ENTERPRISE SYSTEM MANAGEMENT

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

5 June 2006

Developed by DISA for the DoD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

This page is intentionally left blank.

LIST OF FIGURES

LIST OF TABLES

This page is intentionally left blank.

1. INTRODUCTION

This Enterprise System Management (ESM) Security Technical Implementation Guide (STIG) provides security configuration guidance for software products designed to deliver enterprise-class system management functions. While the boundaries of the ESM discipline are such that there is no authoritative definition of an ESM product, *Section 2, Enterprise System Management Overview*, provides a generic description of the elements characteristic of most ESM products. *Section 3, Enterprise System Management Security*, provides general guidance for ESM products; specific commercial products are addressed in appendices.

Use this document in conjunction with the other STIGs developed by the Defense Information Systems Agency (DISA). The operating system (OS) STIGs provide crucial guidance for securing the platforms on which the ESM products run. The STIGs that cover database and web server products provide guidance to ensure that those services used by ESM products also support a secure environment.

1.1 Background

For many years, network management products have been used to monitor and manage networks that span wide areas. These products helped to automate repetitive tasks and allow remote configuration changes to be made. Management disciplines and industry standards were eventually created to promote the use and further development of the products. The success of network management products encouraged vendors to develop system management products to provide similar functions for the number of growing individual server and client machines.

While the number of network elements and individual hosts continues to increase, more consistency and efficiency is being sought for management functions. Scalability has been, and continues to be, a significant issue. To address these needs, ESM software is built on the foundation created by network and system management products. The ESM products are designed to automate and centralize the administration, monitoring, operations, and support of applications, systems, and platforms on an enterprise scale.

The use of ESM products to track software usage and to deploy security updates provides obvious benefits. The extent of an organization's vulnerability to a specific worm or virus can be quickly understood. Server and client hosts can be made more secure against attack with less effort and in a shorter period of time. The need for System Administrators to manually install updates on a large number of machines is mostly eliminated.

The configuration and use of ESM products can introduce and increase the number of potential vulnerabilities to an enterprise. ESM software frequently runs with elevated privileges and has a large span of control over hosts as a result any compromise of ESM elements could lead to widespread problems. Part of an attack might include disabling the ESM software so that security patches cannot be deployed, leaving a large number of hosts open to further attack. Another attack strategy could include using configuration management functions in the ESM product to deliver corrupt software or to maliciously alter configuration settings on a large scale.

The goal of this document is to provide guidance that allows ESM products to be used without degrading the confidentiality, integrity, or availability of the enterprise. It should be noted that Field Security Operations (FSO) support for the STIGs, Checklists, and Tools is only available to DoD Customers.

1.2 Authority

DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems 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, NSA." This document is provided under the authority of DoD Directive 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 MAC II Sensitive level, containing sensitive information.

1.3 Scope

This document describes security requirements to be applied to ESM products used in DoD environments. The information is designed to assist Security Managers, Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with the creation of more secure ESM configurations. As noted in the previous section, application of the requirements is intended to provide a certain level of assurance. Individual sites must determine if this level of assurance is appropriate to their environment.

This document provides both general and product-specific security guidance. Vendor implementation of ESM functions does vary; and most commercial products provide only subsets of all the functions generally associated with ESM.

Specific guidance is provided for the following:

- Tivoli enterprise management products
- Microsoft Systems Management Server 2003

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. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

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. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*)." If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "(*N/A: CAT III)*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1. Vulnerability Severity Codes

1.6 Information Assurance Vulnerability Management (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 Joint Task Force Global Network Operations (JTF-GNO) web site: http://www.cert.mil.

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 NIPRNet URL for the IASE site is http://iase.disa.mil/. The National Institute of Standards and Technology (NIST) site is http://csrc.nist.gov/pcig/cig.html. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov** address. The STIGs are available to users that do not originate from a **.mil** or **.gov** address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@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.

2. ENTERPRISE SYSTEM MANAGEMENT

2.1 General Overview

ESM can be described as the automation of activities involved in administering, monitoring, operating, and supporting multiple information systems. The systems are commonly of various platform types and connected by one or more networks. Geographical configurations may vary from many systems collocated to a few systems distributed over a wide area. ESM commonly involves automating repetitive tasks and remotely performing activities that would otherwise be performed by local System Administrators. This document provides implementation guidance for security controls that apply to ESM applications.

Because the scope of ESM functions is broad, it is not always obvious that a specific product is an ESM application. In fact, there is a close functional similarity between ESM applications and network management applications that generally preceded them. Network management applications traditionally focused on network devices and not application hosts, but that focus has gradually been softened. In some cases, ESM product suites include network, host, and application management components.

This section provides an overview of what an ESM application does and some of the elements that might be used by the application. This should provide a background to determine if a given application should be called an ESM application and should be subject to the requirements in this document.

There are two particular concepts that impact the security requirements for DoD implementation of ESM applications. The first of these is the notion of an enclave. The Committee on National Security Systems (CNSS) *National Information Assurance (IA) Glossary* defines an enclave as the "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." This is discussed in detail in the *Enclave STIG* and the NSA *Information Assurance Technical Framework*. This impacts ESM implementation because some requirements vary according to whether an ESM application spans enclave boundaries. Because applications that operate entirely within an enclave boundary are protected by the enclave perimeter defenses, less stringent requirements apply to those implementations. However, most ESM applications are designed with the capability to operate across networks that could easily span enclave boundaries, so it is necessary to determine if a specific implementation crosses enclave boundaries when applying the requirements.

The second concept impacting DoD ESM implementations is the definition of IA and IA-enabled products as discussed in DoD Directive 8500.1 and DoD Instruction 8500.2. The definition is detailed in *Section 3.2.1, Application Design Characteristics*. This impacts ESM implementation because additional requirements apply to IA and IA-enabled products. Those products provide some level of security services so their implementation requires greater caution. While most ESM applications are not IA products, many are IA-enabled because they implement access controls over ESM administrative functions. Therefore, it is necessary to determine if an ESM application is an IA or IA-enabled product when applying the requirements.

A final general note concerning ESM applications and the importance of their security is necessary. Certain types of ESM applications have the ability to generate very significant impact to the systems under their control. Acting as automated System Administrators, these applications may change operational status and configuration, report state information, and distribute critical security data such as suspicious event notices and virus signature updates. These functions generally take on the importance of the availability of the systems on which they are performed. In short, an ESM application may become a mission-essential application. In addition the applications have privileged access in order to accomplish their functions. Therefore, the security of these applications demands careful implementation in order to ensure the integrity and availability of the systems they manage.

The following sections describe functional areas and implementation elements that are common to ESM applications. While there is no practical consensus that these items must be found in every ESM application, there are some standards that provide a common basis for discussion.

2.1.1 ESM Functional Areas

The International Telecommunication Union (ITU) Open Systems Interconnection (OSI) standards relating to management functions provide a helpful framework in which to discuss ESM applications. Recommendation X.700, "Management framework for Open Systems Interconnection (OSI) for CCITT applications" describes five Management Functional Areas (MFAs): Fault management, Configuration management, Accounting management, Performance management, and Security management. This characterization is sometimes referred to as the FCAPS model, after the first initial of the name of each of the areas. The following figure shows these areas with some of their associated functions from the X.700 Recommendation:

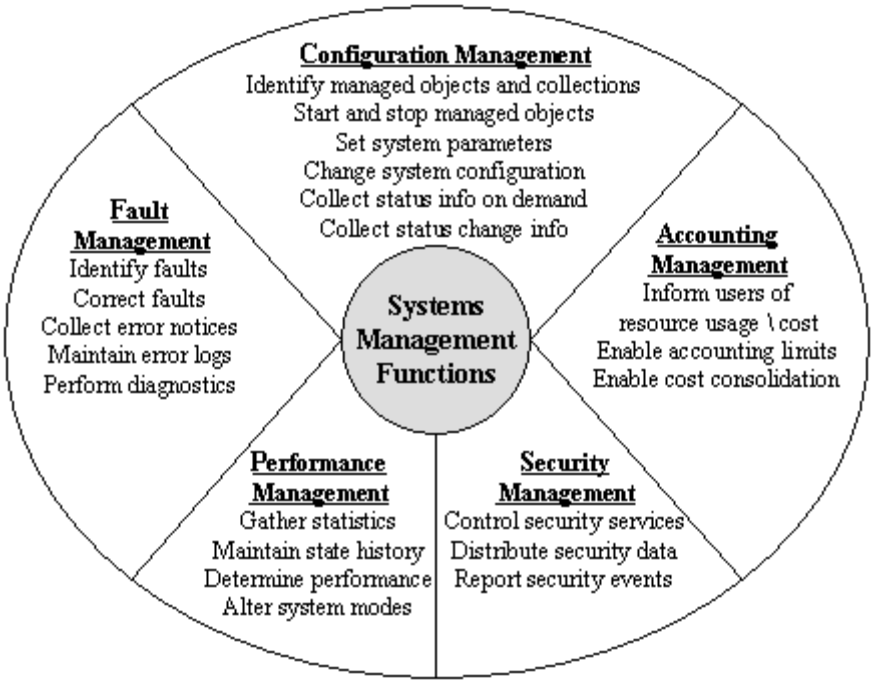

Figure 2-1. ESM Management Functional Areas

Two important notes apply to the FCAPS model:

- Though there are five functional areas, most products rely on shared mechanisms to deliver their functions. For example, a common mechanism is likely to be used to collect fault data as well as performance data.

- This same model is used to describe functional areas used for network management. ITU Recommendation M.3400, "TMN management functions" uses the same terminology in its discussion of functions.

In terms more specific to ESM, the functional areas may be implemented in the following ways:

- Fault Management - ESM applications providing centralized monitoring and reporting of function availability on client systems fit in this area. Some applications also perform diagnostic and corrective action on clients. Applications that are described as offering generic event management are generally providing fault management functions.

- Configuration Management - ESM applications providing remote management of client systems fit in this area. These applications may change the operating parameters or state of the systems under their control. Applications providing hardware and software inventory and applications that deploy software and other data also fit in this area.

- Accounting Management - ESM applications that monitor system resource usage for the purpose of limiting consumption or collecting data for cost allocation fit in this area.

- Performance Management - ESM applications providing longer-term pictures of client system availability and workload management data fit in this area.

- Security Management - ESM applications providing centralized monitoring and reporting of security events fit in this area. Data may be consolidated from firewalls, intrusion detection systems, or other host security services. Applications with sophisticated event correlation engines may offer the capability to change security parameters or to isolate hosts that may have been compromised.

ESM products are quite likely to span these functional areas because the mechanisms and data used are often common. Most ESM products use elements of configuration management to organize their tasks and data. With the possible exception of security management functions, the requirements for securing ESM applications are generally the same for all the functional areas.

2.1.2 ESM Implementation Elements

ESM products are like other categories of software products in terms of the diverse ways in which they are designed and implemented. The concept of ESM has developed concurrently with open system standards, but vendors frequently choose proprietary versions of elements to deliver ESM functions. While proprietary solutions may have efficiency or performance advantages, their unique elements can create interoperability issues when combined and they certainly lead to confusion when discussed.

This section provides a very brief discussion of some of the implementation elements for ESM applications. The objective is to provide terminology that can be used to describe common elements that exist in diverse vendor implementations. Some of the organizations and the standards they promote are mentioned as context for later ESM application discussions.

The body of this document uses generic terms to discuss ESM application elements. In the vendor-specific appendices, these generic terms are related to the vendor terminology as appropriate.

- Manager - An ESM manager is an application that usually runs on a dedicated host server. The application is responsible for organizing and controlling functions that are carried out on, or for, clients within the manager's span of control. ESM manager applications include elements that maintain data about the clients. The applications usually include support that enables remote administration and status displays.

- Agent - An ESM agent is an application, usually small, that runs on a client host that may be called a managed element. The agent application is responsible for collecting data, performing actions on the managed element, and responding to commands issued by an ESM manager. Agents may maintain continuous or periodic network connections to their associated manager.

- Console - An ESM console is an application that provides an interface to the ESM manager for an administrator to enter commands and display data. In current products, ESM consoles are usually implemented as graphical interfaces that are run on hosts remote to the manager. Some ESM consoles are implemented as web applications using a browser to provide the graphical user interface.

- Management Data Repository - An ESM management data repository is the logical database used by an ESM manager to store information about the clients on which agents are deployed. An object-oriented approach is common, representing clients as objects associated with attributes and methods that apply to them. The repository may also contain definitions of configuration settings that are to be applied to groups of clients.

There are a number of ways in which these elements can be assembled as an ESM application. The elements are arranged in a hierarchy with the ESM manager residing on a server at the top, and the clients with ESM agents at the bottom. The following figure shows two common implementations. The configuration on the left shows a basic example. On the right, an additional tier of manager servers is shown. The multiple tier management configuration is useful for large organizations that have many clients that are distributed over a wide area. The middle tier of managers can be co-located with the clients. This distributes the workload from the top tier to the middle tier servers and reduces the number of network connections to the top tier server. These characteristics make this solution scalable to very large environments.

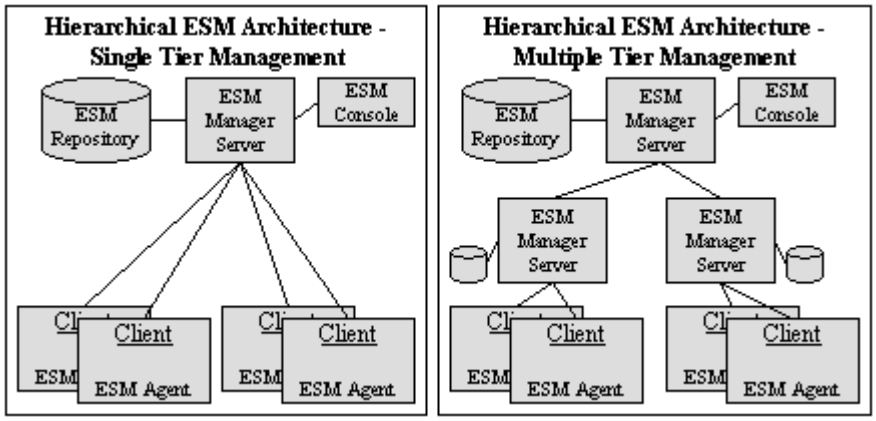

Figure 2-2. Hierarchical ESM Architectures

Another possible configuration involves the use of multiple ESM manager servers for each client with an ESM agent. The following figure shows a basic example. The manager servers operate in parallel, each with specific areas of responsibility. The managers may communicate in order to share information about the clients.

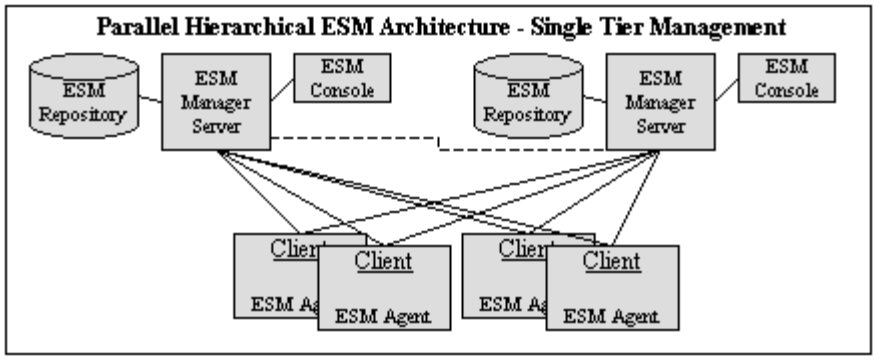

Figure 2-3. Parallel Hierarchical ESM Architecture

Common to all of these configurations is the transfer and storage of management data. This data is carried by network connections between managers and agents. It is stored in management data repositories. Several standards efforts have been undertaken in order to promote greater interoperability among products from different vendors.

A discussion of the standards related to management data can be helpful in identifying ESM applications. However, this is a complex subject that requires extensive material for explanation. A review of the documents from the Internet Engineering Task Force (IETF) (http://www.ietf.org/) and the Distributed Management Task Force (DMTF) (http://www.dmtf.org/) is strongly recommended. The following brief notes identify the most prominent standards that may be employed in ESM applications:

- SNMP - The Simple Network Management Protocol (SNMP) is defined by the IETF as "a simple protocol by which management information for a network element may be inspected or altered by logically remote users". The objective for SNMP is to "provide a simple, workable architecture and system for managing TCP/IP-based internets and in particular the Internet." Although SNMP was initially intended for management of network devices, it has been widely adopted for use in diverse management environments. SNMP is described by many documents; RFC1157 provides the basic definition.

- CMIP - The Common Management Information Protocol (CMIP) is a protocol for network management defined by the ITU as part of the OSI management standards. CMIP was designed for OSI-based communication protocols and was intended to replace SNMP. CMIP Over TCP (CMOT) was defined for use with IP-based networks. RFC1189 defines a network management architecture using CMOT. CMIP and CMOT have not been widely adopted.

- DMI - The Desktop Management Interface (DMI) specification was defined by the Distributed Management Task Force (DMTF) as a framework for the management of Desktop systems and servers. The DMI architecture consists of layers that allow interoperability between management server and client implementations from different vendors. The DMTF has announced an "end of life" for the DMI standard in favor of more broadly focused management standards.

- CIM - The Common Information Model (CIM) incorporates a specification and a schema defined by the DMTF as "a conceptual information model for describing managed entities, their composition, and relationships." An object-oriented architecture is used in the definition and structure of the data. The CIM management schema is divided into a Core Model, Common Models, and extension schemas. The Core Model covers elements applicable to all management areas. The Common Models cover elements common to particular management areas including systems, applications, databases, networks, and devices. Technology specific extensions can be created through the extension schemas. DMTF incorporated the use of directories in the CIM through the Directory Enabled Networks (DEN) initiative. DEN provides a mapping for CIM to an LDAP structure to enable the use of directories to locate management information and access management

data. Both the DMTF and the IETF have done work to enable the representation of policy information as an extension to the CIM. The DMTF CIM Policy Model and the IETF Policy Core Information Model (PCIM) (RFC3060 and RFC3460) are designed to allow the expression of policy in vendor and device-independent terms that can be translated by software into device-specific configuration changes that implement the policy.

- WBEM - Web-Based Enterprise Management (WBEM) is defined by the DMTF as "a set of management and Internet standard technologies developed to unify the management of enterprise computing environments." WBEM is expressed primarily by three core standards: the CIM, the Representation of CIM in Extensible Markup Language (XML) specification, and the CIM Operations over HTTP specification. The Representation of CIM in XML specification provides the format for encoding CIM declarations (classes, instances, and qualifiers) and CIM messages in XML. The CIM Operations over HTTP specification defines "a mapping of CIM operations onto HTTP" to support the transport of CIM messages. Vendors have developed implementations of WBEM to enable management of their products. Microsoft's Windows Management Instrumentation (WMI) is one well-known implementation of WBEM standards for Windows environments.

Concise descriptions of some of these technologies can be found in the Carnegie Mellon Software Engineering Institute's Software Technology Roadmap (http://www.sei.cmu.edu/str/).

To close the discussion of ESM implementation elements, it is reasonable to briefly raise two issues: the role of customization and the logical points of vulnerability.

The implementation of ESM requires some flexibility to account for the variety of objects and configurations that should be managed. In addition, ESM applications are frequently called on to perform ad hoc and non-standard operations on a one-time basis. Implementation flexibility is achieved by customizing ESM functions. Coding programs that are compiled into binary executables, as well as scripts that are interpreted at run time, may be used to accomplish this. In any case, these items become elements, though often temporary, of a specific ESM implementation. It is important to recognize that these "local" elements have to be considered when evaluating the security characteristics of an ESM implementation.

Finally, it is important to recognize some logical points of vulnerability that arise from elements in the ESM architecture. Briefly, these areas include:

- ESM managers and agents are applications that might be vulnerable due to errors in coding or configuration. ESM application failures can have negative impacts that are similar to administrator errors, but on a much larger scale.

- ESM data repositories are likely to hold data that represents, at a minimum, sensitive information. This is because that data includes specific configuration information. Disclosure or corruption of that data could lead to more serious vulnerabilities.

- ESM network communications are often critical to operations. Fault data that is not received by the manager or configuration commands that do not arrive at the agent can result in a loss of function that might be critical to maintaining system availability.

Reducing and eliminating vulnerabilities in ESM applications requires correct configuration and attention to vulnerability information for all of its elements. During 2002 serious vulnerabilities were discovered in a wide variety of vendor implementations of SNMP. This occurrence provided a good example of the potential impact of vulnerabilities in management applications. A failure to install the patches for these vulnerabilities could have seriously degraded the availability of a significant portion of the network management infrastructure. Avoiding such problems is essential to support DoD's net-centric operations.

3. ESM SECURITY

3.1 Introduction

ESM applications commonly perform sensitive functions, requiring elevated privileges, on multiple hosts. Some of these functions, such as security patch management, are essential to operations because they help to maintain secure environments. The conclusion from these facts is that security controls on ESM applications are critical.

While the impact can vary significantly, a compromise of an ESM application could result in a serious loss of the confidentiality or integrity attributes of hosts. Beyond that, the loss of a particular ESM function could result in a loss of an essential information assurance function that would effectively render the affected hosts inaccessible.

This section provides the general security requirements for the implementation of ESM products. Because of the diversity of products, these requirements are somewhat generic in nature. The product sections of this document further explain the requirements as they relate to specific implementations.

This section is broken into subsections that align with the IA control subject areas defined in Department of Defense (DoD) Instruction 8500.2, *Information Assurance (IA) Implementation*. These subject areas are as follows:

- Security Design and Configuration
- Identification and Authentication
- Enclave and Computing Environment
- Enclave Boundary Defense
- Physical and Environmental
- Continuity
- Vulnerability and Incident Management.

Some of these areas are further divided to provide a more cohesive presentation. The Personnel subject area is not included as there are no controls in that subject area that are addressed in an ESM product security review.

It is important to understand some of the specific terminology used in this section:

- ESM Administrator - An ESM administrator is responsible for configuring and operating one or more ESM products. An ESM administrator, using an ESM product, may perform some or all of the functions of a host SA.

- I&A Services - Identification and authentication (I&A) services are used to establish and verify the identity of an entity. Secure host operating systems always perform I&A services. In determining the privileges that an individual ESM administrator can exercise, some ESM products rely on host I&A services while others implement their own versions. If an ESM product manages some form of password file, that product provides I&A services.

3.1.1 Encryption for Data in Transit

The nature of the data that flows between ESM hosts is such that some of that data has to be encrypted. Because of the importance of this issue and the potential confusion surrounding it, some general remarks are necessary.

