events include source IP, destination IP, UserID, protocol used and action taken.*

- *(MED0780: CAT III) The IAO/NSO will ensure administrator logons, changes to the administrator group, and account lockouts are logged.*

6.2 Wireless

Refer to the Wireless STIG and the DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD GiG, for additional guidance and configuration requirements of personal digital assistants (PDAs) and wireless LAN devices.

- *(MED0800: CAT II) The IAO will ensure wireless LANs and devices are configured in accordance with the Wireless STIG.*

- *(MED0810: CAT I) The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/Personal Computer (PC) connection methods, and services) are approved by the DAA prior to installation and use for processing DoD information.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Federal Food, Drug, and Cosmetic Act (FD&C Act), Amended December 31, 2004
Code of Federal Regulations - Title 21 - Food and Drugs
Medical Device User Fee and Modernization Act of 2002
Food and Drug Administration (FDA) - Safe Medical Devices Act of 1990
FDA - Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software
IEC 80001

DoD Directive (DoDD) 8500.1, "Information Assurance (IA)"
DoD Instruction (DoDI) 8500.2, "Information Assurance (IA) Implementation"
DoDI 8551.1, "Ports, Protocols, and Services Management (PPSM)"
DoD CSC-STD-002-85, "DOD Password Management Guideline"
CJCSM 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)"
DoD CM-400-260-01, "Software Requirements Specification (SRS) for the Network Management (NM) Functional Area Of The Defense Information Infrastructure (DII)"
DoD Directive Number 3020.26, Continuity of Operations (COOP) Policy and Planning
DoDI Number 3020.39, Integrated Continuity Planning for Defense Intelligence, ASD (C3I)
DoDD Number O-8530.1, Computer Network Defense (CND)
Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)" and Supplements 1 and 2, not dated
ASD (NII) Memo, "Internet Protocol Version 6" (IPv6)
CJCSI 6212.01D "Interoperability and Supportability of Information Technology and National Security Systems"
Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Guidance for Milestone Objectives 2 (MO2),
DoD 5200.1-R, "Information Security Program,"
ASD (C31) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives"
(DoDD) 5200.28 - Security Requirements for Automated Information Systems
DoDI 5200.40 – DoD Information System Technology Security Certification
MHS Policy - Sanitization and Disposal of Electronic Storage Media
MHS Information Technology Equipment Procedures
MHS Standard Operating Procedures for Management of Unauthorized Disclosure of DoD Sensitive Information Incidents, July 19 2005
MHS Memorandum: MHS IS Policy Guidance, March 27, 2007
MHS Memorandum: MHS IA Implementation Guide, March 27, 2007
MHS Implementation Guide 12 (Information Assurance Vulnerability Program), March 27, 2007
JCAHO Hospital Accreditation Standards (HAS) 2008
Health Insurance Portability and Accountability Act (HIPAA) of 1996
USCYBERCOM Net Defense home page – https://www.cybercom.mil
DISA STIGs (Network, Wireless, OS) http://iase.disa.mil/stigs/stig/index.html

This page is intentionally left blank.

APPENDIX B. GLOSSARY OF TERMS

Access Control List (ACL) – Mechanism implementing discretionary and/or mandatory access control between subjects and objects.

Authority to Operate (ATO) – The IAM monitors IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). The IAM bases ATO decisions based on this status to ensure that the established baseline of the system has no significant changes.

Common Access Card (CAC) – The CAC is a United States DoD smartcard issued as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel.

Community of Interest (COI) – A network of people who are committed to the mutual exchange of ideas and information.

Demilitarized Zone (DMZ) – Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. A DMZ is also called a "Screened Subnet." A method for placing web and other servers that serve the general public outside the firewall and, therefore, isolating them from internal network access.

DIACAP – DoD Information Assurance Certification and Accreditation Process.

Enclave – A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.

External Certificate Authority (ECA) – An external issuer of digital certificates, which are then used for digital signatures or key pairs.

Inside Security Screening Router (ISSR) – A router placed between the firewall and internal trusted enclave in an effort to provide VLAN separation.

Intrusion Detection System (IDS) – Tools that identify and respond to attacks using defined rules or logic. IDS can be networked or host-based.

IPv6 – Internet Protocol version 6 (IPv6) is an Internet Layer protocol for packet-switched internetworks. The Internet Engineering Task Force (IETF) has designated IPv6 as the successor of IPv4, the first and still dominant version of IP for general use on the Internet.