Data flowing among ESM hosts may fall into one or more categories:

- Identification and authentication data may be exchanged between ESM servers and clients in order to verify each other's identity. This exchange helps to defeat spoofing attacks in which a counterfeit server might try to assume control over or extract information from a client. Identification and authentication data might also be transmitted when an ESM administrator is using a management client to administer an ESM server from a desktop machine, or when an authorized ESM user is using a reporting client to query the ESM data repository.

- Configuration commands or programs may be transmitted from an ESM server to be executed on a client. A common example of this type of communication is the use of SNMP GET, SET, and TRAP commands. Some of these commands may contain detailed configuration information that is required for the command to be executed.

- Very detailed hardware and software configuration data may be transmitted from ESM clients to servers running ESM configuration management applications. Using this data an attacker could select specific strategies that would be more likely to succeed in exploiting vulnerabilities.

The specific requirements for encrypting data in transit between ESM hosts are stated in the following sections and product-specific appendices of this document. However, the following general guidance provides context for these requirements.

- Authentication data must be encrypted in all cases.

- Configuration command or program data must be encrypted unless that data traverses only controlled-access networks dedicated to network or system management.

- Hardware and software configuration data, such as that collected by ESM inventory applications, must be encrypted when the path of transmission includes public or wireless networks. The data must also be encrypted if it pertains to systems hosting classified data or if the IAO considers the related information systems data to be sensitive.

It is acknowledged that only a subset of some ESM applications or specific implementations may need encryption. However, the application may not provide granular controls that allow selective implementation. That is, there may be only one configuration option for enabling client-to-server data encryption. In these cases, encryption must be enabled in order to ensure that the data for which it is required receives the necessary protection.

3.2 Security Design and Configuration

This section describes ESM security requirements based on applicable DODI 8500.2 IA controls in the Security Design and Configuration subject area. These requirements address three general areas: design characteristics, implementation and configuration, and network access.

3.2.1 Application Design Characteristics

The most effective security characteristics of an application are integrated into its design. In order to ensure objectively that the desired characteristics are present and properly implemented, a formal evaluation and validation process is necessary. The requirements in this section are designed to achieve two goals:

- To ensure that IA and IA-enabled ESM applications have been through the standardized evaluation processes and meet the requirements for products used in DoD information systems

- To ensure that software for which there is no formal review, extension, or repair process is not used unless specific safeguards are employed.

The National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security Systems (CNSS), issued *National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11* to specify evaluation and validation requirements related to the acquisition of IA and IA-enabled IT products. The NSTISSP-11 Fact Sheet is available from the CNSS web site at http://www.nstissc.gov/html/library.html. DODI 8500.2 available at http://www.dtic.mil/whs/directives/corres/html/85002.htm reiterates the requirements. A detailed discussion of the requirements can be found in the *Enclave STIG*.

It must be noted that some of the requirements in this section apply to ESM applications that are classified as IA or IA-enabled products. DODI 8500.2 defines these terms as follows:

- An IA product is a product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data, correct known vulnerabilities, and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks).

- An IA-enabled product is a product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities.

A few ESM applications, such as those that perform provisioning of user identities, are IA products. Most ESM applications are IA-enabled because they provide security services such as controlling the authorization of ESM administrators to perform privileged functions. Both types of products are required to meet the requirements that follow.

- *(EGA.0010: CAT III) The IAM will ensure the acquisition of all IA and IA-enabled Government-Off-the-Shelf (GOTS) ESM products meets the applicable NSA evaluation and validation requirements specified in NSTISSP No. 11 and DODI 8500.2.*

- *(EGA.0020: CAT III) The IAM will ensure the acquisition of all IA and IA-enabled Commercial-Off-the-Shelf (COTS) ESM products meets the applicable Common Criteria, NIAP, or FIPS evaluation and validation requirements specified in NSTISSP No. 11 and DODI 8500.2.*

Specific system configuration data that is collected, transmitted, and stored by ESM applications could be useful to a potential intruder trying to exploit vulnerabilities on the subject systems. To deter this threat, the ESM data needs to be protected at the same confidentiality level as the systems on which that data is based. IA and IA-enabled COTS and GOTS ESM products provide a level of protection through their administrator access controls. In order to ensure that those controls are strong enough for the confidentiality level of the data, the products must meet the appropriate high, medium, or basic robustness levels as defined in DODI 8500.2.

- *(EGA.0030: CAT III) The IAM will ensure all IA and IA-enabled COTS and GOTS ESM products, which manage data from sensitive systems meet the medium robustness requirements defined in DODI 8500.2 when any of the following is true:*

  - *ESM data traverses public networks.*

  - *ESM data resides on systems are accessible by individuals not authorized to access the information.*

Software that is classified as public domain, freeware, or shareware represents a risk to information systems because the Government does not have access to the original source code to review, extend, or repair it when needed. To minimize this risk, specific conditions must be met before software in these classes is used.

- *(EGA.0040: CAT III) The IAM will ensure binary or machine executable public domain software and other software with limited or no warranty (such as those known as freeware or shareware) is not used to fulfill an ESM function unless the following conditions are met:*

  - *The software is necessary for mission accomplishment and there are no alternative IT solutions available.*

  - *The software is assessed for information assurance impacts and approved for use by the DAA.*

It should be noted that this specific restriction does not apply to open source software. It is permissible to use open source software as long as it conforms to the same DoD policies that govern COTS and GOTS software. This includes those requirements relating to IA and IA-enabled components. Specific guidance is found in the DoD Memorandum, *Open Source Software (OSS) in the DoD.*

3.2.2 Application Implementation and Configuration

Even a well-designed application can open or be subject to security vulnerabilities if it is not implemented properly. In this instance, implementation refers to how an application is installed and maintained in the environment as well as the configuration settings for the application. The requirements in this section are designed to ensure that ESM applications are installed and configured in a secure manner and that documented processes are used to maintain that secure configuration.

Some ESM applications perform management functions by having a server transmit and schedule the execution of code on client hosts. When used with appropriate controls such as mutual authentication, this practice is acceptable. However, the use of certain types of mobile code is prohibited as described by the following requirements defined in DODI 8500.2 available at http://www.dtic.mil/whs/directives/corres/html/85002.htm:

- Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO must not be used.

- Category 1 mobile code must be signed with a DoD-approved Public Key Infrastructure (PKI) code-signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

- Category 2 mobile code, which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host), may be used.

- Category 2 mobile code, which does not execute in a constrained environment, may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code signed with a DoD-approved code signing certificate).

- Category 3 mobile code may be used.

The *Enclave STIG* provides a general description of mobile code. DoD Memorandum, *Policy Guidance for Use of Mobile Code Technologies in DoD Information Systems*, provides specific details on the assignments of technologies to individual mobile code categories.

- *(EGA.0050: CAT III) ESM administrators will ensure remote management functions used in ESM operations are in compliance with the mobile code requirements of DODI 8500.2 and the Enclave STIG.*

As documented in other sections of this document, certain types of ESM data require cryptographic protection. Encryption, key exchange, digital signature, and hash algorithms are used in various cryptographic services to provide this protection. Proprietary or less robust commercial algorithms cannot be used because their level of protection may be too weak. Product implementations that have not been appropriately evaluated and validated might not provide the intended protection. The use of NIST-approved implementations ensures the appropriate strength and correct implementation of a cryptographic service.

- *(EGA.0060: CAT II) ESM administrators will ensure ESM software is configured to use FIPS 140-2 approved encryption, key exchange, digital signature, and hash algorithms for data storage and transmission.*

Most ESM applications provide automation of configuration management tasks for ESM clients as a primary function. However, the products are tools that simplify tasks; they cannot perform impact evaluation, scheduling, and strategic direction setting responsibilities that are required for a complete configuration management process. If configuration changes are performed without satisfying these responsibilities, the availability, integrity, and confidentiality of the ESM clients might be compromised.

DODI 8500.2 specifies the implementation of a configuration management process that includes:

- Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;

- A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems;

- A testing process to verify proposed configuration changes prior to implementation in the operational environment; and,

- A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

- *(EGA.0070: CAT III) The IAM will ensure ESM software implements configuration changes are used only in conjunction with a documented configuration management (CM) process.*

ESM applications generally provide functions that ensure continuing and efficient operation of information systems. Applications that provide I&A services may even be part of the operational software required to control access to a system. Because of these operational roles, an inventory of the ESM products being used is essential to adequate configuration management and disaster recovery planning.

- *(EGA.0080: CAT III) The IAM will ensure a current and comprehensive baseline inventory includes all ESM software is maintained by the CCB and as part of the C&A documentation,*

and a copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Because ESM applications typically have the ability to impact the operational condition or monitoring capability for client systems, it is critical to ensure that libraries containing the software elements and configuration controls are protected from malicious or unintentional change. Without proper access controls, negative impacts ranging from denial of service to the introduction of malicious code are possible.

Although it is of less immediate concern for operations, it is also important to ensure that proprietary vendor code and data is protected in accordance with applicable licenses or agreements. For example, use of an application by more than the agreed-upon number of users could expose the Government to additional costs or the loss of rights to use the product.

ESM software often includes one or more programs with the ability to perform privileged functions. These functions may directly impact system availability or the integrity or confidentiality of data on client systems. To prevent unauthorized use, access to the programs providing the privileged functions has to be restricted.

The following requirements ensure that ESM software libraries and configuration files retain their integrity and that access to privileged programs is properly restricted.

- *(EGA.0090: CAT II) The IAO will ensure access to ESM software libraries (including executable and configuration files) is limited:*

  - *Only authorized ESM application processes, ESM administrators, or SAs requiring it, have update access.*

  - *Only authorized ESM application processes, ESM administrators, SAs, or other users that require it and are within applicable license agreements, have read access.*

- *(EGA.0100: CAT II) The IAO will ensure access to ESM software libraries is limited so only authorized ESM application processes, ESM administrators, or SAs can execute privileged programs.*

As with all applications, a coding error may be found in ESM software that results in security vulnerabilities. Policies vary, but if the affected software is no longer supported, the vendor does not provide fixes to address the problem. In addition, the vendor may not even confirm whether a security vulnerability exists in an unsupported release, leaving users without assurance that their configurations are secure.

To address these issues, it is necessary to ensure that only supported software is used. When a vendor announces that support is being discontinued, an upgrade or removal plan must be developed.

- *(EGA.0110: CAT I) The IAO will ensure ESM software is removed or upgraded prior to the vendor dropping support.*

- *(EGA.0120: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading ESM software prior to the date the vendor drops security patch support.*

Many ESM products incorporate data repositories such as those used to store hardware and software inventory data. The ESM product architecture may allow partitioning of the repository management from user interfaces used to display and report the data. In practical terms, this means that programs that display the data execute on one host and the database management system (DBMS) holding the data can reside on a different host. This type of architecture can provide security benefits in two ways. It provides a more controlled access path to the data and it allows for further restrictions of access to the platform on which the data resides.

The *Database STIG* recommends that any DBMS be installed on a host system dedicated to its support. By separating the DBMS server, access to that platform can be more finely controlled, resulting in reduced exposure to vulnerabilities in the DBMS software. DODI 8500.2 requires a physical or logical separation of user interface services from data storage and management services.

- *(EGA.0130: CAT III) ESM administrators will ensure ESM components are implemented to logically or physically separate the user interface elements from data storage and management elements.*

It is recognized that some products and environments do not support this type of partitioning. These cases are addressed through product-specific guidance in this document.

For the ESM products that provide specific IA functions, a special requirement exists to isolate the security support structure. Products such as those that perform provisioning of user identities or enterprise resource access control require special attention due to the potential impact of compromises of the integrity or availability of the security services.

Isolation of the security support structure is best provided through the use of separate partitions or domains that allow control of access to, and integrity of, the hardware, software, and firmware used. In operational terms this can mean dedicated hosts for ESM IA applications. However, this requirement applies only where the nature or architecture of a specific application supports it.

- *(EGA.0140: CAT II) ESM administrators and IAOs will ensure ESM hardware and software components that perform security functions, including but not limited to user account administration and resource access control, are isolated by logical or physical means.*

3.2.3 Network Access

The use of networks is inherent to ESM applications in their performance of remote monitoring, reporting, and configuration functions. Unfortunately, the design of some older applications was

based on the assumption that data transmission would occur over closely controlled or closed networks with minimal security exposure. This design assumption has led to serious security issues when applied to current networks, especially those with higher levels of interconnection and associated risk.

The requirements in this section are intended to ensure that the combination of ports, protocols, and services (PPS) used by ESM applications is consistent with secure practices identified in DoD network security guidance, including *DOD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM)* and the associated *Ports, Protocols, and Services (PPS) Assurance Category Assignments List.* The *PPS Assurance Category Assignments List* provides detailed guidance for specific services and port numbers. The following are extracts of the PPS usage principles from the PPSM instruction:

- PPS are assessed for vulnerabilities and assigned to one of three assurance categories: RED, YELLOW, or GREEN.

- PPS designated as RED has a low level of assurance. These PPS implemented in applications expose DoD networks to an unacceptable level of risk for routine use. A RED PPS will only be allowed when approved by the DISN DAAs for a specific DoD information system under defined conditions and restrictions and if no suitable alternative exists.

- PPS designated as YELLOW have a medium level of assurance. These PPS expose DoD networks to an acceptable level of risk for routine use only when implemented with the required mitigation strategy and approved by the DISN DAAs for a specific DoD information system.

- PPS designated as GREEN have a high level of assurance. These PPS are considered best security practices and are recommended for use when implemented with the required mitigation strategy and approved by the DISN DAAs for a specific DoD information system.

- *(EGA.0150: CAT II) The IAO will ensure ESM use of specific network PPS conforms to the requirements of the DoD PPSM instruction and the PPS Assurance Category Assignments List.*

- *(EGA.0160: CAT III) If an ESM application traverses a DoD enclave boundary, the ESM administrators will ensure the ESM application is registered through the designated DoD Component POC as defined by the PPS homepage at* http://iase.disa.mil/ports/index.html

Although some COTS ESM products do not conform to the specified PPS restrictions, there are some potential mitigating implementations:

- The requirements apply unconditionally to ESM implementations that traverse enclave boundaries. However, for implementations in which network traffic is contained within a

DoD Component enclave (e.g., does not traverse a backbone network such as the NIPRNET), the requirements are reduced to strong recommendations.

- The requirements also drop to the level of strong recommendations where ESM products are deployed in a closed network such as the DISA Computing Services Out-of-Band (OOB) network. Such a network would have to be equipped with appropriate security controls to limit protocol access to management servers and clients and authenticated Virtual Private Networks (VPN).

The product specific sections of this document provide requirements for individual applications, but there is one additional issue to note. Some ESM applications may provide for remote installation using PPS that are normally not permitted. It is strongly recommended that products with this design be installed locally rather than remotely. However, the use of a coordinated installation window that uses the restricted PPS for a period of a few hours is not prohibited by this document as long as the traffic can be restricted to the network addresses of the source and target hosts.

3.3 Identification and Authentication

This section describes ESM security requirements based on applicable DODI 8500.2 IA controls in the Identification and Authentication subject area. These requirements address items that are used to identify and authenticate a user and as input to encryption processes. These items include account IDs, PKI certificates, authenticators such as passwords, and symmetric and asymmetric keys.

The concept of I&A services was defined earlier, but deserves a note here. An I&A service establishes a user's identity and verifies that the requesting user is correctly associated with that identity. Because of the sensitive nature of this service, some of the requirements stated here apply specifically to ESM applications that provide that service.

A final general note on I&A services involves the choice where multiple options exist. Some products allow a choice between using host or application-based I&A services. A single point of security control is generally better because it simplifies account maintenance and auditing, and it provides an integrated point for assigning privileges. Therefore, when the option exists and there are no significant security advantages to the contrary, host I&A services should be implemented instead of the equivalent application services.

3.3.1 Individual Identification

The concept of individual identification is basic to access control decisions and to auditing. With the possible exception of data or systems that are assigned a confidentiality level of public, individual identification is always necessary. Although in some cases it is acceptable to make access control decisions at a group level, meaningful auditing always requires individual identification.

In almost every case, ESM administrator accounts have access to sensitive data and privileged functions. If this access is not sufficiently controlled, the confidentiality, integrity, and

availability attributes of one, many, or all of the hosts executing components of an ESM application could be compromised. If access to sensitive data or a privileged function cannot be attributed to a specific user, it may be impossible to determine the source of a compromise or attack. An individual identifier, along with an associated authenticator, provides access control and audit capability.

- *(EGB.0010: CAT II) The IAO will ensure each ESM user account is associated with an individual identifier, such as a unique token or user login ID, and a password.*

Although user IDs and passwords may currently be the most common form of identification and authentication, newer technologies with greater strength are being widely implemented. The DoD Class 3 and Class 4 PKI implementations are a strategic option for positive authentication for access to information systems. While it is recognized that older ESM applications may not be PKI-capable, all new acquisitions and upgrades should incorporate PKI technologies that are compatible with the DoD PKI or other technologies implemented through an NSA-certified product.

- *(EGB.0020: CAT III) If an ESM application provides internal I&A services, the IAO will ensure I&A is accomplished using a DoD PKI Class 3 or 4 certificate and hardware security token (when available), or an NSA-certified product.*

A group authenticator is any mechanism for authentication, shared by members of a group. A common example of the use of a group authenticator is referred to as a group ID; it allows access to systems or data by all the members of the group who have access to (i.e., knowledge of) a single password. Using a group authenticator definitely provides ease of use. However, if used alone, it also eliminates the ability to attribute a specific action to a unique individual and therefore significantly reduces the value of audit data.

Some group authenticators are inherently less secure because it is more difficult to control them. In the example of a shared password, one authorized user can easily disclose the password to additional, unauthorized users and thus reduce or eliminate the security value of the password. Authenticators such as hardware tokens are more secure because they are not, if correctly implemented, easily shared or duplicated.

To diminish the problems with group authenticators, while still taking advantage of their benefits, some mitigating controls are needed. By requiring that an individual authenticator also be used as part of processes that use a group authenticator, it can become possible to track actions back to an individual user. By ensuring that group authenticators are based on an implementation that has been reviewed and determined to be sufficiently robust, it is possible to have an adequate level of trust in their security.

- *(EGB.0030: CAT II) If an ESM application provides internal I&A services, the IAO will ensure ESM group authenticators are used only in conjunction with an individual authenticator.*

- *(EGB.0040: CAT II) If an ESM application provides internal I&A services, the IAO will maintain documentation verifying that any definition of group authenticators not based on the DoD PKI is explicitly approved by the DAA.*

3.3.2 Authenticator Strength and Protection

Authenticators are the means for proof of identity. If an authenticator is compromised, access control over the resources available to the associated user account is lost. Therefore authenticators must be strong enough to resist circumvention and must be protected from unauthorized disclosure.

Passwords are the most common form of authenticator. The chief means to strengthen passwords is by controlling their composition, expiration interval, and change options. Requiring that passwords are composed of multiple character types and that they are changed regularly helps to deter attacks based on simple guessing, dictionary, or brute force techniques. DODI 8500.2 IA control IAIA includes password requirements. Additional authentication requirements pertaining to passwords are located in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND).* These requirements are implemented through the following guidance.

- *(EGB.0050: CAT II) If an ESM application provides internal I&A services and passwords are used, the IAO will ensure the ESM application is configured to the extent system capabilities permit to enforce the following password composition, automatic expiration, and reuse requirements:*

  - *Passwords are at least eight characters long.*
  - *Passwords are composed of a case sensitive mix including at least one upper case letter, lower case letter, number, and special character.*
  - *Passwords are not the same as the associated ID.*
  - *At least four characters are changed when a new password is created.*
  - *Passwords cannot be changed more than once in any 24-hour period without the intervention of the IAO.*
  - *Passwords expire automatically at least every 90 days.*
  - *The last 10 passwords are not reused.*

The following additional guidance should be implemented where resources require more robust protection:

- Passwords are 12 to 16 characters long.
- Repeating characters are not used.
- Passwords do not include dictionary words, names, dates, or phone numbers.
- Passwords for privileged users expire automatically at least every 30 days.

The strength of an authenticator becomes largely irrelevant if unauthorized users or processes are able to extract it from a file or intercept it as it traverses a network. For that reason it is essential to protect authentication data both at rest and in transit. In addition to any physical means of

protection such as partitioning, encryption services are needed to adequately protect authentication data.

- *(EGB.0060: CAT I) If an ESM application provides internal I&A services, the IAO will ensure the ESM password repository is encrypted.*

- *(EGB.0070: CAT II) The IAO will ensure the transmission of authentication data for access to ESM applications is encrypted.*

In addition to the mechanisms enforced by the ESM application, there are some procedural requirements that enhance the protection of authenticators. The first is meant to ensure that authenticators stay exclusive to the rightful owner.

- *(EGB.0080: CAT II) The IAO and ESM administrators will ensure authenticators (e.g., passwords) for ESM accounts are not shared, are not embedded in access scripts, and are not stored on function keys.*

The other procedural requirement is related to software implementation. For simplicity, some vendors provide installation procedures that include or specify the use of particular IDs and passwords. These are referred to as the factory set, default, or standard values. While there are some cases where deviating from the specified values renders an application inoperable or enormously increases the installation complexity, most vendors allow the password or both the ID and password to be chosen by the installer. While the security vulnerability of using default values may seem obvious, this is a common security problem. If not eliminated for an ESM application, this vulnerability might allow anyone with knowledge of the vendor documentation to have privileged access to a system. When performed at the appropriate time in the implementation cycle, eliminating this vulnerability is usually easy and the benefit is significant.

- *(EGB.0090: CAT III) The IAO will ensure all factory set, default, or standard user IDs and passwords for the ESM application are removed or changed.*

It is important to note that software maintenance might install new factory set, default, or standard values as well as re-introduce original ones. Therefore, it is essential to review vendor documentation carefully and check for compliance with this requirement when maintenance is applied.

3.3.3 Key Management

Various cryptographic operations use keys as input to their algorithms. Since knowledge of some key data can effectively negate the security value of encryption, hash, and digital signing operations, the importance of secure key management is clear.

The use of keys in ESM applications can include symmetric, asymmetric, or both key types. Symmetric keys, also called secret keys, have to be shared among the entities using them. Due to this characteristic, symmetric key lengths must be more carefully selected and all the key data securely managed. Asymmetric keys involve a private and public key pair and are the basis for

Public Key cryptography. Although the public key portion of the key pair can be disclosed, the corresponding private key data must be securely managed.

A Key Management Infrastructure (KMI) is used to manage both symmetric and asymmetric key types. DODI 8500.2 defines KMI services. "The KMI provides a common unified process for the secure creation, distribution, and management of cryptographic products, such as asymmetric keys (e.g., PKI) and traditional symmetric keys (e.g., Electronic Key Management System (EKMS)) that enable security services for DoD information systems."

Secure key management for ESM applications is achieved by conforming to the policies and procedures implemented through the NSA-managed DoD KMI. This currently includes symmetric key management provided by EKMS and asymmetric key management provided by the DoD PKI.

- *(EGB.0100: CAT III) If an ESM application utilizes symmetric keys, the IAO will ensure those keys are produced, controlled, and distributed using NSA-approved key management technology and processes.*

- *(EGB.0110: CAT III) If an ESM application utilizes asymmetric keys, the IAO will ensure those keys are produced, controlled, and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens protect the user's private key.*

- *(EGB.0120: CAT I) If an ESM application utilizes symmetric or asymmetric keys on a system processing classified information, the IAO will ensure those keys are produced, controlled, and distributed using NSA-approved key management technology and processes.*

3.4 Enclave and Computing Environment

This section describes ESM security requirements based on applicable DODI 8500.2 IA controls in the Enclave and Computing Environment subject area. These requirements address five general areas: data protection, user account management, application customization, auditing, and network access.

3.4.1 Data Protection

ESM applications may capture or create a variety of data including current availability and event data; historical availability, performance, and accounting data; and hardware and software configuration data. This data is a significant asset for several reasons:

- Current availability and event data represent the operational status of one or more information systems. The information may be used as the basis for reallocating resources or for corrective action.

- Historical data provides usage information for short and long term resource planning, cost allocation, and forensic investigations.

- Hardware and software configuration data are used for asset inventory and deployment activities.

It is noted earlier that ESM application data needs to be protected at the same confidentiality level as the systems on which that data is based. This reflects the fact that unauthorized access to this data might have several negative effects:

- Invalid data, used as the basis for configuration changes or corrective action, could result in a loss of availability.

- Specific configuration data might expose a subject system to specific attacks based on known vulnerabilities.

- The loss of logging data for ESM actions could make it impossible to identify the source of malicious activity.

The following requirements ensure that access to ESM data is appropriately restricted and that access is recorded for subsequent review if needed.

- *(EGC.0010: CAT II) The IAO will ensure access to data created by ESM applications is limited so only authorized ESM application processes and users can read or update it.*

- *(EGC.0020: CAT II) ESM administrators will ensure ESM actions that access or change data are logged and that the logs are reviewed at least weekly or immediately upon system security events.*

It should be noted that the requirement for data access and change logging can be satisfied using OS facilities as well as ESM application functions.

ESM data can itself be sensitive or classified if it includes specific hardware or software configuration data for systems processing sensitive or classified data. As this data traverses networks, it must be protected from disclosure according to its confidentiality level and in accordance with need-to-know requirements. In this case protection is mandated in the form of data encryption.

- *(EGC.0030: CAT II) ESM administrators will ensure ESM data that includes unclassified, sensitive information (including system hardware or software configuration data) traverses a commercial or wireless network is encrypted, at a minimum, using NIST-certified cryptography.*

- *(EGC.0040: CAT I) ESM administrators will ensure ESM data that includes classified systems' hardware or software configuration data traverses a network cleared to a lower level than the ESM data is encrypted using NSA-approved cryptography.*

3.4.2 User Account Management

User accounts defined for access to ESM applications grant privileges that allow various interactions with the systems running the applications. These interactions can be relatively benign, such as access to availability information, or quite powerful, such as reconfiguration or even restart of multiple systems. Span of control is also a factor. Some ESM account privileges are intended to allow an end user to perform maintenance only on their own system. While this can be cost effective, it must be defined carefully so that privileges over other systems are not granted unintentionally. It is important that privileged accounts are used only when required in order to closely document and control the use of privileges.

Access controls over ESM programs and data are directly related to privileges granted through ESM account definitions. The controls provide little protection if the practices used for account management are weak. In large organizations, careful account management can be a significant administrative burden. One mechanism for dealing with that burden is the use of role based access controls in applications that support it. This helps to control privileges according to a user's functional need for them and should simplify account maintenance.

The following requirements enforce the principles of least privilege and separation of duties for ESM accounts. This means that privileges are not granted unless necessary and not used unless intended. The requirement to use role based access control, where feasible, helps to reduce the complexity and potential errors associated with privileged account maintenance.

- *(EGC.0050: CAT II) The IAO will ensure ESM administrator accounts are assigned the minimum privileges required for the user's job function.*

- *(EGC.0060: CAT III) The IAO will ensure ESM administrator accounts are not used for non-privileged functions.*

- *(EGC.0070: CAT III) The IAO will ensure ESM administrator accounts are established and administered in accordance with a role-based access scheme to the maximum extent technically feasible within the ESM software.*

Errors or omissions in account management may be the result of process problems. Processes that are documented and implemented are helpful in avoiding problems that could weaken security over ESM accounts. Formal documentation of privilege assignment is an essential part of the management process.

- *(EGC.0080: CAT II) The IAM will ensure a process is documented and implemented for the management of ESM accounts.*

- *(EGC.0090: CAT II) The IAM will maintain documentation of the assignment of ESM accounts and roles.*

The account management process must incorporate manual or automated steps to handle situations that would otherwise allow continued privileged access after it is no longer authorized.

The following requirements provide for disabling and deleting accounts that are no longer needed.

- *(EGC.0100: CAT II) The IAO will ensure the account management process applicable to ESM accounts includes manual or automated procedures to enforce the following for inactive, suspended, and terminated accounts:*

  - *Accounts for which unauthorized activity is identified are disabled immediately.*
  - *Accounts to be terminated due to user re-assignment or departure are disabled or deleted within two days of notification by the user or user's supervisor.*
  - *Accounts inactive for more than 35 days are disabled.*
  - *Accounts disabled for more than 180 days are deleted.*

3.4.3 Application Customization

It is sometimes necessary to customize COTS or GOTS applications to get functions to work properly or efficiently in a specific environment. Customizations may be in the form of changes to existing programs or the addition of new programs.

Because ESM applications often run as privileged processes on many systems, invalid or malicious changes to those applications have the potential to cause significant problems over an extended area. The installation and propagation of improperly modified ESM programs could cause serious compromises of confidentiality, integrity, and availability to a single site or an entire enclave.

Part of the defense against such compromises is the use of a formal configuration management process. Such a process includes review and approval of change requests and controls to allow only authorized personnel to implement changes. In this way, ESM application changes are adequately reviewed before implementation and the changes are not implemented without the explicit knowledge and consent of the appropriate parties.

- *(EGC.0110: CAT III) If an ESM application is altered by the addition of locally written programs or changes to COTS or GOTS programs, and if those added or changed programs are executed during ESM operation by a privileged process or user, the IAO will ensure a documented configuration management (CM) process exists for the implementation of those added or changed programs.*

3.4.4 Auditing

Auditing for information systems involves the collection and retention of data so that it is possible to assess the adequacy of system controls and the degree of compliance with policies and procedures. Audit data provides information needed to evaluate the source, scope, and impact of a security incident.

As with other areas of concern, auditing for ESM applications has additional significance because the applications often execute as privileged processes. Certain user actions, performed within a limited time period and in certain patterns, can be signs of preparation or attempts to

exploit system vulnerabilities that involve privileged access. These actions include attempts to access security files and attempts to access an interactive application. Certain actions taken by an application, in response to a perceived threat, are also potential signs of an attack. These actions include denying access due to successive invalid password entries; disabling IDs, network ports, or other access mechanisms; or otherwise flagging actions that appear to be malicious.

Taken individually, these events are not absolute indicators and any response to them could be premature. However, if the execution of the actions is not recorded, it becomes impossible to recognize later the pattern that confirms the occurrence of an attack. Therefore, it is necessary to capture this information as the events occur.

- *(EGC.0120: CAT II) To the extent technically feasible from and applicable to the ESM application, the IAO will ensure audit data containing user ID, date and time of event, type of event, and success or failure of event are written for the following:*

  - *Successful and unsuccessful attempts to access security (e.g., account or permission) files*
  - *Successful and unsuccessful logon to (attempt to access) the application*
  - *Denial of access resulting from excessive number of logon attempts*
  - *Blocking or blacklisting a user ID, terminal, or access port, and the reason*
  - *Activities that might modify, bypass, or negate safeguards controlled by the application.*

As mentioned, it may take a collection of data over time to recognize an attack. Because the time span of an attack can be lengthy, some period of data retention has to be selected. Also, because investigations can take extended periods of time, it is necessary to be sure that important evidence is not inadvertently lost.

- *(EGC.0130: CAT II) The IAO will ensure audit data generated by an ESM application is retained for at least one year.*

Some ESM applications offer built-in facilities for the collection and reporting of audit data, or even for generating warnings based on the data. While such features may not appear to be immediately important from an operational view, waiting until malicious activity is suspected to deploy the features can mean that the data is lost or is not processed in time to detect an attack in progress. An ESM application might also have the ability to take defensive action such as disabling user access. Deploying these product capabilities early ensures that they will be available when needed.

- *(EGC.0140: CAT II) ESM administrators will deploy tools that provide audit data review and report capabilities.*

- *(EGC.0150: CAT II) To the extent technically feasible from and applicable to ESM applications, ESM administrators will ensure an automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications and with a*

user configurable capability to automatically disable the application if serious IA violations are detected.

A primary benefit of collecting audit data is lost if the data is only reviewed when a security incident has been confirmed. A proactive approach to reviewing the data on a regular basis is important for early detection and for prevention of attacks.

- *(EGC.0160: CAT II) The IAO will ensure audit data generated by ESM applications are reviewed at least weekly for indications of inappropriate or unusual activity and suspected IA policy violations are analyzed and reported.*

Protecting audit data requires safe physical storage and appropriate access control. To accomplish this, the data is backed up and access control definitions are implemented to limit updates to the original and backup copies. The destruction of audit data due to media failures or the absence of update access controls represents a double loss. The ability to recognize and possibly recover ESM data that was tampered with is lost and the system resources expended to collect, process, and store the data are effectively lost.

- *(EGC.0170: CAT II) The IAO will ensure ESM audit data is backed up not less than weekly onto a different system or media than the system on which the ESM application executes.*

- *(EGC.0180: CAT II) The IAO will ensure access to ESM audit data, including backup copies, is limited so only authorized ESM application processes, ESM administrators, or SAs can read, update, or delete it.*

3.4.5 Network Access

It was noted earlier that the use of networks is inherent to ESM applications. The requirements in this section are designed to protect three aspects of network access for ESM applications:

- ESM administrators and other ESM users may access ESM servers under the control of I&A services provided by an ESM application. As noted in *Section 3.1, Introduction*, these services establish and verify the identity of the user or process.

- ESM servers are necessarily part of a network that connects many hosts. The presence of a network connection on any application host warrants protective measures.

- In one form or another, virtually all ESM data transits a network. The nature of this data and the possible impact of corruption or interception indicate a need for supplementary integrity controls.

I&A services provided by ESM applications must include protective controls equivalent to other providers (such as operating systems) of those services. These controls address repeated logon attempts, concurrent sessions, and notification of privacy and security conditions. If the controls are not implemented, the system is more vulnerable to password attacks, continuing use of compromised accounts, and the loss of the right to use audit data.

- *(EGC.0190: CAT II) If an ESM application provides internal I&A services, ESM administrators will ensure successive logon attempts are controlled using one or more of the following:*

  - *Access is denied after multiple unsuccessful logon attempts.*
  - *The number of access attempts in a given period is limited.*
  - *A time delay control system is employed.*

- *(EGC.0200: CAT II) If an ESM application provides internal I&A services and it supports multiple logon sessions for each user ID, ESM administrators will ensure a session maximum is defined.*

The requirement for a warning banner is essential because it preserves the Government's right to monitor, record, and audit session activities. If this requirement is not fulfilled, data that is collected may have to be excluded from any prosecution of an intruder.

- *(EGC.0210: CAT III) The IAO will ensure access to an ESM application includes the presentation of a warning banner from the ESM host. The banner will consist of statements that advise the user of the following elements:*

  - *The system is a DoD system.*
  - *The system is subject to monitoring.*
  - *Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.*
  - *Use of the system constitutes consent to monitoring.*
  - *The system is for authorized U.S. Government use only.*

An example of an acceptable warning banner can be found in the *Network Infrastructure STIG*. Questions concerning the legal validity of specific text should be addressed to the DoD Component's General Counsel.

It should be noted that the requirement for a warning banner may be satisfied using OS facilities on the ESM host as well as ESM application functions.

Although technically possible, the use of ESM applications on systems operating at different classification levels is not permitted. The use of ESM applications on systems connected by non-DoD networks or on a mix of DoD and non-DoD systems is also not permitted. Those configurations would require a controlled interface and it has not been determined that such a configuration for ESM applications could be adequately secured. The primary issue with those configurations would be the lack of ability to segregate the ESM data to the level of assurance required.

- *(EGC.0220: CAT II) The IAO and ESM administrators will ensure ESM applications are not implemented across DoD information systems operating at different classification levels or across mixed DoD and non-DoD systems or networks.*

The sensitive nature of ESM applications and data necessitate increased protection for the ESM application hosts. One tool to accomplish this is a host-based intrusion detection system (HIDS). A discussion of HIDS functions can be found in the *Enclave STIG*. The requirements in this document for encryption of ESM data traversing a network are a primary driver to the need for a HIDS on ESM servers.

- *(EGC.0230: CAT II) The IAO will ensure ESM application hosts are protected by a HIDS.*

There are a number of problems that can be introduced when applications depend on the transfer of data across networks. Some of these are:

- Data traversing any network may be subject to corruption from hardware problems.
- Deliberate tampering during transmission might corrupt data.
- If a host's network identity is spoofed, counterfeit data might be introduced into the transmission and corrupt data on the receiving host.

Integrity checking and host authentication mechanisms help to combat data corruption. Integrity checking mechanisms can operate at the file level and at the message level. Host authentication can occur at the session or message level.

Some ESM applications that transmit data incorporate hash checking or similar integrity checks at the file level. An entire file on the sending host is passed through a hash algorithm and the hash value is sent with the file. On the receiving host, the file is passed through the same algorithm and the receiver's hash value is compared with the sender's. If the values do not match, an error is recorded and the file is retransmitted. Hash checking or similar integrity mechanisms that are applied to entire files are embedded features of the ESM application.

Integrity checking at the message level and host authentication are frequently related to network sessions. One common implementation is the use of the Secure Sockets Layer (SSL) or a follow-on protocol. Session protocols like SSL offer hash checking as messages are exchanged to validate the contents of each message. Host authentication occurs at session startup and periodically thereafter. By requiring both the server and client to authenticate each other, the data source is established with higher assurance than simple network address validation. The use of session protocols requires some integration by the ESM vendor, but offers a standards-based solution that can be implemented using elements of the DoD PKI.

Another common way for ESM applications to implement data integrity and host authentication would be the use of components that adhere to the SNMP version 3 (SNMPv3) User-based Security Model (USM). This standard is documented in RFC 3414. The SNMPv3 USM specification requires the implementation of an authentication protocol that is responsible for data integrity and data origin authentication. The *Network Infrastructure STIG* requires network management tools using SNMP to implement the SNMPv3 Security Model.

ESM applications may provide varying options for ensuring data integrity over a network. The requirements here are intended to enforce the implementation of those options in the ESM products that have these capabilities.

- *(EGC.0240: CAT II) ESM administrators will ensure ESM applications are configured to use integrity mechanisms such as parity checks, cyclic redundancy checks, or hash checks to ensure the integrity of transmitted data.*

- *(EGC.0250: CAT II) ESM administrators will ensure ESM applications are configured to assure session integrity and to detect or prevent session hijacking through the use of mutual (both server and client) authentication mechanisms such as those available through SSL and successor protocols.*

3.5 Enclave Boundary Defense

This section describes ESM security requirements based on applicable DODI 8500.2 IA controls in the Enclave Boundary Defense subject area. These requirements address remote access to ESM applications. For the purposes of this document, remote access is described as any access to an ESM application from a host outside of the enclave in which the ESM application host resides.

All remote access to DoD information systems, including privileged and unprivileged, requires a restricted access path that includes encryption and strong authentication. The following requirements address those security measures for any remote ESM application access.

- *(EGD.0010: CAT II) The IAO will ensure remote access to ESM applications is secured through the following:*

    - *Use of a managed access control point such as a remote access server in a DMZ*
    - *Session encryption using, according to the data classification, NIST-certified or NSA-approved cryptography*
    - *Strong user authentication resists spoofing, such as a two-factor system.*

ESM applications enable privileged functions and provide access to data that is likely to be sensitive, and may be classified. Therefore, in practically all cases, ESM administrators are identified as privileged users. A discussion of privileged user remote access can be found in the *Enclave STIG*. Because of the potential for serious impact from the compromise of privileged access, additional security for sessions and special attention to auditing to those sessions is necessary.

The following requirements address the need to protect remote ESM administrator access and to review use of that access because it represents remote user privileged access.

- *(EGD.0020: CAT II) The IAO will ensure remote access for ESM administrators uses:*

  - *Session security measures such as a VPN configured in blocking mode to discard all but authorized traffic*
  - *A process, which creates an audit log for each remote session.*

- *(EGD.0030: CAT II) The IAM/IAO will review the audit log for every remote session of an ESM administrator.*

While VPN implementations do provide desirable session protection, they can also be used to conceal malicious traffic. A network-based intrusion detection system (IDS) is a tool to address this risk. A discussion of network IDS functions can be found in the *Enclave STIG*. The requirement in this document enforces the specific need for remote ESM administrative traffic that uses a VPN to be examined for intrusive behavior.

- *(EGD.0040: CAT II) The IAO will ensure VPN traffic for remote ESM administrator sessions is visible to a network intrusion detection system (IDS).*

3.6 Physical and Environmental

This section describes ESM security requirements based on applicable DODI 8500.2 IA controls in the Physical and Environmental subject area. These requirements address a specific need for the physical security of ESM application hosts.

Some ESM applications perform functions that monitor or reconfigure the operational status of other information systems. It has also been noted that some ESM applications perform privileged functions. If the availability or integrity of the ESM application is negatively impacted, many or all of the other information systems may also be negatively impacted. Tampering with the physical configuration or environment of the host system is a simple way to cause availability and integrity issues for ESM applications.

Though all application hosts require physical access controls, the operational role, privileged functions, and potential far-reaching impact of problems with ESM applications establish a greater need to provide appropriate physical security for the ESM host servers.

- *(EGE.0010: CAT II) The IAO will ensure physical access to ESM application hosts is restricted to specifically authorized personnel.*

It is expected that the physical access controls for ESM hosts will be of a more robust nature than those that might be used for less critical resources such as local file and print servers. This could be implemented by more restricted physical isolation or other measures. The specific nature of this robustness is at the discretion of the responsible IAO.

3.7 Continuity

This section describes ESM security requirements based on applicable DODI 8500.2 IA controls in the Continuity subject area. These requirements address the need for steps that will enable recovery of ESM application functions when some event causes the primary processing resources to be damaged or lost.

The need for a recovery capability is driven by the fact that some ESM applications provide information assurance functions (such as I&A services and security patch management) or monitoring and reconfiguration functions that are required to maintain operational status. Their loss would degrade or seriously reduce overall capability to meet mission objectives.

The following requirements are related to the need for specific attention to ESM applications in disaster recovery planning. The objective is to see that ESM applications that provide a business or mission essential function to an environment are not overlooked.

- *(EGF.0010: CAT II) The IAM will ensure the disaster recovery plan for the enclave includes appropriate provision for the continuity of ESM applications that provide I&A services, other essential information assurance functions such as security patch management, or other services required to monitor or maintain operational status.*

  - *For ESM applications serving MAC III systems, resumption within five days of activation.*
  - *For ESM applications serving MAC II systems, resumption within 24 hours of activation.*
  - *For ESM applications serving MAC I systems, transfer to an alternate site for the duration of an event with little or no loss of operational continuity.*

- *(EGF.0020: CAT II) The IAM will ensure ESM applications that provide I&A services, other essential information assurance functions such as security patch management, or other services required to monitor or maintain operational status are identified for priority restoration planning.*

***NOTE*:** Separate plans for ESM applications are not required. On the contrary, the best implementation would be an integrated plan for the enclave that included ESM and other essential applications.

In addition to facilities and hardware required for recovery, it is necessary to have copies of the data and software used by ESM applications. The following requirements specify what is necessary, while recognizing that different recovery capabilities are needed for ESM services for systems with different availability requirements.

- *(EGF.0030: CAT II) The IAO will ensure ESM application data is managed appropriately to the MAC of the systems served by the ESM application.*

  - *For ESM applications serving MAC III systems, ESM data is backed up at least weekly.*

- *For ESM applications serving MAC II systems, ESM data is backed up daily and the recovery media is stored at an off-site location that affords protection in accordance with the mission assurance category and confidentiality level of the data.*
- *For ESM applications serving MAC I systems, ESM data is backed up by maintenance of a redundant secondary system, not collocated, and can be activated without loss of data or disruption to the operation.*

- *(EGF.0040: CAT II) The IAO will ensure backup copies of software for ESM applications that provide I&A services, other essential information assurance functions such as security patch management, or other services required to monitor or maintain operational status are stored in a fire-rated container or otherwise not collocated with the operational software.*

3.8 Vulnerability and Incident Management

This section describes the ESM security requirements based on applicable DODI 8500.2 IA controls in the Vulnerability and Incident Management subject area. These requirements address the need to adopt and implement a process to mitigate hardware and software vulnerabilities as they are identified.

It appears that no vendor's products are immune from the identification and exploit of vulnerabilities. Many vulnerabilities have been linked to deficient programming and, although those issues have received a lot of attention, serious problems are still discovered. The proliferation of vulnerability and exploit information on the Internet exacerbates these problems by making the information widely and easily accessible. Unfortunately, mitigating action is often not taken, even when a fix has been identified and made available. These facts indicate the necessity for a process to make sure that efficient and rapid mitigating action is taken.

An effective vulnerability management process includes the elements needed to identify and take mitigating action for vulnerabilities. Automated assessment tools can speed identification. An ESM configuration management application can enable rapid deployment of mitigating actions. When these or equivalent manual procedures are part of an enclave's documented work processes, successful vulnerability management is much more likely.

To make certain that vulnerabilities are addressed, a formal commitment to security patch implementation is essential. It is not necessary to have a unique policy for ESM resources, only to have a policy that covers ESM resources. Manual or automated documentation indicating that patches have been applied provides auditable evidence that mitigating action has been taken.