Medical Device Types – These devices are used for diagnostic, monitoring, and therapeutic purposes. These device types are used together to influence patient outcome. These devices often possess network connectivity capabilities with the resulting interconnectivity allowing device to device interaction via the MTF network. The three Medical Device Types are:

- **Diagnostic** – Diagnostic devices assist in efforts to determine the presence or absence of a disease process or traumatic injury.

- **Monitoring** – Monitoring equipment allows a real-time and/or a recorded history of a patient's physiological status. Real-time monitoring allows for an immediate response to a deterioration or change in patient status. The collecting/data-logging aspects of monitoring allow for observation of changes over time, patient activity levels, or other environmental factors exerting an impact on patient condition.

- **Therapeutic** – Therapeutic devices provide the patient with some form of medical or pharmacological treatment.

Mission Assurance Category (MAC) – MACs are based on the mission needs of the warfighter and used primarily to determine requirements for IS integrity and availability. A MAC is always combined with an independent level of confidentiality. The three levels of confidentiality are as follows: High (processing of classified information), Medium (processing sensitive information), and Public (processing public information). Enclaves always assume the highest MAC and confidentiality classification of the applications or IT-based processes they support and derive their security requirements from those systems (DoD 8500.2). DoD has defined three Mission Assurance Categories as follows:

- **MAC I**: Requires the most stringent protection measures. MAC I systems require high integrity and high availability for IS handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

- **MAC II**: Requires additional safeguards beyond best practices to ensure adequate assurance. MAC II systems require high integrity and medium availability for IS handling information that is important to the support of deployed and contingency forces.

- **MAC III**: Requires protective measures, techniques, or procedures generally commensurating with commercial best practices. MAC III systems require basic integrity and basic availability for IS handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term.

Network-Enabled Medical Devices – These are devices designed and intended to reside on a facility;s network.

Out-of-Band (OOB) Management – Employing a management channel that is physically isolated from the data channel.

Security Zones – A method for isolating a system from other systems or networks.

Sensitive – Any information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under 5 U.S.C Section 552a (the Privacy Act), but that has not been specifically authorized to be kept classified in the interest of national defense or foreign policy.

Sensitivity Level – Information representing elements of the security label(s) of a subject and an object. Sensitivity labels are used by the trusted computing base as the basis for mandatory access control decisions.

Simple Network Management Protocol (SNMP) – The management protocol created for sending information about the health of the network to network management consoles.

Transmission Control Protocol/ Internet Protocol (TCP/IP) –. The protocol suite developed by the DoD in conjunction with the Internet. It was designed as an internetworking protocol suite that could route information around network failures. Today, it is the de facto standard for communications on the Internet.

Virtual Private Network (VPN) – A system that uses the public Internet as the backbone for a private interconnection (network) between locations.

Virus – A program intended to damage a computer system. Sophisticated viruses are encrypted and hide in a computer and may not appear until the user performs a certain action or until a certain date.

This page is intentionally left blank.

APPENDIX C. LIST OF ACRONYMS

Acronym	Definition
ACL	Access Control List
AIS	Automated information System
ATO	Authority to Operate
AUX	Auxiliary
B2B	Business to Business
BAA	Business Associate Agreement
C&A	Certification & Accreditation
CAC	Common Access Card
CAT	Category
CBER	Center for Biologics Evaluation and Research
CC/S/A	Combatant Command/Services/Agencies
CDRH	Center for Devices and Radiological Health
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CJCSI	Chairman Joint Chiefs of Staff Instruction
CJCSM	Chairman Joint Chiefs of Staff Manual
CNDSP	Computer Network Defense Service Provider
COI	Community of Interest
CTO	Communications Tasking Order
DAA	Designated Approving Authority
DIACAP	DoD Information Assurance Certification and Accreditation Process
DiD	Defense in Depth
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITO	DoD IPv6 Transition Office
DMZ	Demilitarized Zone
DNS	Domain Name Service
DKO	Defense Knowledge Online

Acronym	Definition
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSAWG	DISN Security Accreditation Working Group
ECA	External Certificate Authority
ePHI	Electronic Protected Health Information
FA	Firewall Administrator
FDA	Food and Drug Administration
FD&C Act	Federal Food Drug & Cosmetic Act
FIPS	Federal Information Processing Standards
FSO	Field Security Operations
GiG	Global Information Grid
HID	Host Intrusion Detection
HIPAA	Health Information Portability and Accountability Act
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IDS	Intrusion Detection System
IDPS	Intrusion Detection/Protection System
IEC	International Electrotechnical Commission
INFOCON	Information Operations Condition
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS	Information Systems