- *(EGG.0010: CAT II) The IAM will ensure a vulnerability management process encompasses ESM applications and server hardware is documented and implemented.*

- *(EGG.0020: CAT II) The IAO will ensure all security related patches to ESM applications are applied and that completion is documented for each applicable asset.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government Publications:

Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01, “Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND),” 25 March 2003

Committee on National Security Systems (CNSS) Instruction No. 4009, “National Information Assurance (IA) Glossary,” May 2003

Committee on National Security Systems (CNSS), “National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11,” July 2003

Department of Defense Directive 8500.1, “Information Assurance (IA),” 24 October 2002

Department of Defense Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” 30 December 1997

Department of Defense Instruction 8500.2, “Information Assurance (IA) Implementation,” 6 February 2003

Department of Defense Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling", 1 April 2004

Department of Defense Instruction 8551.1, “Ports, Protocols, and Services Management (PPSM),” 13 August 2004

Department of Defense Memorandum, “Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA),” 30 December 1999

Department of Defense Memorandum, “Open Source Software (OSS) in the Department of Defense (DoD)”, 28 May 2003

Department of Defense Memorandum, “Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems,” 7 November 2000

Defense Information Systems Agency (DISA), “Database Security Technical Implementation Guide,” Version 6, Release 1, 7 July 2003

Defense Information Systems Agency (DISA), “Enclave Security Technical Implementation Guide,” Version 2 Release 1, 1 July 2004

Defense Information Systems Agency (DISA), “Network Infrastructure Security Technical Implementation Guide,” Version 5, Release 2, 29 September 2003

Defense Information Systems Agency (DISA), “OS/390 Security Technical Implementation Guide,” Version 4, Release 1, 4 August 2003

Defense Information Systems Agency (DISA), "UNIX Security Technical Implementation Guide," Version 4, Release 4, 15 September 2003

Defense Information Systems Agency (DISA), "Web Server Security Technical Implementation Guide," Version 4, Release 1, 29 August 2003

Defense Information Systems Agency (DISA), "Windows NT/2000/XP Addendum," Version 4, Release 1, 26 February 2004

National Security Agency, "Information Assurance Technical Framework (IATF)," Release 3.1, September 2002

Vendor Publications:

International Business Machines, "Tivoli Business Systems Manager Administrator's Guide," Version 2.1.1, with Fix Packs 1-10 GC32-0799-01

International Business Machines, "Tivoli Business Systems Manager Getting Started," Version 2.1.1, with Fix Packs 1-10, GC32-0801-01

International Business Machines, "Tivoli Business Systems Manager Installation and Configuration Guide," Version 2.1.1, Re-released with Fix Packs 1–10 GC32-0800-02

International Business Machines, "Tivoli Business Systems Manager Release Notes," Version 2.1.1, SC23-4841-01

International Business Machines, "Tivoli Enterprise Console Adapters Guide," Version 3.9, SC32-1242-00

International Business Machines, "Tivoli Enterprise Console Command and Task Reference," Version 3.9, SC32-1232-00

International Business Machines, "Tivoli Enterprise Console Installation Guide," Version 3.9, SC32-1233-00

International Business Machines, "Tivoli Enterprise Console Release Notes," Version 3.9, SC32-1238-00

International Business Machines, "Tivoli Enterprise Console Rule Developer's Guide," Version 3.9, SC32-1234-00

International Business Machines, "Tivoli Enterprise Console Rule Set Reference," SC32-1282-00

International Business Machines, "Tivoli Enterprise Console User's Guide," Version 3.9, SC32-1235-00

International Business Machines, “Tivoli Monitoring for Business Integration Installation and Setup Guide,” Version 5.1.1 SC32-1402-00

International Business Machines, “Tivoli NetView for UNIX Release Notes,” Version 7.1.4, SC32-1239-00

International Business Machines, “Tivoli NetView for Windows Release Notes,” Version 7.1.4, SC32-1240-00

Microsoft Corporation, “Microsoft Systems Management Server 2003 Concepts, Planning, and Deployment Guide”

Microsoft Corporation, “Microsoft Systems Management Server 2003 Operations Guide”

Microsoft Corporation, “Scenarios and Procedures for Microsoft Systems Management Server 2003: Security”

Tivoli Systems, “Application Development Environment Release Notes,” Version 3.6.5, 8 January 2001

Tivoli Systems, “Application Development with TME 10 ADE,” Version 3.6, September 1998

Tivoli Systems, “Tivoli Enterprise Firewall Security Toolbox User’s Guide,” Version 1.3.1, GC23-4826-01

Tivoli Systems, “Tivoli Enterprise Installation Guide,” Version 4.1.1, GC32-0804-01

Tivoli Systems, “Tivoli Event Integration Facility Reference,” Version 3.9, SC32-1241-00

Tivoli Systems, “Tivoli Inventory Release Notes Version 3.6.2,” December 1999

Tivoli Systems, “Tivoli Management Framework, Version 4.1.1. Documentation Road Map,” November 2003, GI11-0891-01

Tivoli Systems, “Tivoli Management Framework Maintenance and Troubleshooting Guide,” Version 4.1.1, GC32-0807-01

Tivoli Systems, “Tivoli Management Framework Planning for Deployment Guide,” Version 4.1.1, GC32-0803-01

Tivoli Systems, “Tivoli Management Framework Release Notes,” Version 4.1.1, GI11-0890-01

Tivoli Systems, “Tivoli Management Framework User’s Guide,” Version 4.1.1, GC32-0805-01

Tivoli Systems, “Tivoli Manager for MQSeries Revised February 14, 2003, Release Notes,” Version 2.4.0, GI10-3059-06

Tivoli Systems, “Tivoli NetView for UNIX Administrator’s Guide, Version 7 1, SC321246-00

Tivoli Systems, “Tivoli NetView for Windows User’s Guide,” Version 7, Release 1.4, SC32-1245-00

Tivoli Systems, “TME 10 ADE Application Services Manual, Volume I,” Version 3.6, September 1998

Tivoli Systems, “TME 10 ADE Application Services Manual Volume II,” Version 3.6, September 1998

Tivoli Systems, “TME 10 AEF User’s Guide,” Version 3.6, September 1998

Tivoli Systems, “TME 10 AEF Release Notes,” Version 3.6, September 1998

Tivoli Systems, “TME 10 Inventory User’s Guide Version 3.6,” September 1998

Tivoli Systems, “TME 10 Software Distribution AutoPack User’s Guide Version 3.6,” September 1998

Tivoli Systems, “TME 10 Software Distribution Release Notes Version 3.6,” September 1998

Tivoli Systems, “TME 10 Software Distribution User’s Guide Version 3.6,” September 1998

Other Publications:

International Telecommunication Union (ITU), “CCITT Recommendation X.700 (09/92), Management Framework for Open Systems Interconnection (OSI) for CCITT Applications”

International Telecommunication Union (ITU), “ITU-T Recommendation M.3400 (02/2000), TMN Management Functions”

Web Sites:

Carnegie Mellon Software Engineering Institute's Software Technology Roadmap	http://www.sei.cmu.edu/str/
Committee on National Security Systems (CNSS) Library	http://www.cnss.gov/
Distributed Management Task Force (DMTF)	http://www.dmtf.org/
DoD Ports and Protocols Program	http://iase.disa.mil/ports/index.html
IBM Tivoli Documentation	http://www-306.ibm.com/software/sysmgmt/products/support/
Information Assurance Support Environment	http://iase.disa.mil/ http://iase.disa.smil.mil/
Information Assurance Technical Framework (IATF) Forum	http://www.iatf.net/
Internet Engineering Task Force (IETF)	http://www.ietf.org/
Microsoft Lifecycle Dates	http://support.microsoft.com/ http://www.microsoft.com/
Microsoft Security Bulletin Search	http://www.microsoft.com/technet/security/current.aspx
Microsoft SMS Home	http://www.microsoft.com/smserver/
Microsoft SMS 2003 Toolkit 1	http://www.microsoft.com/smserver/downloads/2003/tools/toolkit.asp
Microsoft TechNet: Systems Management Server	http://www.microsoft.com/technet/prodtechnol/sms/default.mspx
National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)	http://csrc.nist.gov/pcig/cig.html

This page is intentionally left blank.

APPENDIX B. TIVOLI

The evolution of open systems has led to the creation of large enterprises. Tivoli Software, a member of the IBM Software group, considers enterprises to be large collections of heterogeneous hardware and software connected by different sized networks that support the distributed computing requirements of an organization. Due to the diverse hardware and software components located in an enterprise, the different methodologies and procedures used to support them, and the different types of personnel needed, Enterprise Systems Management (ESM) has become a major challenge for many data processing organizations. Additionally, these areas have created significant security challenges in enterprise systems management.

In order to resolve many of the challenges and problems encountered by ESM personnel, Tivoli Software has developed a suite of integrated software products specifically designed to address the management, administrative, and security requirements of enterprise architecture in a consistent and standardized manner.

B.1 Tivoli Enterprise Architecture

Tivoli's approach to enterprise architectures is to break the enterprise into one or more smaller sections referred to as Tivoli Management Regions (TMRs). Each TMR is a self-contained entity. In early releases of Tivoli, the TMRs were two tier structures having a management server and a series of clients, now referred to as endpoints. Because the TMR Server was limited to the number of clients/endpoints that could be connected and serviced, gateway servers, which work as proxy servers, were added. Gateway servers absorbed some of the responsibilities of the management server and enabled more endpoints to be connected. In addition, Tivoli Management Agents (TMAs), or endpoints, were added to receive distributions, execute tasks, run monitors, and send events. TMAs are used to manage many of the Tivoli systems as opposed to Managed Nodes or PCs running the PC agent (PC managed nodes).

By standardizing much of the management, administrative, and security procedures, TMRs can be interconnected across networks thus creating the Tivoli Management Enterprise (TME) architecture. In order to manage and administer many of the elements of a TME, many Tivoli organizations utilize configuration diagrams, which describe the hardware, software and network elements involved. ESM configuration diagrams also provide organizations with the information needed to ensure accountability and continuity of the ESM environment.

- *(TME.0001: CAT II) The IAO will ensure a current configuration document exists describing the Tivoli enterprise architecture, to include such items as TMR server(s), gateways, managed nodes, firewalls, and endpoints. This documentation is maintained as part of the SSAA.*

B.1.1 Tivoli Management Region (TMR)

A TMR is the most basic element in a Tivoli enterprise. TMRs consist of a Tivoli Management Server(s), one or more Tivoli Gateways, and one or more Tivoli Endpoints. TMRs can exist independently in conjunction with other TMRs or interconnected either wholly or partially to other TMRs.

Because of the possible configurations that can exist in a Tivoli enterprise regarding TMRs, functionality and support can be centralized or decentralized. Centralized support uses a top down structure where everything is initiated at the TMR server level and flows downward through the gateways to the endpoints. Decentralized support is different in that much more of the support is initiated at the local gateway layer and distributed accordingly. In either case, since a standardized methodology is used and a common interface provided implementation, communication and problem resolution can be easier.

B.1.2 Tivoli Servers

In a TME there are various types of Tivoli servers. They may be TMR servers, Managed Node(s), Tivoli Gateway(s), and Tivoli Endpoint Gateway(s). In all cases, Tivoli servers run the Tivoli Management Framework (TMF) software and have the libraries, binaries, data files, and the graphical user interface (GUI), the Tivoli Desktop, needed to support their portion of the Tivoli environment. A typical Tivoli server contains the following components:

- A database used to maintain data for either the entire Tivoli region or a specific portion of the Tivoli region.

- The object dispatcher, oserv, is used to coordinate communications with managed nodes and gateways.

- The endpoint manager is used to manage all of the endpoints in the TMR.

- *(EGE.0010: CAT II) The IAO will ensure physical access to all Tivoli servers is restricted to Tivoli administrators, SAs, and IAM authorized personnel.*

B.1.2.1 TMR Server

The Tivoli Management Environment (TME) contains a set of systems that are managed by one server called the TMR Server. You can interconnect TMR's in order to execute management functions across your entire TME, however the master TMR must be created first. A TMR server is the central controlling element in a Tivoli Management Region. TMR servers are placed on either UNIX or Windows platforms. The TMR server is responsible for maintaining the TMR server's database. It contains information about all of the resource components of a TMR to include security and functionality of the resources. TMR servers are capable of creating the other Tivoli servers in a TMR.

TMR Servers communicate with other TMR servers, gateways or managed nodes, by using the oserv daemon, which is an object dispatcher. The oserv daemon normally begins executing when the TMR server starts up and terminates when the server comes down. In order to manage the endpoints, TMR servers use an endpoint manager service, which also runs on the TMR server.

Communication with a TMR Server by an administrator is performed through three types of interfaces: A graphical user interface GUI, known as the Tivoli Desktop, the Command Line Interface CLI and the Tivoli Web Interface. The TMR server is responsible for performing all

authentication and verification necessary to ensure the security of TMR data. All major TMR administration, security, and management functions are generally performed at the TMR server level.

B.1.2.2 Tivoli Managed Nodes

A Tivoli Managed node is a server or a PC that runs the TMF software. Tivoli Managed nodes run the oserv daemon, maintain a local database, and allow for the use of the Tivoli Desktop facility.

The primary difference between the TMR server and a managed node is that the TMR server database contains all information about the entire TMR and a managed node's database contains information about the managed node and its subordinates. There can be multiple Manage Nodes in a TMR, all of which are subordinate to the TMR server.

B.1.2.3 Tivoli Gateways

A Tivoli gateway is a managed node that resides between the TMR server and endpoints within a TMR. Gateways are proxy servers responsible for controlling communication between the TMR server and endpoints. They perform operations on endpoints on behalf of the TMR server. Gateways can launch TMR programs that run on endpoints and the results reported to the TMR server by the gateways.

Depending on the Tivoli products running on the gateways and their processing capabilities, they can manage large numbers of endpoints, thus relieving the TMR server to perform other services on behalf of the TMR. Finally, gateways provide an additional benefit in that they can be organized to support specific subsections of a TMR thus allowing for localized management, administration, and security of sections of a TMR.

B.1.3 Security Considerations for Tivoli Servers

As mentioned earlier in *(Section B.1.2)*, there are various types of Tivoli servers, their functionality determines the type of server they are. The following security considerations apply to all Tivoli servers:

- Access to Tivoli Server functions is controlled through the assignment of Tivoli authorization roles to Tivoli users. Without proper assignment of these roles, the integrity of Tivoli software could be compromised.

- All Tivoli Servers require Tivoli software to be installed. As with most software products, many are composed of program and data files for which proper access controls are essential. Although most of the product files reside in directories subject to access controls required for the TMF software, there are some Tivoli product directories and files that will require specific access controls.

- If web interface features are used, user transactions are processed through HTML pages. The integrity of the HTML files must be assured to maintain transaction security.

  - Tivoli Servers may be located in many locations within a TMR. The placement of these servers is important because of the type of information located on them and their functional importance to the TMR. Careful consideration must also be given as to personnel access, maintenance, backup, recovery and connectivity.

- Tivoli may use various types of database management systems (DBMS) to support the Tivoli products on Tivoli Servers. All databases supporting Tivoli products, excluding the internal proprietary object database under TMF Release 3.6, must be configured in accordance with the Database STIG. Because such Tivoli commands as the wchkdb command are used to maintain the Tivoli database, careful consideration must be given to file permissions and authorization roles. *(Section B.2.3 provides additional information regarding the object database.)*

- Unauthorized remote access to the Tivoli Servers can have a major impact on the integrity of the TME. As a result, careful consideration as to firewalls, ports, and physical locations of the Tivoli Servers must comply with the *Enclave* and *Network STIGs*.

- Auditing controls must be implemented so as to ensure accountability and recoverability.

  - Encryption must be implemented to assure confidentiality and data integrity within the TME. Set encryption level in accordance with *FIPS 140-2* approved encryption, key exchange, digital signature, and hash algorithms for data storage and transmission.

- Restrict endpoint access to a TMR by assigning Tivoli servers that are using DHCP Dynamic Host Configuration Protocol DHCP to a group of static IP addresses.

  - Ensure that the handling of Tivoli server files and data are included in the disaster recovery plans and procedures.

- *(COE.0010: CAT I) The IAO will ensure regularly scheduled execution of continuity of operations or disaster recovery plans are executed annually.*

- *(EGA.0060: CAT II) The IAO will ensure the Tivoli administrators have configured the Tivoli software, which resides on Tivoli servers, to use FIPS 140-2 validated encryption algorithms, key exchange, digital signature, and hash algorithms for data storage and transmission.*

- *(EGA.0090: CAT II) The IAO will ensure access to Tivoli software libraries (including executable and configuration files) is limited so:*

  - *Only authorized Tivoli application processes, Tivoli administrators, SAs, or IAM authorized personnel, which require it, have update access.*

  - *Only authorized Tivoli application processes, Tivoli administrators, SAs, or other IAM authorized personnel require it and are within applicable license agreements, have read access.*

- *(EGA.0100: CAT II) The IAO will ensure access to Tivoli software libraries is limited so only authorized Tivoli application processes. Tivoli administrators, SAs, or IAM authorized personnel can execute privileged programs.*

- *(EGA.0110: CAT I) The IAO will ensure Tivoli software is removed or upgraded prior to the vendor no longer providing support.*

- *(EGA.0120: CAT III) The IAO will ensure the site has a formal migration plan for removing or upgrading Tivoli software prior to the date the vendor no longer provides security patch support.*

- *(EGE.0010: CAT II) The IAO will ensure physical access to Tivoli servers is restricted to Tivoli administrators, SAs, and IAM authorized personnel.*

- *(EGF.0010: CAT II) The IAM will ensure the disaster recovery plan for the Enclave includes appropriate provisions for the continuity of Tivoli if it is used to provide essential information assurance functions such as security patch management or antivirus signature deployment.*

    - *For Tivoli applications serving Mission Assurance Category (MAC) III systems, resumption within five days of activation;*

    - *For Tivoli applications serving MAC II systems, resumption within 24 hours of activation;*

    - *For Tivoli applications serving MAC I systems, transfer to an alternate site for the duration of an event with little or no loss of operational continuity.*

- *(EGF.0030: CAT II) The TMR Administrator will ensure Tivoli data is managed appropriately to the assigned MAC of the systems served by the Tivoli application.*

    - *For Tivoli configurations managing MAC III client systems, Tivoli data is backed up at least weekly;*

    - *For Tivoli configurations managing MAC II client systems, Tivoli data is backed up daily and the recovery media is stored at an off-site location affords protection in accordance with the mission assurance category and confidentiality level of the data;*

    - *For Tivoli configurations managing MAC I client systems, Tivoli data is backed up by maintenance of a redundant secondary system, not collocated, can be activated without loss of data or disruption to the operation.*

B.1.4 Tivoli Endpoints

In a Tivoli environment Tivoli endpoints make up the lowest level of a TMR. They are systems that ultimately receive Tivoli operations. Endpoints run the Tivoli endpoint lcfd daemon or

service and are capable of receiving distributions, executing tasks, running monitors, and sending events. Tivoli endpoints can run on Windows, UNIX, OS/2, and NetWare Systems.

B.1.4.1 Security Considerations for Endpoints

Unlike Tivoli servers, endpoints do not require a large amount of software to be loaded on the platform. As a result, they rely on the platform for providing the security for the endpoint processes and files. The following areas apply when securing endpoints:

- *(NA/NA) The IAO will ensure the Tivoli endpoint libraries, binaries, and resource files are restricted from unauthorized access and update.*

- *(NA/NA) The IAO will ensure the administrator commands are restricted from unauthorized access, update and use.*

- *(NA/NA) The IAO will ensure the endpoint port utilization is limited to approved ports.*

- *(NA/NA) The IAO will ensure encryption is implemented to assure confidentiality and data integrity within the TME. Set encryption level in accordance with FIPS 140-2 validated encryption algorithm, key exchange, digital signature, and hash algorithms for data storage and transmission.*

- *(NA/NA) The IAO will ensure auditing controls are implemented to ensure accountability and recoverability.*

- *(NA/NA) The IAO will ensure the tmersrvd account, a general-purpose account used by Tivoli methods, is enabled to utilize system authority on endpoints.*

- *(NA/NA) The IAO will ensure the tmersrvd account is authorized to utilize non-expiring passwords.*

- *(EGA.0060: CAT II) The IAO will ensure the Tivoli administrators have configured the Tivoli endpoint software; to use FIPS 140-2 validated encryption algorithms, key exchange, digital signature, and hash algorithms for data storage and transmission.*

- *(EGA.0090: CAT II) The IAO will ensure access to endpoint Tivoli software libraries (including executable and configuration files) is limited so:*

    - *Only authorized Tivoli application processes, Tivoli administrators, or SAs, that require it, have update access.*

    - *Only authorized Tivoli application processes, Tivoli administrators, SAs, or other users that require it and are within applicable license agreements, have read access.*

- *(EGA.0100: CAT II) The IAO will ensure access to endpoint Tivoli software libraries is limited so only authorized Tivoli application processes, Tivoli administrators, or SAs can execute privileged programs.*

- *(EGE.0010: CAT II) The IAO will ensure physical access to Tivoli endpoints is restricted to Tivoli administrators, SAs, and IAM authorized personnel.*

- *(TME.0002: CAT II) The IAO will ensure documentation exists, which justifies the existence and use the tmersrvd account on endpoint platforms.*

B.2. Tivoli Management Framework

B.2.1 Overview

The TMF is the backbone software of a Tivoli Enterprise. The TMF provides a standardized set of administration and management services that are used by all Tivoli products.

In a normal enterprise, there are many different types of functions that must be performed. They include such activities as the distribution of software patches and new releases, hardware, software and network monitoring, backup and recovery, and user administration. Tivoli administrators, who use the other Tivoli products that are integrated onto the TMF, perform these types of functions. As a result, as new functions are identified, additional Tivoli products are integrated onto the TMF.

The TMF software is loaded on each TMR server, managed node and gateway in a Tivoli Management Enterprise. In general, the TMF software does not affect the configuration of the platform on which it is installed, whereas the other Tivoli products from the Tivoli software suite may. Because of the importance of the TMF software in relation to the Tivoli Enterprise and the other Tivoli products, it is critical that the physical security of the platforms, network connectivity, file access controls, change management and backups and recovery be addressed so as to ensure the confidentiality, availability and integrity of the Tivoli Enterprise and the resources that exist in it.

- *(TMF.0001: CAT II) The IAM will ensure a current Tivoli Enterprise or Tivoli Management Region architecture / configuration document exists and is documented in the SSAA.*

- *(TMF.0002: CAT II) The IAO will ensure the TMR server, gateways and managed nodes are located in controlled areas accessible to IAM documented authorized personnel.*

- *(TMF.0003: CAT II) The SA and TMR Administrator will ensure the TMF software is restricted from unauthorized update and access.*

- *(TMF.0004: CAT II) The Tivoli Administrators or SAs will maintain currently supported Tivoli software on all platforms within the Tivoli Enterprise.*

- *(TMF.0005: CAT II) The IAM will ensure public domain software products (freeware or shareware) are not used in the Tivoli environment without DAA approval.*

- *(TMF.0006: CAT II) The IAM will ensure a System Security Plan is established and describes the technical, administrative, and procedural IA program and policies that govern the Tivoli Management Environment (TME)/TMR.*

- *(TMF.0007: CATII) The IAM will ensure all systems that host Tivoli software are configured in accordance with the appropriate STIG.*

- *(TMF.0008: CAT II) The Tivoli Administrators or platform SAs will apply all security related patches.*

- *(TMF.0009: CAT III) The IAO will ensure a comprehensive set of procedures is implemented to test all patches, upgrades, and new applications prior to deployment.*

- *(TMF.0010: CAT III) The IAM will ensure a current processing plan exists for the Tivoli Enterprise or TMR.*

- *(TMF.0011: CAT III) The IAM will maintain documentation on file demonstrating the performance of annual contingency testing on the Tivoli Enterprise or TMR.*

- *(TMR.0012: CAT II) The TMR administrator and Tivoli administrators will maintain documentation describing the procedures necessary to perform a trusted recovery of the TMR, policy regions, managed nodes and gateways in the event of a technical failure.*

- *(TMF.0013: CAT II) The IAM will ensure the TMF and all integrated Tivoli products are configured to use only authorized ports and protocols in accordance with the Network STIG and DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) and the associated Ports, Protocols, and Services (PPS) Assurance Category Assignments List.*

- *(TMF.0014: CAT II) The IAM will ensure the following software/services are removed from the TMR server: telnet, ftp, rsh, and rlogin.*

- *(TMF.0015: CAT III) The IAM will ensure a documented change management (CM) process is implemented for the TME/TMR.*

- *(TMF.0016: CAT III) The IAM will ensure a current and comprehensive baseline inventory of all Tivoli software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support the TMF is maintained by the IAM. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.*

B.2.2 Interfaces

The TMF provides administrators with three types of interfaces: The Tivoli Desktop, the Command Line Interface (CLI) and the Tivoli Web Interface. The following sub sections describe each and their security considerations.

B.2.2.1 Tivoli Desktop

The Tivoli Desktop is the standard graphical user interface (GUI) provided by Tivoli that enables administrators to communicate with the TMF and the other Tivoli products in the Tivoli Enterprise. There may be many Tivoli Desktops depending on the number of administrators and the functions they perform. The TMR Administrator uses a Tivoli Desktop to maintain global control over the TMR server and the TMR resources. Policy Region administrators use Tivoli Desktops to maintain policy region (local) control over their resources. Because of the capabilities of this tool, the Tivoli Desktops must be located in a controlled area, accessed only by authorized Tivoli administrators and protected by the firewall and other perimeter defenses.

- *(TMF.0017: CAT II) The IAM will ensure all Tivoli desktops are located in an area, which is restricted from unauthorized access and protected by the local firewall.*

- *(TMF.0018: CAT II) The IAM will ensure the TMR Administrator restricts Tivoli Desktop usage by Policy Region.*

B.2.2.2 Command Line Interface

The CLI is an alternate way of performing many Tivoli functions in a TMR. The CLI enables an administrator to use Tivoli commands instead of navigating through the different panels of the Tivoli desktop. The CLI also provides administrators the ability to develop scripts that can be executed to perform management or administrative tasks in a single step. The Tivoli commands can also be used in shell scripts and with system utilities such as the UNIX cron utility.

- *(TMF.0019: CAT II) The IAM will ensure the SA restricts CLI access to the TMR Administrator, the Policy Region Administrator(s), and IAM documented authorized personnel.*

B.2.2.3 Web Interface

The TMF also provides access to Web-enabled Tivoli Enterprise applications through a browser. When HTTP requests are submitted to a TMR server, the requests are redirected to the Web server that processes them. The TMF, using a collection of servlets and support files that are installed on the Web server is able to establish a secure connection between the Web server and the Tivoli server, thus allowing an administrator to perform specific functions such as view Tivoli Management Agents and endpoints.

- *(TMF.0020: CAT II) The IAM will ensure the Web Administrator restricts all Tivoli servlets and support files from unauthorized update and access by unauthorized personnel.*

- *(TMF.0021: CAT II) The IAO will ensure remote access for Tivoli administrators employs at a minimum: Session security measures such as a VPN configured in non-tunnel (blocking) mode and to allow only authorized traffic.*

- *(TMF.0022: CAT II) The IAO will ensure the httpserv.log and the httptran.log files are included as part of the regularly scheduled site backups.*

B.2.3 Components

The TMF is the backbone infrastructure of the Tivoli software suite. It is considered the backbone because it provides and enforces a standardized consistent methodology for enterprise system management. Other Tivoli software products use many of the TMF's components as they are integrated onto the TMF. The following subsections describe the components of the TMF and the security requirements to be addressed.

B.2.3.1 Administrators

Tivoli Administrators are responsible for the management, administration and operational support for the TME. Many of these functions require Tivoli administrators to have root or privileged account authority on the systems they support. In order to allow administrators to use the system root or privileged account, the TMF delegates its usage without allowing administrators the system password or full root authority. It is accomplished through the assignment of Tivoli authorization roles.

When the TMF is first installed, a Tivoli root administrator is automatically created with a default password. That administrator is created to enable the Tivoli root administrator to configure Tivoli, to create other administrators and assign authorization roles to them.

In addition to Tivoli Administrators requiring privileged authority, most Unix or Windows system administrators, that have the Tivoli software installed on their machine, have a Tivoli administrator mapped to their system account. Authorization roles will be further discussed later in this document.

- *(TMF.0024: CAT II) The IAM will ensure all access and use of privileged accounts is limited to Tivoli administrators and IAM documented authorized personnel.*

- *(TMF.0025: CATI) The SA or TMR administrator will ensure all Tivoli default accounts or passwords are disabled.*

B.2.3.2 Resources

In a TME, many resources exist ranging from network to system resources. In order for resources to be managed by Tivoli, they must be defined as managed resources. When a managed resource is created, it is assigned a default policy (which controls it) and is defined in a policy region. Once a managed resource is created, Tivoli administrators are able to manage, administer and operationally support them.

Many of the different Tivoli products represent the managed resources they control as icons on the Tivoli desktops. Icons provide a model of the physical resources to be managed by Tivoli applications. Thus, as new Tivoli products are installed in the TMR, new icons may be added onto the administrator's desktops. This will depend on the authorization roles assigned the administrator and the functionality needed.

- *(TMF.0025: CAT III) The TMR administrator will maintain documentation listing all authorized resources in the TMR/TME.*

- *(TMF.0026: CAT II) The IAM will ensure resource creation is restricted to the TMR administrator and IAM documented authorized personnel.*

B.2.3.3 Policy and Policy Regions

A policy is a set of rules that is used by the TMF to manage resources. In addition, policies can be used to customize Tivoli products in a Tivoli environment. A policy has two parts: a default policy and a validation policy. A default policy describes the default properties assigned to a resource when it is created and a validation policy defines valid attributes that are to be checked when a new instance of a resource is created or when a resource is modified.

A policy region is a logical collection of resources that are controlled by one or more policies. The set of managed resources that may exist in a policy region depends on the applications and the products installed in the TMR. Resource access is controlled when resources are organized in policy regions and authorization roles are assigned at the resource level. In this way, administrators are limited to only those resources contained within the policy.

- *(TMF.0027: CAT II) The IAM will ensure all policy creation and installation is limited to the TMR administrator and IAM documented authorized personnel.*

- *(TMF.0028: CAT II) The IAM will ensure Tivoli administrators, other than the TMR administrator, are granted access at the policy region level and assigned resource roles granting them access to the specified policy region.*

B.2.3.4 Tasks and Task Libraries

Tasks are used to define operations that are to be performed on a routine basis. They identify such information as the executable files, the user ID or group ID that will be used for execution, and the authorization role needed. Tasks do not specify such information as execution location, output type and any special execution parameters. Either an administrator or a job that executes the task provides that type of information. In order for a Tivoli administrator to execute a task, the administrator must have the appropriate authorization role assigned in the policy region where the task will be executed.

Task libraries are used to store tasks, jobs, binaries, scripts, and programs that may be used by applications. Multiple task libraries can exist in a TMR and are organized by policy region. This enables tasks and jobs to be restricted to a specific group of resources.

- *(TMF.0029: CAT II) The IAO will ensure task creation and installation is restricted to the TMR administrator and IAM documented authorized personnel.*

- *(TMF.0030: CAT II) The IAO will ensure task libraries are backed up as part of the regularly scheduled backup process.*

B.2.3.5 Scheduler

In a TME, jobs are run to perform various types of administration and management functions. The scheduler component is not only responsible for controlling the scheduling and execution of jobs, but also the verification and authorization of administrators who submit jobs for execution. Jobs are the same as tasks. They reside in task libraries and provide execution parameters needed for task execution.

Control of the scheduler, (to include the starting, stopping and viewing of scheduled jobs) is accomplished through the use of scheduler commands. Tivoli administrators must be authorized with the correct authorization roles and permissions/group authorizations to interface with the scheduler.

- *(TMF.0031: CAT II) The IAM will ensure the starting, stopping and configuration of the scheduler daemon is limited to the TMR administrator, and IAM documented authorized personnel.*

B.2.3.6 Notification, Notices and Notice Groups

The notification facility provides Tivoli administrators information about operations and changes in a TMR. The information is created as a notice and upon generation, is sent via email to special locations knows as notice groups. The message text for notices is stored in Message catalogs thus allowing administrators to view messages in different languages, based on the Tivoli desktop.

When the TMF is installed, default notification groups are created. Additional notice groups may be created as needed. In order for a Tivoli administrator to obtain notices, the administrator must subscribe, (belong), to the appropriate notice group. Because of the types of information that may be contained in notices, notices can be used as an audit trail and reviewed on a regular basis for security violations.

- *(TMF.0032: CAT II) The IAM will ensure notice group creation is restricted to the TMR administrator and IAM documented authorized personnel.*

- *(TMF.0033: CAT II) The IAO will ensure notice group subscriptions are restricted to the TMR administrator; the policy region administrators or IAM documented authorized personnel.*

- *(TMF.0034: CAT II) The SA or Tivoli administrators will ensure the message catalogs are backed up as part of the regularly scheduled backup process.*

B.2.3.7 Relational Database Management System (RDBMS) Interface Module

The RDBMS Interface Module (RIM) is responsible for providing a common interface between Tivoli application products and relational databases. RIM enables Tivoli application products to store and retrieve information in a database-independent manner. RIM is installed as part of the TMF installation, and is created on a managed node referred to as the RIM host.

Several components work together to make communication through the RIM possible. The client application uses RIM Application Program Interfaces (APIs) to make requests. The RDBMS_Interface translation layer processes requests and submits them the RIM host, and the vendor adaptor layer sends the vendor-specific requests to the database.

In order for a Tivoli application to use RIM, it must have RIM objects created in the object database and configuration changes applied by the administrator to the RIM configuration file.

- *(TMF.0035: CAT II) The SA or TMR administrator will ensure the tnsnames.ora configuration file is restricted from unauthorized access and update.*

- *(TMF.0036: CAT II) The IAO will ensure the Oracle instance ID specified in tnsnames.ora configuration file complies with instance names as specified in the Data Base STIG.*

- *(TMF.0037: CAT II) The IAM will ensure the port specified for SQL*Plus in tnsnames.ora configuration file complies with the approved ports as specified in DoDI 8551.1, (PPSM).*

- *(TMF.0038: CAT II) The SA or TMR administrator will ensure the communication protocol specified in the tnsnames.ora configuration file complies with the approved protocols as specified in DODI 8551.1, (PPSM).*

- *(TMF.0039: CAT II) The SA or TMR administrator will ensure the Oracle database and audit log are backed up as part of the regularly scheduled site backups.*

- *(TMF.0040: CAT II) The IAO will ensure the Oracle audit log is restricted from unauthorized access.*

- *(TMF.0041: CAT II) The IAM will ensure the RIM APIs are protected from unauthorized update and access.*

B.2.4 Services

As mentioned in the previous section regarding components the TMF is the backbone infrastructure of the Tivoli software suite. Other Tivoli software products use many of the services provided by the TMF as they are integrated onto the TMF. The following subsections describe the TMF services and the security requirements to be addressed.

B.2.4.1 Object Dispatcher

The Object Dispatcher daemon, oserv, is responsible for coordinating communication between systems within a TME. All managed modes run the oserv daemon. The oserv daemon may or may not be started when the TMR server or the gateways are started. It should be noted that when the object dispatcher runs on a Windows Managed Node it starts as the Windows built-in system account because it is a service. As the object dispatcher starts, it attempts to validate the Tivoli remote access account, *tmersrvd*. Oserv uses a log file to record information about activity. This log file is called oservlog.

- *(TMF.0042: CAT II) The IAO will ensure the oserv service is restricted from unauthorized access, update, starting and stopping.*

- *(TMF.0043: CAT II) The IAO will ensure the TMR log file, $DBDIR/oservlog, is restricted from unauthorized update and access.*

B.2.4.2 TMF Management Database

The TMF uses a logical database to store information about objects in the TMR. The database is distributed between the TMR server and all of the managed nodes that are configured in a TMR. When the management database is installed on a Windows system the database file must be installed on the local NT File System (NTFS) partition.

- *(TMF.0044: CAT II) The SA or TMR administrator will ensure the TMF management database is restricted from unauthorized access and update.*

- *(TMF.0045: CAT II) The TMF management database is included as part of the regularly scheduled backup process.*

B.2.4.3 Application Services

Application services are the primary Tivoli capabilities and services that are used by the other Tivoli products. These services include task libraries (for remote or local command execution), schedulers, a notification mechanism, and file distribution capabilities.

In order to support file distributions, the TMF supports Multiplex Distribution (MDist). It provides a fan-out mechanism that enables a more efficient method of file distributions to many systems. Repeaters are used to perform the fan-out mechanism. They receive a copy of a distribution and pass the files onto one or more targets systems, which saves bandwidth.

Finally, in order for the other Tivoli Application product services to provide support they must utilize profiles and profile managers.

- *(TMF.0046: CAT II) The IAM will ensure the use of MDist is limited to the TMR administrator and policy region administrator(s).*

B.2.4.4 Installation Services

The TMF is able to install other TMF components and Tivoli application products. These services use the TMF's ability to transfer files and execute commands on client systems. Installation services are a core part of the TMF. They can be used directly or through the Tivoli Software Installation Services (SIS), which provides a Java-based front end.

- *(TMF.0047: CAT II) The IAO will ensure the use of SIS is limited to the TMR Administrator and Policy Region Administrators.*

B.2.4.5 Tivoli Management Agent Support

A Tivoli Management Agent (TMA) is a managed system that runs the TMA endpoint software. The TMA software works in conjunction with the other products to manage the endpoint resources. Because it is designed to provide full management of systems that do not have the oserv daemon and the Tivoli distributed database loaded, the TMA software is able to use less resources.

In order to track TMA endpoints, the TMR server uses the endpoint manager, which is a service (or daemon) on the TMR. The endpoint manager is responsible for controlling and configuring gateways and endpoints, assigning endpoints to gateways, and maintaining the endpoint list, which contains information about each endpoint in a TMR.

- *(TMF.0048: CAT II) The IAO will ensure the creation and installation of TMAs is limited to the TMR Administrator, and IAM documented authorized personnel.*

- *(TMF.0049: CAT II) The IAO will ensure the epmgrlog* file *is included as part of the regularly scheduled backups.*

B.2.4.6 Name Registry

The Tivoli Name Registry (TNR) is a table of managed resources in the TMR. It provides such information as resource labels and object identifiers and is used to prevent name-space conflicts. Not all resources are registered in the TNR. In most cases resources are added and deleted automatically by the TMF. Tivoli administrators are able to manipulate resources on the TNR.

The TNR plays a significant role during interconnected TMR communications. TNR corruption could significantly impact the communications between TMRs. The causes for TNR corruption can vary from resources being created improperly, to synchronization problems. In either case, the availability and performance can be impacted. The Tivoli documentation provides additional detail on corruption issues and resolution.

- *(TMF.0050: CAT II) The IAO will ensure updates to the TNR are limited to the TMR administrator and IAM documented authorized personnel.*

B.2.4.7 Profiles and Profile Managers

A profile is a collection of Tivoli application information as it relates to users, software and hardware in the Tivoli environment. Profiles serve as templates or prototypes that enable Tivoli administrators to centrally manage and control data distribution to groups of systems. Much of the information contained in profiles relates to configuration information. Profiles are represented as icons on the Tivoli administrator's desktops.

A profile manager is a container where individual profiles can be created and organized into groups of profiles. In addition subscribers can be linked to them. Profile managers are created within a policy region. A profile manager can logically be viewed as having two sections, a profile section and a subscriber section. Profile managers control the distribution of profiles to subscribers. Subscribers to a profile manager can be in the same policy region as their profile manager or in other policy regions.

- *(TMF.0051: CAT III) The IAO will ensure the creation and maintenance of profiles and profile managers is limited to the TMR administrator and IAM documented authorized personnel.*

B.2.5 Authorization Roles

Tivoli authorization roles may be assigned either as TMR roles (globally) or as resource-based roles to a collection of resources. When authorization roles are assigned globally, they pertain to all resources across all policy regions within a TMR. By assigning roles at the resource level and assigning them to policy regions, the principle of least privilege is applied to Tivoli management and administration.

- *(TMF.0052: CAT II) The IAO will ensure the authorization of global TMR roles is limited to the TMR administrator and IAM documented authorized personnel.*

- *(TMF.0053: CAT II) The IAO will ensure the SA removes the default Tivoli root administrator account or TMR administrator and a new Tivoli administrator root account, under a different name, is created.*

- *(TMF.0054: CAT II) The IAM will ensure Tivoli administrators, who have been assigned administrative access to specific managed nodes, are not provided administrative access to the TMR server from any Tivoli managed node.*

B.2.6 Commands

As stated earlier in this document, the CLI enables administrators to perform administrative and maintenance functions by entering commands in place of using pre-specified panels. In order for an administrator to perform these functions using commands, the administrator must be authorized at the local platform and through the assignment of Tivoli roles.

- *(TMF.0055: CAT II) The IAO will ensure Tivoli commands are restricted from unauthorized access and usage through the assignment of permissions or group authorizations.*

- *(TMF.0056: CAT II) The TMR administrator will ensure the use of Tivoli commands is limited to IAM documented authorized personnel.*

B.2.7 Supported Platforms

- *(TMF.0057: CAT II) The SA and TMR administrator will limit the installation of the Tivoli software to supported platforms as documented by the vendor.*

B.2.8 Files

The TMF software is installed into a series of Tivoli directories on the TMR server and the managed nodes in a TMR. As part of the installation process, certain script system variables are set. The variables are used to make the installation flexible when dealing with different platforms. Some of the variables established are: BINDIR, DBDIR, INTERP, LIBDIR, MANPATH. The Object Permissions section defines these and others and cites their usage when applicable. It should be noted that for Unix platforms a $ will precede the variable and for Windows platforms a % sign will be used before and after the symbol.

- *(TMF.0058: CAT II) The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of Tivoli software, do not exist in the currently distributed Tivoli directories.*

- *(TMF.0059: CAT II) The SA will restrict the Tivoli directories from unauthorized access and updates through file permissions or group authorizations.*

- *(TMF.0060: CAT II) The SA and TMR administrator will ensure the Tivoli install files are removed from the system upon successful completion of the installation process.*

B.2.9 Interconnected TMR Resource Exchange

TMRs can be interconnected to allow for an exchange and management of selected resources. In the first configuration, known as a one-way connection, one TMR is established as the managing TMR and the other as the managed TMR. This connection is built to stop the managed TMR from knowing what resources are located in the managing TMR.

The second configuration is referred to as a two-way connection. In a two-way connection, both TMRs are totally aware of each other. When two TMRs are connected to each other in a two-way connection, the TMR in each region can exchange information with the other about registered resources. Management, and recovery of a two-way connection is more complex.

- *(TMF.0061: CAT II) The IAO will ensure the assignment of roles necessary to update and access resources of interconnected TMRs are limited to the TMR administrator and IAM documented authorized personnel.*

B.2.10 Intraregion and Interregion Encryption

- *(TMF.0062: CAT II) The IAM will ensure NIST FIPS 140-2 validated cryptography is used to implement encryption (e.g., AES, 3DES), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512) and that newer standards are applied as they become available.*

B.2.11 Related Products

B.2.11.1 Tivoli Application Extension Facility (AEF)

The Tivoli AEF is used to dynamically customize the other Tivoli products by adding site-specific options or values. The Tivoli AEF can be used to add fields to a dialog, create custom attributes and methods for application resources, and create custom icons and bitmaps. It should be noted that even though the AEF is able to extend the capabilities of the other Tivoli products, it does not change their primary function.

- *(TMF.0063: CAT II) The TMR administrator will restrict access and use of the Tivoli AEF to IAM documented authorized personnel.*

- *(TMF.0064: CAT II) The IAO will ensure all installations and updates to the Tivoli AEF are restricted to the SA, the TMR administrator and IAM documented authorized personnel.*

B.2.11.2 Tivoli Event Integration Facility (EIF)

The Tivoli EIF is a toolkit that can be used to map events from a product resource, or component into a format compatible with Tivoli Enterprise Console and develop additional adapters that are tailored to a specific network environment. Event adapters are used by Tivoli to monitor managed resources and send events to the TEC or other products such as Managed Objects. The Tivoli EIF can be used to create event listeners that receive events. As a result, event listeners can be placed in a TMR where there is a need to distribute events to other management applications. Additionally, the Tivoli EIF can be used to filter events reducing event traffic on the network and the event server.

- *(TMF.0065: CAT II) The TMR administrator will restrict access and use of the Tivoli EIF to IAM documented authorized personnel.*

- *(TMF.0066: CAT II) The IAO will ensure all installations and updates to the Tivoli EIF are restricted to the SA, the TMR administrator and IAM documented authorized personnel.*

B.2.11.3 Tivoli Application Development Environment (ADE)

The Tivoli ADE is used to design and develop applications for distributed object systems. The Tivoli ADE contains programming tools that can be used for creating new custom management applications on top of the Tivoli Management Framework.