Acronym	Definition
ISSR	Inside Security Screening Router
IT	Information Technology
IV	Intravenous
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Mission Assurance Category
MHS	Military Health Systems
MO3	Milestone Objective 3
MTF	Military Treatment Facility
N/A	Not Applicable
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPRNet	Non-Classified Internet Protocol Routing Network
NSA	National Security Agency
NSO	Network Security Officer
OOB	Out of Band
OS	Operating System
OSSR	Outside Security Screening Router
PC	Personal Computer
PDA	Personal Digital Assistant
PHI	Protected Health Information
PII	Personally Identifiable Information
PIT	Platform IT Certification
POA&M	Plan of Action and Milestone
POC	Point of Contact
PPS	Ports, Protocols, and Services
SA	System Administrator
SM	Security Manager
SNMP	Simple Network Management Protocol

Acronym	Definition
SPAN	Switch Port Analyzer
SRR	Security Readiness Review
SSP	System Security Plan
STIG	Security Technical Implementation Guide
STIGID	Security Technical Implementation Guide Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
USCYBERCOM	United States Cyber Command
VLAN	Virtual Local Area Network
VMS	Vulnerability Management System
VPN	Virtual Private Network
WARNORD	Warning Order

APPENDIX D. MEDICAL DEVICE SPECIALITIES

Anesthesiology: Science dealing with partial or complete loss of sensation with or without less of consciousness as a result of disease, injury, or administration of an agent, usually by injection or inhalation. (Examples include: 868.1040-Powered Algesimeter; 868.23-Breathing Frequency Monitor)

Cardiovascular: Pertains to the heart and blood vessels. (Examples include: 870.2300-Cardiac Monitor; 870.3700-Pacemaker Programmers)

Clinical Chemistry and Clinical Toxicology: Pertains to the molecular structure and composition of substances. Toxicology involves the detection of toxic substances and treatment of toxic manifestations and the prevention of poisoning. (Examples include: 8622900-Automatic Urinalysis System and 862.1120-Blood Gas/Ph Test System)

Dental: Pertains to the teeth. (Examples include: 872.4850-Ultrasonic Scaler; 872.3661-Optical Impression System's for CAD/CAM)

Ear, Nose, and Throat: (Examples include: 874.1060-Acoustic Chamber for Audiometric Testing and 874.1820-Surgical Nerve Stimulator/locator)

Gastroenterology and Urology: Pertains to the stomach, intestines, urinary tract, and genital tract. (Examples include: 876.2040-Enuresis Alarm and 876.1400-Stomach PH Electrode)

General and Plastic Surgery: Manual and operative procedures for correction of deformities and defects, repair of injuries, and diagnosis and cure of certain diseases. Plastic surgery deals with the restoration, repair, or reconstruction of body structures. (Examples include: 878.4160-Surgical Camera and 878.5910-Pneumatic Tourniquet)

General Hospital and Personal Use: (Examples include: 880.2460-Electrically Powered Spinal fluid Pressure Monitor and 880.5410-Neonatal Transport Incubator)

Hematology and Pathology: The study of blood and the nature and causes of disease processes. (Examples include: 864.5680-Automated Heparin Analyzer and 864.5350-Microsedimentation Centrifuge)

Immunology and Microbiology: The study of the immune response to infectious diseases, transplantation of organs, allergy, autoimmunity, cancer, and microorganisms. (Examples include: 866.4520-Immunofluorometer equipment and 866.2560-Microbial Growth Monitor)

Neurology: Pertains to the nervous system and its diseases. (Examples include: 882.1855-Electroencephalogram (EEG) Telemetry System and 882.5820-Implanted Cerebellar Stimulator)

Obstetrical and Gynecological: Pertains to female reproductive organs including breasts. This field concerns management of women during pregnancy, childbirth, and puerperium. (Examples include: 884.2600-Fetal Cardiac Monitor and 884.2800-Computerized Labor Monitoring System)

Ophthalmic: Pertains to the eye. (Examples include: 886.1120-Opthalmic Camera and 886.1850-AC Powered Slitlamp Biomicroscope)

Orthopedic: Pertains to loco motor structures such as, skeleton, joints, muscles, fascia, ligaments, and cartilage. (Examples include: 888.3080-Intervertebral body fusion Device and 888.1240-AC Powered Dynamometer)

Physical Medicine: (Examples include: 890.5360-Measuring Exercise Equipment and 890.1925-Islkinetic Testing and Evaluation System)

Radiology: Pertains to radioactive substances such as, X-rays, radioactive isotopes, and ionizing radiations. (Examples include: 892.1750-Computed Tomography X-ray System and 892.1680-Statiomary X-ray System)