- *(TMF.0067: CAT II) The TMR administrator will limit access and use of the Tivoli ADE to IAM documented authorized personnel.*

- *(TMF.0068: CAT II) The IAO will ensure all installations and updates to the Tivoli ADE are restricted to the SA, the TMR administrator and IAM documented authorized personnel.*

B.3 Tivoli Enterprise Console (TEC)

B.3.1 Overview

TEC is a Tivoli product designed to provide the performance monitoring and automated problem management of the TME. Tivoli administrators are able to view, manage and administer TME resources and the event monitors (adapters). TEC enables administrators to create, distribute and implement new adapters as new resources are added to the TME.

When an event occurs on a managed resource, the TEC adapter captures information about the event, reformats the information and sends it to the event server for processing. Events may be discarded, or acted upon automatically based on rules that have been preprogrammed into TEC. Whether or not an automated response is required, TEC displays the information on the TEC console so that TEC administrators can monitor activity and respond to events as needed.

TEC can be installed in one of two ways, either through the TMF SIS or manually via shells and scripts provided by Tivoli.

- *(TEC.0001: CAT II) The IAM will ensure a current TEC architecture / configuration document exists.*

- *(TEC.0002: CAT II) The TMR administrator and SA will install the TEC product either using the TMF SIS or approved vendor-supplied scripts.*

- *(TEC.0003: CAT II) The TMR administrator and SA will remove unauthorized copies of the TEC product, such as old release levels, from the Tivoli Enterprise.*

- *(TEC.0004: CAT II) The SA and TMR administrator will restrict the TEC software from unauthorized update and access.*

- *(TEC.0005: CAT II) The SAs and TMR administrator will maintain currently supported Tivoli software on all platforms within the TME.*

- *(TEC.0006: CAT II) The IAM will ensure all systems, which host Tivoli software, are configured in accordance with the appropriate STIG.*

- *(TEC.0007: CAT II) The Tivoli Administrators or platform SAs will apply all security related patches to all TEC platforms.*

- *(TEC.0008: CAT III) The IAO will ensure a comprehensive set of procedures is documented and implemented to test all patches, upgrades, and new applications prior to deployment.*

- *(TEC.0009: CAT III) The IAM will ensure a contingency processing plan exists for the TEC servers, database, applications and adapters in the TME.*

- *(TEC.0010: CAT II) The SA and TMR administrator will ensure the TEC event database and server files are backed up as part of the regularly scheduled backup process.*

- *(TEC.0011: CAT III) The TMR administrator, TEC administrator and Tivoli administrators will maintain documentation describing the procedures necessary to perform a trusted recovery of the TEC to include the event server, database, adapter files, software and configuration files.*

B.3.2 Components

TEC is composed of a group of components designed to perform specific functions and work in conjunction with the TMF software. The following subsections describe the components, and security considerations.

B.3.2.1 Event Adapters

An event adapter is a process (program) that is used to monitor and collect information about events that occur with respect to TME resources. Some of the types of resources that can be monitored by event adapters are: operating systems, databases, applications and networks. Event adapters not only collect information about resource events in the TME, but also reformat the data and send the data to the event server for processing. Corrupted adapters could impact the TEC's ability to automatically respond to a potential enterprise problem or impact the information provided by the adapter.

There are two types of event adapters, TME event adapters and non-TME event adapters. The difference between the two is where they are loaded and how they transmit the information back to the event server. TME adapters run on systems that are supported by the TMF and send the information to the event server using TMF services. Non-TME event adapters run on systems that are not supported by the TMF and send the information to the event server using standard communication protocols.

Non-TME adapters and managed nodes, that are running adapters, send their event information directly to the event server. Endpoints, that are running adapters, send their event information to the TEC gateway, which forwards the information to the event server. Some additional functions that can be performed by event adapters are: checking files at configurable intervals and polling system resources or system condition at predetermined intervals.

- *(TEC.0012: CAT II) The IAM will ensure the roles, authorizations and permissions necessary for the creation, distribution and implementation of TME endpoint adapters, TME managed node adapters, and non-TME adapters are limited to the TMR administrator, the TEC administrator and IAM documented authorized personnel.*

- *(TEC.0013: CAT II) The SA will limit the access and update authority of the adapter files to the TMR administrator, TEC administrator and IAM documented authorized personnel.*

B.3.2.2 Event Server

The TEC event server is responsible for the centralized processing of all events collected by the adapters in a TME. The TEC event server consists of five daemons that run on the event server host. The event server must be installed on a managed node and only one may exist in each TMR of a TME. As events are received from adapters, the event server creates an entry in the Tivoli event database and also evaluates each event against predefined sets of rules to determine if an automatic response is necessary or the information is to be discarded. Automatic responses free TEC administrators from addressing non-problem situations regarding TME resources.

If more event servers are needed in a TME, they can be set up in a hierarchy by establishing the communications and the exchanging of data between each TMR in the TME. In a TME where each TMR supports its own TEC event server, one TEC event server may act as a backup for the other in case of network or TEC event server failures. The event adapters are able to automatically reroute their events to an available secondary TEC event server based on the adapter's configuration file. The software and files utilized by the event server require careful security consideration, because of the processing support of the event server. Normal platform security mechanisms, such as file permissions, are used to protect the software and files.

- *(TEC.0014: CAT II) The IAO will ensure the TEC event server is located in a controlled area accessible by only IAM documented authorized personnel.*

- *(TEC.0015: CAT II) The IAM will ensure the TMR administrator has configured the TEC event server to use only authorized ports and protocols in accordance with the Network STIG and DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) and the associated Ports, Protocols, and Services (PPS) Assurance Category Assignments List.*

B.3.2.3 Event Console

The event console is a GUI that enables TEC administrators and operators to monitor and respond to events in a TME. There may be multiple TEC event consoles in a TME. TEC event consoles are also used to run automated tasks, which are executed when predetermined types of events are received from the adapters. There are two versions of TEC event consoles that may exist in a TME; the Java version and the Web version.

The Java version enables TEC administrators to perform configuration tasks, start Tivoli NetView functions, run local automated tasks, and monitor events. Operators are also able to use the Java version to start Tivoli NetView functions, run local automated tasks, and manage events.

The Web version can only be used to perform event monitoring by both the TEC administrators and operators. In order for the Web console to be utilized, WebSphere Application Server (WAS), Version 5.0 Base Edition must be installed in a dedicated WAS environment. Secure

Socket Layer (SSL) is used to secure communications between web consoles and WAS. By default, the web console is not configured to operate in SSL mode. In order for SSL to be used, it must be activated through WAS configuration. Access to the event consoles is controlled through platform security and roles assigned to the administrator or operator. Failure to secure the communications between the web consoles and WAS could open up the enterprise to a Man-in-the-Middle attack.

- *(TEC.0016: CAT II) The IAO will ensure all event consoles are located in controlled areas accessible only by IAM documented authorized personnel.*

- *(TEC.0017: CAT II) The IAM will ensure the Web Administrator restricts all TEC web console access via platform access security authorizations and web server security manager policies.*

- *(TEC.0018: CAT II) The IAM will ensure the web Administrator has activated SSL in the WAS configuration file.*

- *(TEC.0019: CAT II) The IAO will ensure the WAS server is located in a controlled area accessible to IAM documented authorized personnel and implemented in accordance with the guidelines as specified in the platform and Web Server STIGs.*

- *(TMF.0020: CAT II) Remote access for TEC administrators will employ at a minimum:*

  - Session security measures such as a VPN configured in non-tunnel (blocking) mode and to allow only authorized traffic;

  - A process that creates an audit log for each remote session

B.3.2.4 User Interface Server (UI)

The UI server, ***tec_ui_server,*** is responsible for providing communication services between the event consoles, the event server and the event database. The UI server provides transaction locking during event console status updates, thus preventing multiple event consoles from responding to the same event. In addition, it automatically updates the status of events on all event consoles by forwarding the event changes from the event consoles to the dispatch engine of the event server, which sends the changes to the event database.

Only one instance of a UI server may exist in a TMR and because it is not part of the event server, it can be installed on any managed node in a TMR. A corrupted UI server could potentially impact the locking and unlocking of consoles during status updates and the information sent to the event database. In the event of a UI server failure, all error messages are written to the UI server log file. In order to recover information, the UI server's log file must be controlled through standard platform security mechanisms. In addition, file must be backed up in order to resolve potential problems.

The UI server provides a set of commands that enable operators to change any event attribute, list events in a specific event group, and display a message on the operator's desktop. The Tivoli documentation for TEC should be consulted for specific commands and their capabilities. In order for an administrator or operator to utilize the commands, the administrator or operator must be authorized on the local platform and through the assignment of Tivoli roles. Failure to secure the TEC commands related to the UI server could significantly impact TMR confidentiality of the data, the integrity of the environment and the availability of the consoles.

- *(TEC.0021: CAT II) The IAO will ensure the UI server is located in a controlled area accessible only by IAM documented authorized personnel.*

- *(TEC.0022: CAT II) The SA, TMR administrator, and TEC administrator will limit access and updates of the UI server files to IAM documented authorized personnel.*

- *(TEC.0023: CAT II) The SA and TMR administrator will restrict usage of UI server commands to the TEC administrator and IAM documented authorized personnel.*

- *(TEC.0024: CAT II) The IAM will ensure the TMR administrator, and SA has enabled encryption between the UI server and the event server. NIST FIPS 140-2 validated cryptography is used to implement encryption (e.g., AES, 3DES), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512) and that newer standards is applied as they become available.*

B.3.2.5 Adapter Configuration Facility (ACF)

The ACF is a profile-based application that enables administrators to configure and distribute TME adapters using a GUI. As mentioned previously, adapters are processes that collect event information about TME resources. Because they are generic processes, they require configuration files and configuration profiles to provide specific details about the resources, event types, methods for collecting the data, the format of the event information, and the final disposition of the information once it has been collected.

TEC administrators use the ACF to create and manipulate profiles for adapters, set configuration options and distribute them. Adapters can then be distributed to the profile's subscribers by either using the menu options of the ACF GUI, or by dragging and dropping the profiles to the appropriate profile manager. TEC administrators require specific roles to perform these types of functions.

- *(TEC.0025: CAT II) The TMR administrator, TEC administrator and SA will restrict access to the ACF via platform security requirements and Tivoli roles.*

- *(TEC.0026: CAT II) The TMR administrator will limit the creation, distribution and installation of profiles to the TEC administrator and IAM documented authorized personnel via Tivoli authorization roles.*

B.3.2.7 NetView Server

The Tivoli NetView server is a program, which is responsible for performing network management functions. The NetView server uses Simple Network Management Protocol (SNMP) to discover, monitor, and configure TCP/IP networks. In a TME, the NetView server can only be installed on Unix operating system (IBM AIX and Sun Solaris) managed nodes. In a non-Tivoli environment the NetView server program can be installed on Solaris, Linux, zLinux, AIX, and Windows operating systems.

The NetView server is able to communicate with the event server using either Tivoli-based communication or non-Tivoli-based (socket-based) communication. For Tivoli-based communication to occur, an endpoint must be installed on the computer where the NetView server is installed and a TEC gateway must exist between the NetView server and the event server. Even though there can be multiple endpoints on a single computer, that are connected to different gateways, the NetView server forwards events to only one event server at a time. In addition, the NetView server requires that an SNMP agent be installed. The NetView server is manually configured in a Tivoli environment, thus requiring normal platform security authorization and the Tivoli roles necessary to perform this function. Failure to secure the NetView server files could impact the administrator's ability to respond to network problems and allow intruder access, thus harming the integrity of the overall enterprise.

- *(TEC.0027: CAT II) The IAM will ensure the Tivoli NetView Server is located in controlled areas accessible to IAM documented authorized personnel.*

- *(TEC.0028: CAT II) The IAM will ensure access and updates to the Tivoli NetView Server software is restricted to the SA, TMR administrator and IAM documented authorized personnel.*

- *(TEC.0029: CAT II) The IAM will ensure the SA and TMR administrator have configured the TEC event server to use only authorized ports and protocols in accordance with the Network STIG and DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) and the associated Ports, Protocols, and Services (PPS) Assurance Category Assignments List.*

B.3.2.8 NetView Web Console

The Tivoli NetView Web console is a Java-based GUI that enables TEC operators to view network topology, obtain diagnostic information, and perform network troubleshooting and problem resolution. The NetView Web console is installed automatically when the NetView server is installed. For the NetView Web console to work, it must be installed on the same computer as the event console (Java version), which can only be a non-Tivoli environment. Console location, access and file control are key areas which must be protected in order minimize risk.

- *(TEC.0030: CAT II) The NetView Web Console is located in a controlled area accessible to IAM documented authorized personnel.*

- *(TEC.0031: CAT II) The TMR administrator and SA will restrict access and use of the NetView Web Console to IAM documented authorized personnel via platform access authorizations and Tivoli roles.*

B.3.2.9 NetView Native Console

The Tivoli NetView native console is an X/Motif-based (UNIX) or MFC-based (Windows) GUI that enables administrators to configure the NetView server. It also provides the same type of operator functionality as the Tivoli NetView Web console. The Tivoli NetView native console is automatically installed during the Tivoli NetView server installation. The native NetView console supports customization of the menu structure using Application Registration Files (ARF). The ARF files enable the addition of menu items to the menu bar. Careful consideration must be given to the protection of the ARF files and the authorization roles necessary to access the NetView native console.

- *(TEC.0032: CAT II) The IAM will ensure the SA and TMR administrator limits access to the NetView Native console through Tivoli roles and platform security.*

- *(TEC.0033: CAT II) The TMR administrator and the SA will limit ARF file creation, maintenance, and implementation via authorization roles to IAM documented authorized personnel.*

B.3.3 Tivoli Event Database

The Tivoli Event database is used by TEC to store information about events. The TEC event database is an external RDBMS in that it can be Oracle, Informix, DB2 and Sybase or Microsoft SQL server. In either case, the event database is comprised of two main areas, the reception log, ***tec_t_evt_rec_log,*** and event repository, ***tec_t_task_rep***. The reception log is used to track information about events that are received by the reception process of the event server. The event repository is used to store the results of the execution of tasks that are run as a result of receiving an event.

It should be noted that RIM supplies TEC and the other applications with the Application Program Interface (API) necessary for retrieving and storing data. RIM also converts data into the format of the appropriate database type. RIM is controlled by the TMF roles: ***rim_view*** and ***rim_ update***. Anyone, with the appropriate ***rim_**** access role can access the event database without having to be defined to the database and granted access to database resources. This could present a potential corruption problem if the granting of ***rim*** authorization roles is not controlled. A corrupted TEC event database could severely impact the integrity of the reporting and support capabilities of TEC.

- *(TEC.0034: CAT II) The IAO will ensure the TEC database is restricted from unauthorized access and update in accordance with the Database STIG.*

- *(TEC.0035: CAT II) The IAO will ensure the TEC database is included as part of the regularly scheduled backup process.*

- *(TEC.0036: CAT II) The IAO will ensure RIM authorization roles are limited to the TEC administrator and IAM documented authorized personnel.*

B.3.4 Tivoli Enterprise Console Gateway

The TEC console gateway is designed to receive events from TME adapters and non-TME adapters, filter them, and pass the information to the event server for processing. When the TEC gateway is initiated it establishes a connection-oriented service connection to the event server and continues to use it for passing all event information to the event server.

The TEC gateway is comprised of two programs, ***tec_gateway*** and ***tec_gwr***. The ***tec_gateway*** program processes events from TME adapters. The ***tec_gwr*** program, which is an endpoint adapter, receives events from non-TME adapters and sends them to the ***tec_gateway*** program. In order for the TEC gateway to receive events from non-TME adapters, the configuration file of TEC gateway configuration file must be enabled. It should be noted that the configuration file for the TEC gateway is optional and does not exist on the managed node until an adapter configuration profile containing the gateway configuration information is distributed to the endpoint on that managed node. The TEC gateway uses default values unless modified and an adapter configuration profile containing the changed gateway configuration information is distributed. Whenever a value is not specified in the configuration file, the TEC gateway assumes the default specification.

Once the configuration file is enabled***, tec_gwr*** uses the LCF transport type to send events to the ***tec_gateway*** program. The TEC gateway forwards events to the event server and communicates with the event server using the Tivoli Event Integration Facility. The ***tec_gateway*** program and its adapter files for each endpoint operating system are installed as part of the ACF installation process on a managed node. The ACF must be installed on any managed node that is configured as a TEC gateway.

- *(TEC.0037: CAT II) The IAO will ensure the Tivoli Enterprise Console gateway is located in a controlled area accessible to IAM documented authorized personnel.*

- *(TEC.0038: CAT II) The SA and the TMR administrator will restrict access and updates to Tivoli Enterprise Console gateway files to IAM documented authorized personnel.*

- *(TEC.0039: CAT II) The IAM will ensure the SA and the TMR administrator have implemented NIST FIPS 140-2 validated cryptography (e.g., AES, 3DES), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512) communication between the Tivoli Enterprise Console gateway and the event server and that newer standards are applied as they become available.*

- *(TEC.0040: CAT II) The IAO will ensure the Tivoli Enterprise Console gateway is configured to use only authorized ports and protocols in accordance with the Network STIG and DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) and the associated Ports, Protocols, and Services (PPS) Assurance Category Assignments List.*

B.3.5 ACF Authorization Roles

Authorization roles defined within the TMF provide role based access control over functions in the Tivoli products. A Tivoli administrator must be assigned the associated roles to be permitted to perform specific product functions. Authorization roles of *senior* or *super* enable a broad range of TEC administrator capabilities such as: assigning administrative roles for the event server, configuring event viewer preferences, assigning event group roles, deleting events, acknowledging and closing events. The capabilities vary based on the context of use and actual job responsibilities. If an authorization role is added to a Tivoli administrator after the operator starts the event console, the authorization role does not take affect until the event console is restarted. Additionally, each operator must be defined as a Tivoli administrator with the appropriate authorization roles before the operator can be assigned to an event console.

In order for administrators to utilize the ACF, they must be assigned ACF authorization roles. Since the ACF controls the creation, editing and distribution of profile policy, careful consideration must be given to ACF authorization roles.

- *(TEC.0041: CAT II) The IAO will ensure the authorization of TEC roles is limited to the TMR administrator and IAM documented authorized personnel.*

B.3.6 Event Classes

Event classes are designed to serve as an agreement between adapters and the event server. They provide the guidelines for the type of information adapters send to the event server for a given event. Event class definition must have a unique name. Event class definitions define each possible event type that can be received at the event server. When a new adapter is created, the types of events that the adapter can send to the event server is defined in a *baroc* file and loaded on the event server. Multiple *baroc* files can exist on an event server. The creation of *baroc* files requires specific Tivoli authorizations and the protection of the files depends on the platform security mechanisms, such as file permissions.

Event classes are organized in a hierarchy with the top of the hierarchy being the base event class named EVENT. Event classes can be further sub-divided into subclasses that provide for a more detailed set of rules for breaking down event information. Event classes are defined in event class definition files. The base event class definition file *root.baroc* is located in the *$BINDIR/TME/TEC/default_rb/TEC_CLASSES* directory, as specified in the Object Permissions section. Other event classes are subclasses of the base event class.

- *(TEC.0042: CAT II) The TMR administrator will limit the creation, distribution and installation of baroc files to the TEC administrator and IAM documented authorized personnel via Tivoli authorization roles.*

- *(TEC.0043: CAT II) The SA will limit access and updates to baroc files in accordance with the minimal file permissions as specified in the Object Permissions section.*

- *(TEC.0044: CAT II) The IAO will ensure the distribution of adapters and event class files is limited to the TMR Administrator, and IAM documented authorized personnel.*

B.3.7 TEC Rules

A TEC rule is a construct that specifies the type of action to be performed when specific events are received. Rules are written in a high-level language called the rule language. The rule language provides a simplified interface to the Prolog programming language, which is the language used internally by the rule engine. Rules, which are in the rule language, are precompiled into Prolog source code, and then compiled into Prolog executable files.

As part of the rule language, a set of predefined predicates is provided by Tivoli. These predicates are frequently used actions in rules. A rule executes when the event under analysis has satisfied all of the conditions specified in the rule's event filter. An event filter can contain tests for an event class name and event attribute conditions. Careful consideration should be given to the assignment of the authorization roles necessary to create, compile and distribute TEC rules.

- *(TEC.0045: CAT II) The TMR administrator will restrict the creation, distribution and installation of TEC rules to the TEC administrator and IAM documented authorized personnel via Tivoli authorization roles.*

B.3.7.1 Rule Base Targets

Rule base targets are the actual rule bases used by rule engines to process events. The TEC event server is the master container from which rule base targets are created. When there is more than one rule engine managing events in the environment, the rule bases used by the rule engines in that environment are referred to as distributed rule bases.

In a distributed rule base environment, event classes and rules must be synchronized among all the rule engines. In order to keep these synchronized, all rule base development must be done with the TEC event server, which is the centralized point of control for managing a distributed rule base environment.

Rule base targets, after compilation of the rule base on the TEC event server, are located in the ***rule_base_directory*/.rbtargets/*target_name*** directories (note the leading period in the ***.rbtargets*** subdirectory name). The name for the rule base target used by the rule engine on TEC event server is ***EventServer***. The ***EventServer*** rule base target is automatically created in every rule base. Distributed event servers only need the rule base target directory structure starting from the ***target_name*** subdirectory for their use.

Because all rule base targets for a rule base use the same set of classes, all rule builder and **wrb** commands manipulate baroc files at the rule base level on the TEC event server. When the rule base is compiled, the event classes are replicated to the rule base targets defined in the rule base. The default rule base directory should never be changed because the default rule base contains default rules and default baroc files, which are necessary for each new rule base. If the rule base is changed, itmay become corrupted, thereby corrupting each newly created rule base. If the rule base is corrupt, it will not compile, and is thereby rendered useless. In the event that there is no valid rule base for the TEC, it will not start; the administrator must create a new directory for all new rule bases.

- *(TEC.0046: CAT II) The SA and TMR administrator will restrict use of the wrb commands to the TMR administrator, TEC administrator, and IAM documented authorized personnel via file permissions and Tivoli authorization roles.*

- *(TEC.0047: CAT II) The TMR administrator will restrict rule base creation and distribution to the TEC administrator and IAM documented authorized personnel*

- *(TEC.0048: CAT II) The IAM will ensure the SA and TMR administrator have restricted rule base target directory permissions in accordance with the Object Permissions section of this document.*

B.3.7.2 Rule Sets and Rule Packs

Rule sets are files that contain rules. Related rules are generally contained within a rule set. When a rule base is compiled, rule sets are replicated to those rule base targets that have specified which rule sets to import. When a rule engine is using a rule base, generally the rules are processed in the order defined within a rule set and within the order in which the rule sets were imported into the rule base target. The regular rule processing order can be altered based on certain predicates called from within rules. It should be noted that the order of rule sets defined for a rule base target is important, because it affects rule engine performance.

A default set of rule sets is provided by Tivoli with the default rule base. A default rule set for the Tivoli Availability Intermediate Manager is also included with the default rule base. Another way to initiate rule sets into a rule base target is with *rule packs*. Rule packs are a convenient way to package a group of rule sets so they can be imported into a rule base target in a single operation. Rule packs are used to combine a group of rule sets that are used in multiple rule base targets. When a rule base is compiled, those rule base targets that are defined to receive rule packs receive their rule pack contents, which are rule sets. Before rule sets and rule packs can be imported into rule base targets, they must first be imported into the rule base on the TEC event server.

B.3.8 Secondary Event Servers

One or more secondary event servers can be specified for an event adapter. A secondary event server is a backup event server that receives events when the TEC gateway cannot contact the adapter-specified event server. Secondary event servers are specified in the TEC gateway configuration file.

B.3.9 Supported Platforms

- *(TEC.0049: CAT II) The SA and TMR administrator will restrict the installation of the TEC software to supported platforms as documented by the vendor.*

B.3.10 TEC Files

The TEC software is installed into a series of Tivoli TEC directories on the TEC event server, the managed nodes, and the endpoints requiring adapters. As part of the installation process,

certain script system variables are set. The variables are used to make the installation flexible when dealing with different platforms. The Object Permissions section defines these variables as well as others, and cites their usage when applicable. It should be noted that for Unix platforms a $ will precede the variable and for Windows platforms a % sign will be used before and after the symbol.

- *(TEC.0050: CAT II) The IAM will ensure unauthorized directories/files, including expired releases of the TEC and TEC related product software, do not exist in the currently distributed TEC directories.*

- *(TEC.0051: CAT II) The SA will restrict the TEC directories from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in Appendix B.7 of this document.*

- *(TMF.0052: CAT II) The SA will remove all TEC installation files from the system upon successful completion of the installation process.*

- *(TEC.0053: CAT II) The SA will restrict the TEC directories on the secondary event servers from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TEC.0054: CAT II) The SA will restrict adapter files from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TEC.0055: CAT II) The SA will restrict the ACF and EIF directories from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TEC.0056: CAT II) The SA will restrict the CDS files from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TEC.0057: CAT II) The SA will restrict the TEC Gateway Configuration file from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TEC.0058: CAT II) The SA will restrict access to the subdirectories of the BINDIR directory, their subdirectories, and all files in those subdirectories on Windows Gateway systems is restricted in accordance with in the Object Permissions section and the Windows STIG.*

- *(TEC.0059: CAT II) The SA will restrict access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems in accordance with the Object Permissions section.*

- *(TEC.0060: CAT II) The SA will restrict access to the TEC adapter files in accordance with the Object Permissions section.*

B.4 IBM Tivoli Monitoring (Tivoli Monitoring)

B.4.1 Overview

Tivoli Monitoring is used to monitor distributed system's resources in a TME/TMR and provide availability management reporting. It accomplishes this by using resource models to identify performance data that is necessary for determining potential bottlenecks and problems. Resource models automatically collect performance data and process it based on predefined algorithms to determine whether a potential problem exists. Once the data is processed, it can be distributed to the Web Health console, to TEC, or a Tivoli desktop for administrator review and, if necessary, respond. Resource models can be either used as is or tailored to meet the needs of the environment.

Tivoli Monitoring can be installed either through the use of the TMF SIS or through installation shells and scripts. It should be noted that the Tivoli Monitoring components of the Tivoli Monitoring product are integrated into the TMF and other Tivoli products, such as TEC. Tivoli Monitoring was originally known as Tivoli Distributed Monitoring (Advanced Edition).

- *(TIM.0001: CAT III) The IAO will ensure a current Tivoli Monitoring architecture / configuration document exists.*

- *(TIM.0002: CAT II) The IAO will ensure the Tivoli Monitoring software is restricted from unauthorized update and access.*

- *(TIM.0003: CAT II) The Tivoli Administrators or SAs will maintain currently supported Tivoli Monitoring software, where installed, on all platforms within the TME.*

- *(TIM.0004: CAT III) The Tivoli Administrators or platform SAs will install the Tivoli Monitoring product in the TME using either the TMF or authorized scripts.*

- *(TIM.0005: CAT I) The IAO will ensure unsupported Tivoli Monitoring software is removed or upgraded prior to a vendor no longer providing support.*

- *(TIM.0006: CAT III) The IAM will ensure the site has a formal migration plan for removing or upgrading DBMS systems prior to the date the vendor drops security patch support.*

- *(TIM.0007: CAT II) The IAO will ensure the creation, distribution and implementation of Tivoli Monitoring endpoint monitors or resource models are restricted to TMR administrators and IAM documented authorized personnel.*

- *(TIM.0008: CAT II) The Tivoli Administrator or platform SA will apply all security related patches.*

B.4.2 Components

Tivoli Monitoring is installed on the TMR server, gateways and endpoints within a TMR. The following subsections describe the components, where they are installed and security implications of each.

B.4.2.1 Tivoli Monitoring Base Component

The Tivoli Monitoring Base component is installed on the TMR server and all of the gateways, which have the endpoints to be monitored. The Tivoli Monitoring Base component consists of a GUI and a CLI. Since it is installed on the TMR server and the gateways, all of the functions and commands can be performed from either node.

Because the database, that contains the default resource models, is located and maintained on the TMR server, all commands that are entered from gateways are routed to the TMR server for execution. The Tivoli Monitoring Base component can also be configured to run the heartbeat function for all endpoints that are directly attached.

B.4.2.2 Web Health Console

The Web Health Console is an optional web-based GUI that enables administrators to view real time problems and status/health information. The Web Health Console can be accessed through an Internet browser connected through the TMR. The Web Health Console is able to be connected to any TMR server or managed node and used to display information about the endpoints found in that region. A numeric value is used to represent the health of the resource. It uses numbers between 100 (which represents perfect health) and zero to do so.

The Web Health Console can also be configured to work with historical data that already resides on the Tivoli Monitoring database. When events are sent to TEC from Tivoli Monitoring, TEC administrators are able to use the Web Health Console to perform an analysis of the problem that is occurring. Access and control of the Web Health Console is controlled through both platform security and through the TMR. Administrators must have valid userids, passwords and the appropriate roles to access the Web Health Console functions.

- *(TIM.0009: CAT II) The IAO will ensure the Web Health Consoles are installed on a platform that is secured in accordance with the appropriate platform STIGs.*

- *(TIM.0010: CAT II) The IAO will ensure the Web Health Consoles are located in an area, which is restricted from unauthorized access and protected by the local firewall.*

- *(TIM.0011: CAT II) The IAO will ensure Web Health Console remote access for Tivoli administrators will employ at a minimum:*

- Session security measures such as a VPN configured in non-tunnel (blocking) mode and to allow only authorized traffic.

NOTE: Remote access to any device must comply with the Network Infrastructure, and Secure Remote Computing STIGs.

- *(TIM.0012: CAT II) The TMR administrator will restrict Web Health Console usage by Policy Region.*

- *(TIM.0013: CAT II) The IAO will ensure encrypted communication sessions are used between the Web Health Console(s) and the supporting servers.*

  It should also be noted that as part of the Web Health Console installation three software components are installed:

  - WebSphere Application Server, Advanced Edition, Single Server, 4.0.2
  - IBM HTTP Server
  - Web Health Console

- *(TIM.0014: CAT II) The SA will implement all security requirements for Internet browsers in accordance with the Desktop Application STIG.*

- *(TIM.0015: CAT II) The IAO will ensure the WebSphere Application Server is secured in accordance with the Web Server and platform STIGs.*

B.4.2.3 Endpoint component

The endpoint component manages resources through the one or more resource models that are distributed to the endpoint. The endpoint component is automatically installed when a Tivoli Monitoring profile is distributed to the endpoint for the first time. In addition, a Tivoli management agent (TMA) is a requirement for installation in order for the endpoint component to function.

- *(TIM.0016: CAT II) The SA will restrict the endpoint component software in accordance with the minimal guidelines as specified in the Object Permissions section.*

B.4.2.4 Tivoli Business Systems Manager Adapter

The Tivoli Business Systems Manager Adapter component is responsible for forwarding discovery and status events to the Tivoli Business Systems Manager. The Adapter component is installed on all gateways in a TMR. The Adapter is responsible for sending events to Tivoli Business Systems Manager about resources that are managed by Tivoli Monitoring. When endpoint systems are discovered, the heartbeat function, which monitors basic system status of the endpoints, obtains health information about the resource and sends the information to the Tivoli Business Systems Manager, the TEC console or a Tivoli Monitoring Notice Group.

- *(TIM.0017: CAT II) The TMR administrator will limit heartbeat configuration updates to IAM documented authorized personnel.*
  - *A process that creates an audit log for each remote session.*
- *(TIM.0018: CAT II) The TMR administrator will limit access to the Tivoli Monitoring Notice Group to IAM documented authorized personnel.*

NOTE: The Tivoli Business Systems Manager Adapter cannot be installed on HP-UX gateways**.**

B.4.2.5 Gathering Historical Data Component

The Gathering Historical Data component is designed to support the Tivoli Monitoring Decision Support and Server Performance Predictions capabilities. Tivoli Monitoring resource models collect and process data, which it is provided to the Gathering Historical Data component. The Gathering Historical Data component then populates a database on the server where it is installed with the collected data. Every 24 hours, the data is aggregated and sent to the Tivoli Monitoring database. The aggregated data is sent to the Tivoli Monitoring database because the data is then available to Tivoli Monitoring for analysis.

- *(TIM.0019: CAT II) The SA will restrict the Gathering Historical database from unauthorized access update.*

- *(TIM.0020: CAT II) The SA will ensure the Gathering Historical database is added to the standard site backups.*

B.4.2.6 TME Data Warehouse Support Component

Tivoli Enterprise Data Warehouse Component, also known as the data collector, enables the storing of historical data in a RIM database and the generation of reports and graphs. The Tivoli Enterprise Data Warehouse Support Component is installed on the TMR server and all gateways.

It should be noted that the integration with Tivoli Data Warehouse is provided through: an ETL1 script responsible for extracting data from the centralized Tivoli Monitoring database and loading it to the Central Data Warehouse, and an ETL2 script responsible for creating a data-mart supporting a set of sample reports.

- *(TIM.0021: CAT II) The TMR administrator and SA will restrict ETL script creation and implementation to IAM documented authorized personnel.*

B.4.3 Authorization Roles

Authorization roles defined within the Management Framework provide role based access control over functions in the Tivoli products. A Tivoli administrator must be assigned the associated roles in order to perform specific product functions. Authorization roles are required for the installation of the product through the Software Installation Services of the TMF and

either through the Administrator group (Windows) or root (Unix). The Tivoli Monitoring documentation provides authorization roles associated with this product.

- *(TIM.0022: CAT II) The IAO will ensure the authorization of global TMR roles is limited to the TMR administrator and IAM documented authorized personnel.*
- *(TIM.0023: CAT II) The IAO will ensure the default Tivoli root administrator account is removed and a new Tivoli administrator root account, under a different name, is created.*

- *(TIM.0024: CAT II) The IAO will ensure the Tivoli administrators, who have been assigned administrative access to specific managed nodes, are not provided administrative access to the TMR server from any Tivoli managed node.*

B.4.4 Profiles and Profile Managers

A profile is a collection of Tivoli application information as it relates to users, software and hardware in the Tivoli environment. Tivoli Monitoring profiles define resource models and are used to distribute them to the subscribing endpoints. Profiles serve as templates or prototypes that enable Tivoli administrators to centrally manage and control data distribution to groups of systems. Profiles are represented as icons on the Tivoli administrator's desktops.

A profile manager is a container where individual profiles can be created and organized into groups of profiles. In addition, subscribers can be connected to them. Profile managers are created within a policy region. Profile managers control the distribution of profiles to subscribers. Subscribers to a profile manager can be in the same policy region as their profile manager or in other policy regions.

- *(TIM.0025: CAT III) The IAO will ensure the creation and maintenance of profiles and profile managers is limited to the TMR administrator and IAM documented authorized personnel.*

B.4.5 Resource Models

Resource models are used by Tivoli Monitoring to specify the performance resource data that is needed and how it is to be processed. The resource models specify one or more algorithms that assist in determining whether or not the resource is performing within expectations. Resource models are stored within profiles. It should be noted that resource models can be run as is provide by Tivoli or tailored to the environment.

- *(TMF.0026: CAT III) The IAO will ensure the creation and maintenance resource models are restricted to the TMR administrator and IAM documented authorized personnel.*

B.4.6 Commands

As stated earlier in this document, Tivoli Monitoring provides a CLI, which enables administrators to perform administrative and maintenance functions by entering commands in place of using pre-specified panels. In order for an administrator to perform these functions using commands, the administrator must be authorized at the local platform and through the

assignment of Tivoli roles. Inappropriate assignment of Tivoli roles could severely impact the administrator's ability to support the product.

- *(TIM.0027: CAT II) The IAO will ensure the Tivoli Monitoring commands are restricted from unauthorized access and usage through the assignment of permissions or group authorizations.*

B.4.7 Files

The Tivoli Monitoring software is installed in a directory structure that is subordinate to a logical directory known as the **BINDIR** directory. The physical implementation of the **BINDIR** directory is dependent on the platform type (e.g., MS Windows or UNIX) and site installation choices. Some of the Tivoli Monitoring software files are installed in directories that are shared with the TMF and TEC. These directories are protected through the specific TMF and TEC requirements elsewhere in this document. Requirements for the Tivoli Monitoring -specific directories are also addressed in the *Object Permissions* section. Tivoli Monitoring may be installed using the TMF or by using a script.

Tivoli files for Windows NT are, by default, stored under the ***\Tivoli*** directory on the root of the selected drive. Tivoli will also write install and other log files to ***%DBDIR%\tmp***.

- *(TIM.0028: CAT II) The IAO will ensure unauthorized directories/files, to include expired releases of Tivoli Monitoring software, do not exist in the currently distributed Tivoli directories.*

- *(TIM.0029: CAT II) The SA will restrict the Tivoli Monitoring directories from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in the Object Permissions section.*

- *(TIM.0030: CAT II) The IAO will ensure the Tivoli Monitoring installation files are removed from the system upon successful completion of the installation process.*

B.4.8 Platforms

- *(TIM.0031: CAT II) The SA and TMR administrator will restrict the installation of the Tivoli Monitoring software to supported platforms as documented by the vendor.*

NOTE: Some platforms have additional restrictions and the Tivoli Monitoring documentation should be consulted.

B.5 IBM Tivoli Configuration Manager

B.5.1 Overview

The IBM Tivoli Configuration Manager is a product of Tivoli, designed to provide inventory and configuration management in a TME. The product resulted from the merging of the Tivoli Inventory and Tivoli Software Distribution products. Tivoli administrators using the IBM Tivoli Configuration Manager are able to perform asset scanning and reporting, change control, software distribution, and patch management in a TME.

In a TME/TMR, the TMF software is the base infrastructure onto which all other Tivoli application products are integrated. The TMF provides a standardized format and approach to managing and administrating the components of the TME. In addition, the TMF provides a role based security structure, which compliments the security of the platforms on which the software resides. As Tivoli application products are integrated onto the TMF, not only is additional functionality realized but also the role-based security is enhanced. Many of the activities performed by administrators are not only controlled by the roles assigned them, but also through the grouping of subscribers, (desktops, users and devices), into Policy Regions. Once subscribers are grouped into Policy Regions, administrators are able to use policies to perform actions on the subscribers. This is referred to as management by subscription.

The IBM Tivoli Configuration Manager benefits from this by making use of the already existing structure and security that has been put in place. In addition, because the TMF provides the base support, the product can be installed using either the Tivoli scripts provided by the vendor or through the TMF SIS.

- *(TCM.0001: CAT II) The IAM will ensure a current IBM Tivoli Configuration Manager architecture / configuration document exists.*

- *(TCM.0002: CAT II) The TMR administrator and SA will install the IBM Tivoli Configuration Manager product either using the TMF SIS or approved vendor-supplied scripts.*

- *(TCM.0003: CAT II) The TMR administrator and SA will remove unauthorized copies of the IBM Tivoli Configuration Manager product, including old release levels, in the TME.*

- *(TCM.0004: CAT II) The TMR administrator and SA will limit the IBM Tivoli Configuration Manager software from unauthorized update and access.*

- *(TCM.0005: CAT III) The IAM will ensure a contingency processing plan exists for the IBM Tivoli Configuration Manager servers, databases/repositories, applications and files.*

- *(TMR.0006: CAT III) The TMR administrator will maintain documentation describing the procedures necessary to perform a trusted recovery of the IBM Tivoli Configuration Manager product to include the servers, databases/repositories, files, software and configuration files.*

B.5.2 Components

The IBM Tivoli Configuration Manager consists of two main components: software distribution and inventory components. The other components and services have been implemented in support of the functionality provided by the main two. The IBM Tivoli Configuration Manager software is installed on the TMR server, gateways and endpoints within a TMR. The following subsections describe the components, where they are installed, and security implications of each.

B.5.2.1 Software Distribution

The Software Distribution component is designed to enable Tivoli administrators to install, configure, and update platform software and applications remotely. The software distribution component must be installed on the TMR server and can be installed on additional managed nodes, as needed. This component is comprised of a series of elements that support the creation, alteration, and distribution of software packages. Tivoli refers to software packages as sets of instructions, which are performed on the platform to install and remove software. The Software Distribution component utilizes SCS and MDist, like the TMF, to distribute software packages across the TME.

Some additional subcomponents of the Software Distribution component, such as the Software Package Editor, provide administrators with the ability to create and maintain software packages. In addition, the Web Interface plug-in enables many of the operations that are performed by the Software Distribution component to access the web server.

In order to store data, such as software packages, the Software Distribution component provides the capability to create the repository. The corruption of any of the elements, the software package repository, or the software packages could severely impact the integrity and availability of the resources in the TME.

- *(TCM.0007: CAT II) The TMR administrator will limit the roles, authorizations and permissions necessary for the creation, distribution and implementation of software packages to IAM documented authorized personnel.*

- *(TCM.0008: CAT II) The SA and TMR administrator will limit access and update authority of the Software Package Editor to IAM documented authorized personnel.*

B.5.2.2 Inventory

The Inventory component is designed to enable the collection of asset information and the ability to use the information to manage the configurations of the hardware and software in the TME. It also provides Tivoli administrators with the ability to perform reporting on the components in the TME.

The Inventory component uses profiles (inventory profiles) to provide information about the type of information that is to be obtained by the scans. Files and directories are examples of the type of information obtained. In addition, the inventory component provides the schema for the configuration repository, the RIM host for communication with the RDBMS that holds the

configuration information, the data handler which sends the data to the configuration repository, and the collectors (also known as repeater sites) that forward the data to the data handler.

The Inventory component must be installed on a TMR server and can be installed on other managed nodes as needed. It should be noted that wherever the Inventory component is installed, the Scalable Collection Service (SCS) must also be installed. The SCS is responsible for managing the collection of data from the endpoint, and the transmission of the data through the repeater hierarchy, to the RDBMS.

- *(TCM.0009: CAT II) The IAO will ensure the creation and maintenance of inventory profiles and profile managers is limited to the TMR administrator and IAM documented authorized personnel.*

B.5.2.3 Activity Planner

The Activity Planner component enables the creation, scheduling, and deployment of activity plans. In addition, the Activity Planner enables the monitoring of activity plans while they are being performed. Activity plans are tasks that are performed on targets and sets of targets. In order for the Activity Planner component to accomplish these functions, it relies on two subcomponents, the Activity Plan Editor and the Activity Plan Monitor to accomplish these functions.

The Activity Planner component must be installed on the TMR server. It may also be installed on other managed nodes in a TMR depending on whether the Activity Planner administrative interface and Activity Planner commands are used. Because activity plans define the types of inventory and software distribution activities that are to be performed, access to the interface and control of activity plans should be restricted.

- *(TCM.0010: CAT II) The IAO will ensure the creation and maintenance of activity plans is limited to the TMR administrator and IAM documented authorized personnel.*

- *(TCM.0011: CAT II) The IAO will ensure access to the Activity Planner administrative interface is limited to the TMR administrator and IAM documented authorized personnel.*

- *(TCM.0012: CAT II) The IAO will ensure access to the Activity Planner commands is limited to the TMR administrator and IAM documented authorized personnel.*

B.5.2.4 Change Manager

The Change Manager service works in conjunction with the Activity Planner to support software distribution, inventory control and change management. The Change Manager uses reference models to manage the resources in a network. Reference models are used to associate the hardware and software configurations with the subscribers, (devices, workstations and users). Reference models are created and updated using the Change Manager administrative interface.

The Change Manager must be installed on a TMR server, and on managed nodes where the Change Manager administrative interface is to be run.

- *(TCM.0013: CAT II) The IAO will ensure the creation and maintenance of reference models is limited to the TMR administrator and IAM documented authorized personnel.*

B.5.2.5 Resource Manager

The Resource Manager is a deployment service that extends a TMR from a three tier architecture, (TMR server, gateways and endpoints), to a four tier architecture. This is accomplished by allowing the inclusion of pervasive devices. The Resource Manager is installed on the TMR server and on gateways in a TMR. It can be used with the Software Distribution, Inventory, and Web Gateway components, to add or remove pervasive devices and provide access to devices for software distribution and inventory control.

The Resource Manager maintains a master database. Because Tivoli allows for the creation of resource manager gateways, each resource manager gateway supports its own database with is subordinate to the master database. Whenever changes occur to resources in the TME the databases notify each other of any changes, thus ensuring current information is maintained about the resources in the TME.

- *(TCM.0014: CAT II) The IAO will ensure pervasive device access to the IBM Tivoli Configuration Manager is limited to IAM documented authorized personnel.*

- *(TCM.0015: CAT II) The Tivoli administrators will ensure pervasive device software is configured so that NIST FIPS 140-2 validated cryptography is used to implement encryption (e.g., AES, 3DES); key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512) and newer standards are applied as they become available.*

- *(TCM.0016: CAT II) The IAO will restrict access and use of pervasive device software libraries to IAM documented authorized personnel.*

B.5.2.6 Web Interface

The Web Interface service is a browser-based tool designed to support the installation and management of Tivoli Configuration Manager Web objects. The Web Interface is composed of two sub components, a server component and an endpoint component. The server component is responsible for pushing software packages, inventory profiles, and reference models from the TMR to the Web Gateway component from where endpoint component pulls them. The Web Gateway component is capable of storing the reference models temporarily.

Because the Software Distribution component, Inventory component, and Change Manager service have a Java plug-in registered with the Web Interface, they are able to use the Web Interface to perform many of the functions of inventory control and software installation management. Unauthorized access through this component could result in the release of configuration information and the introduction of corrupted software packages.

- *(TCM.0017: CAT II) The SA will install at a minimum Java 1.3.0 in support of the IBM Tivoli Configuration Manager.*

- *(TCM.0018: CAT II) The SA will ensure the httpserv.log and the httptran.log are included as part of the regularly scheduled site backups.*

B.5.2.7 Enterprise Directory Query Facility

The Enterprise Directory Query Facility service allows Tivoli administrators to use the information stored in TME directories. The Enterprise Directory Query Facility consists of directory query libraries and directory queries and must be installed on TMR server. The directory query libraries reside in policy regions and are created to contain directory queries. The directory queries are designed to enable Tivoli administrators to find information about the users or the workstations defined in the enterprise directory server.

It should be noted that this component relies on a preconfigured Lightweight Directory Access Protocol (LDAP) directory server.

Tivoli administrators are able to select a specific directory object, or container of directory objects, as subscribers for a reference model or an activity plan. Once they have been selected, the subscribers can be targets for software distributions or inventory scans.

- *(TCM.0019: CAT II) The IAO will ensure the creation, maintenance and deletion of directory query libraries and directory queries is limited to the TMR administrator and IAM documented authorized personnel.*

- *(TCM.0020: CAT II) The IAO will ensure the LDAP server is located in a controlled area, accessible by IAM documented authorized personnel.*

- *(TCM.0021: CAT II) The IAO will ensure the LDAP server is configured in accordance with the appropriate OS and Network STIGs.*

B.5.3 Authorization Roles

Authorization roles defined within the Management Framework provide role-based access control over functions in the Tivoli products. A Tivoli administrator must be assigned the associated roles to be permitted to perform specific product functions. Authorization roles are required for the installation of the product through Software Installation Services of the TMF and either through the Administrator group (Windows) or root (Unix). The IBM Tivoli Configuration Manager documentation provides authorization roles associated with this product.

- *(TCM.0022: CAT II) The IAO will ensure the authorization of TCM roles is limited to the TMR administrator and IAM documented authorized personnel.*

B.5.4 Repositories

In order to store data in an RDBMS, a repository must be created and loaded with the appropriate tablespaces and views. During the installation of the IBM Tivoli Configuration Manager scripts are executed to create databases, known as repositories. There can be one or more repositories depending on the planned component implementation. The following components utilize repositories/databases:

- Change Manager component - uses the ccm repository
- Inventory component - uses the inv_db database
- Resource Manager component - uses the inv_db database
- Software Distribution component - uses the inv_db database
- Activity Planner component - uses the planner repository
- Pristine Manager component - uses the pristine repository

Repositories are created when the *admin* and *schema* scripts, supplied by Tivoli, are executed. Based on the component, a default password and username is specified. Applications communicate with the RDBMS through RIM objects. When the IBM Tivoli Configuration Manager is installed, the required RIM objects are created on systems that become known as RIM hosts.

- *(TCM.0023: CAT II) The IAO will ensure the creation, maintenance and deletion of repositories is limited in accordance with the minimal specifications in the Object Permissions section and the appropriate platform STIGs.*

- *(TCM.0024: CAT II) The IAO will ensure passwords used by the RIM objects and the RDBMS comply with the Database STIG.*

- *(TCM.0025: CAT II) The IAO will ensure the creation, maintenance and deletion of RIM objects are limited to the TMR administrator and IAM documented authorized personnel.*

- *(TCM.0026: CAT II) The SA will ensure the repositories are included as part of the normal site backup process.*

B.5.5 Reference Models

Reference models are used by the Change Manager to distribute software across a TME. They represent the software and hardware requirements of different categories of users in an organization. Reference models are comprised of component models that are organized in a hierarchical structure. The root level defines requirements common to all users and the child models define additional requirements that apply only to a particular group of users. Target machines receive the distributions because they subscribe to a model. Target machines are referred to as subscribers.

- *(TCM.0027: CAT II) The IAO will ensure the creation, maintenance and deletion of reference models are restricted to the TMR administrator and IAM documented authorized personnel.*

B.5.6 Commands

As stated earlier in this document, the CLI enables administrators to perform administrative and maintenance functions by entering commands in place of using pre-specified panels. In order for an administrator to perform these functions using commands, the administrator must be authorized at the local platform level and through the assignment of Tivoli roles.

- *(TCM.0028: CAT II) The SA and TMR administrator will limit Tivoli commands from unauthorized access and usage through the assignment of permissions or group authorizations.*

B.5.7 Supported Platforms

- *(TCM.0029: CAT II) The SA and TMR administrator will restrict the installation of the Tivoli Monitoring software to supported platforms as documented by the vendor.*

NOTE: Some platforms have additional restrictions and the Tivoli Monitoring documentation should be consulted.

B.5.8 Pervasive Devices

Pervasive devices are small computing devices either mobile or embedded in all types of objects that can be interconnected to the Internet. One simple example of a pervasive device is a handheld Personal Digital Assistant (PDA). The Tivoli Inventory component is able to scan pervasive devices to obtain inventory information.

- *(TCM.0030: CAT II) The IAO will ensure pervasive device access is restricted in accordance with the Wireless and appropriate OS STIGs.*

- *(TCM.0031: CAT II) The SA and TMR administrator will ensure the pervasive device access is limited to IAM documented authorized personnel.*

B.5.9 Files

The IBM Tivoli Configuration Manager software is installed into a series of Tivoli TEC directories on the TEC event server, the managed nodes, and the endpoints requiring adapters. As part of the installation process, certain script system variables are set. The variables are used to make the installation flexible when dealing with different platforms. The Object Permissions section, defines these, and other variables, and cites their usage when applicable. It should be noted that for Unix platforms a $ will precede the variable and for Windows platforms a % sign will be used before and after the symbol.

- *(TCM.0032: CAT II) The SA and TMR administrator will ensure unauthorized directories/files, including expired releases of the IBM Tivoli Configuration Manager related product software, do not exist in the currently distributed IBM Tivoli Configuration Manager directories.*

- *(TCM.0033: CAT II) The SA will restrict the IBM Tivoli Configuration Manager directories from unauthorized access and updates, in accordance with the file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TCM.0034: CAT II) The SA and TMR administrator will remove IBM Tivoli Configuration Manager installation files from the system upon successful completion of the installation process.*

- *(TCM.0035: CAT II) The SA will restrict the IBM Tivoli Configuration Manager directories on the secondary event servers from unauthorized access and updates, in accordance with the file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TCM.0036: CAT II) The SA will restrict access to the subdirectories of the BINDIR directory, its subdirectories, and all files in those subdirectories on Windows Gateway systems in accordance with in the Object Permissions section and the Windows STIG.*

- *(TCM.0037: CAT II) The SA will restrict access to the ORACLE_HOME directory, its subdirectories, and all files in those directories on UNIX RIM Host and Windows RIM Host systems in accordance with in the Object Permissions section.*

B.6 IBM Tivoli Monitoring for Business Integration

B.6.1 Overview

The IBM Tivoli Monitoring for Business Integration software product, formerly referred to as Tivoli Manager for MQSeries, is designed to provide centralized management, administration and monitoring of WebSphereMQ resources and activity in a TME. Because the Tivoli Monitoring for Business Integration is integrated with multiple Tivoli software products, such benefits as authorization roles, consolidated event displays, event threshold monitoring, configuration backup and recovery and software distribution are realized.

In order for the Tivoli Monitoring for Business Integration software to be used to manage WebSphereMQ, it must be installed on the TMR server, the TEC Event server, each endpoint running WebSphereMQ resources (that are to be managed), and all gateways (for endpoint support). The product provides automated tasks, which enable administrators to define, change, start, stop and delete WebSphereMQ queue managers, queues, channels, and other resources.

In addition, Tivoli Monitoring for Business Integration provides event adapters specifically designed for the monitoring of WebSphereMQ activity, performance and potential problems. These event adapters collect event information from queue manager's event queues, reformat the information and send the data to the TEC event server for display and potential response. Automated responses may result by the TEC based on rule sets established for the different events.

- *(TMQ.0001: CAT III) The IAO will ensure a current Tivoli Monitoring for Business Integration architecture / configuration document exists.*

- *(TMQ.0002: CAT II) The IAO will ensure the Tivoli Monitoring for Business Integration software is restricted from unauthorized update and access.*

- *(TMQ.0003: CAT II) The Tivoli Administrators or SAs will maintain currently supported Tivoli Monitoring for Business Integration and WebSphereMQ software on all platforms that require it for usage, within the TME.*

- *(TMQ.0004: CAT III) The Tivoli Administrators or platform SAs will install the Tivoli Monitoring for Business Integration product in the TME either using the TMF or authorized scripts.*

- *(TMQ.0005: CAT I) The Tivoli Administrators or platform SAs will ensure unsupported Tivoli Monitoring for Business Integration software is removed or upgraded prior to a vendor no longer providing support.*

- *(TMQ.0006: CAT III) The IAM will ensure the site has a formal migration plan for removing or upgrading Tivoli Monitoring for Business Integration software prior to the date the vendor no longer provides security patch support.*

- *(TMQ.0007: CAT II) The IAO will ensure the creation, distribution and implementation of Tivoli Monitoring for Business Integration endpoint monitors and resource models is limited to TMR administrators and IAM documented authorized personnel.*

- *(TMQ.0008: CAT II) The Tivoli Administrators and/or platform SAs will apply all security related patches.*

B.6.2 Components

Tivoli Monitoring for Business Integration is installed on the TMR server, gateways and endpoints within a TMR. The following subsections describe the components, where they are installed and security implications of each.

B.6.2.1 WebSphereMQ Management Domain(s)

In a TME, where the Tivoli Monitoring for Business Integration software is used, all WebSphereMQ resources that are to be managed are defined and contained in a management domain. At least one management domain must exist in a TME. When a management domain is created, all the profile managers, task libraries, and other objects that belong to the management domain are loaded into the domain. The queue managers are not initially recognized. In order to discover the queue managers for the management domain, a discovery function is run which will create a queue manager object for each manager that is discovered. The label for a queue manager icon is set to qmgrname@hostname.

Additional management domains may be created if a larger number of WebSphereMQ resources exist in an enterprise. If additional management domains are created, multiple administrators may be required to monitor and manage the resources. In addition, because each management domain is implemented as a TME policy region, not only will each domain contain its own set of WebSphereMQ resources, profile managers, monitors, task libraries but may also have different authorizations established. Each management domain may be managed from a different Tivoli Desktop.

Before a queue manager or a queue manager icon is deleted from a Desktop, the queue manager must be unsubscribed from all profile managers to which it is subscribed. Doing this ensures that the queue manager is deleted from the Tivoli database. If an endpoint is to be deleted or moved to another gateway, the queue manager icon must be deleted and then the discovery function rerun.

- *(TMQ.0009: CAT II) The IAO will ensure the creation, maintenance and distribution of all WebSphereMQ resources and profiles are limited to the TMR administrator and IAM documented authorized personnel.*

- *(TMQ.0010: CAT II) The IAO will ensure the creation, maintenance and distribution of all Tivoli Monitoring for Business Integration tasks and task libraries are limited to the TMR administrator and IAM documented authorized personnel.*

B.6.2.2 Remote Administration

The Tivoli Monitoring for Business Integration remote administration facility enables WebSphereMQ commands to be issued to queue managers that do not reside on Tivoli managed nodes or endpoints. Commands may be entered either through the Tivoli Desktop or the Tivoli Business Systems Manager workstation.

- *(TMQ.0011: CAT II) The IAO will ensure all Tivoli Monitoring for Business Integration remote administration consoles are located on a platform is secured in accordance with the appropriate platform STIGs.*

- *(TMQ.0012: CAT II) The IAO will ensure all desktops accessing Tivoli Monitoring for Business Integration are located in an area, which is restricted from unauthorized access and protected by the local firewall.*

- *(TMQ.0013: CAT II) The IAO will ensure all desktops accessing Tivoli Monitoring for Business Integration employ at a minimum:*

  - *Session security measures such as a VPN configured in non-tunnel (blocking) mode and to allow only authorized traffic.*
  - *A process that creates an audit log for each remote session.*

NOTE: Remote access to any device must be in compliance with the Network Infrastructure and Secure Remote Computing STIGs.

- *(TMQ.0014: CAT II) The TMR administrator will restrict Tivoli Monitoring for Business Integration desktop usage by Policy Region.*

- *(TMQ.0015: CAT II) The platform SA will implement all security requirements for Internet browsers in accordance with the Desktop STIG.*

- *(TMQ.0016: CAT II) The IAO will ensure the WebSphere Application Server is secured in accordance with the Web Server and appropriate OS STIGs.*

B.6.2.3 Application Proxy

The Application Proxy is an extension of the Tivoli Framework that provides a common set of services that are used by Tivoli Monitoring for Business Integration. The Application Proxy is installed on the Tivoli server, Event server, each managed node running WebSphereMQ resources, and all gateways.

- *(TMQ.0017: CAT II) The platform SAs will restrict the endpoint component software in accordance with the minimal guidelines as specified in the Object Permissions section of this document.*

B.6.2.4 Tivoli Monitoring for Business Integration Tasks

The Tivoli Monitoring for Business Integration Utility Task library contains tasks that are used to perform common functions related to managing WebSphereMQ. The Tivoli Monitoring for Business Integration Utility Tasks library is located in the policy region assigned for managing WebSphereMQ. Most tasks provided in the Tivoli Monitoring for Business Integration task libraries are available on the pop-up menus on the Manager for MQSeries, the management domain, and the queue manager icons.

Most of the Tivoli Monitoring for Business Integration tasks can run from one region on task endpoints in an interconnected region. Task processing between two interconnected regions requires that the Tivoli Monitoring for Business Integration be installed on both regions and that the regions are interconnected in a two-way connection and share resources.

- *(TMQ.0018: CAT II) The TMR administrator will limit access, update, and execution of tasks from the Tivoli Monitoring for Business Integration Utility Tasks library to IAM documented authorized personnel.*

NOTE: The Tivoli Business Systems Manager Adapter cannot be installed on HP-UX gateways.

B.6.2.5 Tivoli Monitoring for Business Integration for OS/390

The Tivoli Monitoring for Business Integration for OS/390 allows sending MQSeries requests for information from a managed node to an OS/390 system for processing. It can request processing for a monitoring task on a remote OS/390 system. The Tivoli Monitoring for

Business Integration for OS/390 processes requests from a Tivoli Monitoring for Business Integration task or monitor that is sent to the MQSeries queue manager on the OS/390 system.

The Tivoli Business Systems Manager task server provides a channel for forwarding commands to Tivoli Monitoring for Business Integration and to receive responses after command execution. Command requests to the WebSphereMQ queue manager travel from the task server to Tivoli NetView for OS/390 for processing. Tivoli NetView for OS/390 routes the output back to the task server, which forwards the response to the requesting Tivoli Monitoring for Business Integration task or monitor.

Functions that the task server can request include running WebSphereMQ commands, issuing OS/390 commands, and discovering all occurrences of MQSeries queue managers on target OS/390 systems. Running the MQSeries event adapter for OS/390 and the Statistical Event Adapter on an OS/390 system enables events to flow from WebSphereMQ active queue managers on OS/390 systems to the event server.

- *(TMQ.0019: CAT II) The SA will restrict the Gathering Historical database from unauthorized access and update.*

- *(TMQ.0020: CAT II) The IAO will ensure the Gathering Historical database is included as part of the standard site backups.*

B.6.3 Authorization Roles

Authorization roles defined within the TMF provide role based access control over functions in the Tivoli products. A Tivoli administrator must be assigned the associated roles to be permitted to perform specific product functions. Authorization roles are required for the installation of the product through Software Installation Services of the TMF and either through the Administrator group (Windows) or root (Unix). The Tivoli Monitoring for Business Integration documentation provides authorization roles associated with this product.

- *(TMQ.0021: CAT II) The TMR administrator will limit global TMR authorization roles to the TMR administrator and IAM documented authorized personnel.*

- *(TMQ.0022: CAT II) The IAO will ensure Tivoli administrators, who are assigned administrative access to specific managed nodes, are not provided administrative access to the TMR server from any Tivoli managed node.*

B.6.4 Commands

As stated earlier in this document, Tivoli Monitoring for Business Integration provides a CLI, which enables administrators to perform administrative and maintenance functions by entering commands in place of using pre-specified panels. In order for an administrator to perform these functions using commands, the administrator must be authorized at the local platform level and through the assignment of Tivoli roles.

- *(TMQ.0023: CAT II) The IAO will ensure the Tivoli Monitoring for Business Integration commands are restricted from unauthorized access and usage through the assignment of permissions or group authorizations.*

- *(TMQ.0024: CAT II) The TMR administrator will limit the use of Tivoli commands to IAM documented authorized personnel.*

B.6.5 Files

The Tivoli Monitoring for Business Integration software is installed in a directory structure that is subordinate to a logical directory known as the BINDIR directory. The physical implementation of the BINDIR directory is dependent on the platform type (e.g., MS Windows or UNIX) and site installation choices. Some of the Tivoli Monitoring for Business Integration software files are installed in directories that are shared with the Management Framework. These directories are protected through the specific Management Framework requirements elsewhere in this document. Requirements for the Tivoli Monitoring for Business Integration specific directories are also addressed in the Object Permissions section.. Tivoli Monitoring for Business Integration may be installed using the TMF or by using a script.

Tivoli files for Windows NT are, by default, stored under the *\Tivoli* directory on the root of the selected drive for managed nodes and for endpoints, \program files\Tivoli.

- *(TMQ.0025: CAT II) The SA will ensure unauthorized directories/files, to include expired releases of Tivoli Monitoring for Business Integration software, do not exist in the currently distributed Tivoli directories.*

- *(TMQ.0026: CAT II) The SA will restrict the Tivoli Monitoring for Business Integration directories from unauthorized access and updates, in accordance with the minimal file permissions and group authorizations as specified in the Object Permissions section of this document.*

- *(TMQ.0027: CAT II) The IAO will ensure the Tivoli Monitoring for Business Integration install files are removed from the system upon successful completion of the installation process.*

B.6.6 Platforms

- *(TMQ.0028: CAT II) The SAs and TMR administrator will install the Tivoli Monitoring for Business Integration software to supported platforms as documented by the vendor.*

NOTE: Some platforms have additional restrictions and the Tivoli Monitoring documentation should be consulted.

B.7. Tivoli Component Object Permissions

B.7.1 Introduction

The Tivoli Components in this section are divided by Tivoli product. The sub-section number corresponds to the Appendix B section. For example, the sub-section B.7.2 is broken down as follows:

> **B.7** is the number of the Tivoli Component Object Permission section and the number **2** corresponds to Appendix **B.2**. UNIX and Windows platform specifics further subdivide each product. The use of symbolic variables may be used as part of paths names for flexibility purposes. Finally, in some cases, a Tivoli product may not run on a Windows platform and when that is the case, no table exists.

B.7.2 Tivoli Management Framework

B.7.2.1 UNIX File and Directory Permissions

The following system variables may be established during the installation and may be used as part of the paths in the table below:

- $BINDIR - the high level directory structure that holds the subordinate directories in which Tivoli software is installed

- $INTERP - the interpreter type, an OS-specific identifier that is used to separate files required to support different operating systems.

- $DBDIR - the high level directory structure on other managed nodes that holds the subordinate directory in which TMF database files.

- $LIBDIR – the high-level directory structure holds the library files.

- $MANPATH – the high level directory on other managed node holds the subordinate directory in which the manual pages are stored.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Management Framework	TMR Server, Managed Node RIM Host Gateway	**$DBDIR**	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	/usr/lib/X11/app-defaults	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**$BINDIR/**../	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server	**$BINDIR**/../client_bundle	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**$BINDIR**/../generic	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway, Endpoints	**$BINDIR**/../lcf_bundle	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway, Managed Node Endpoints	**$BINDIR**/../lcf_bundle.40	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**$BINDIR**	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**$BINDIR/**../../include	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**$BINDIR/**../../msg_cat	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**$BINDIR/**../../man	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**$BINDIR/**../../doc	[privileged]	[privileged]	755	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	/etc/Tivoli	[privileged]	[privileged]	755	B.2.8

B.7.2.2 Windows File and Directory Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- **%BINDIR%** - the high level directory structure that holds the subordinate directories in which Tivoli software is installed
- **%INTERP%** - the interpreter type, an OS-specific identifier that is used to separate files required to support different operating systems
- **%DBDIR%** - the high level directory structure on other managed nodes that holds the subordinate directory in which the TMF database software resides.
- **%SystemRoot%** - specifies the system root directory.
- **[Tivoli Users]** - a group containing accounts for non-administrative users of Tivoli
- **[Tivoli Admins]** – Policy RegionAdministrators/individual accounts or a group with responsibility for administration of Tivoli on the platform.

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Tivoli Management Framework	TMR Server, Managed Node RIM Host Gateway	**%DBDIR%**\..\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\lcf_bundle	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\lcf_bundle.40	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\client_bundle	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\generic	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\generic_unix	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\..\Tivoli\include	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Traverse / Execute	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%LIBDIR%**\..\lib	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.2.8

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%BINDIR%**\..\..\msg_cat	TMR Administrators SYSTEM [Tivoli Admins]	Full Control Full Control Full Control	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway, Endpoint	**%SystemRoot%**\system32\drivers\etc\Tivoli	TMR Administrators SYSTEM [Tivoli Admins]	Full Control Full Control Full Control	B.2.8
Tivoli Management Framework	TMR Server, Managed Node, Gateway	**%SystemRoot%**\system32\drivers\etc\tll.conf	TMR Administrators SYSTEM [Tivoli Admins]	Full Control Full Control Full Control	B.2.8
Tivoli Management Framework	Endpoint	**%SystemRoot%**\system32\	tmersrvd	Read Execute	B.2.8
Tivoli Management Framework	Endpoint	**%SystemRoot%**\temp\	tmersrvd	Read Execute	B.2.8

B.7.2 Windows Registry Permissions

Tivoli Product	Component	Registry Key	Account Assignment	Permissions	STIG Reference
Tivoli Management Framework	Server	HKEY_LOCAL_MACHINE\SOFTWARE \Tivoli\Platform key	TMR Administrators Policy Region Administrator SSO Platform SA Users	Full Control Execute Full Control Full Control Read	B.2.8

B.7.3 Tivoli Enterprise Console

B.7.3.1 Tivoli Enterprise Console Server

B.7.3.1.1 UNIX File Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- $BINDIR - the high level directory structure that holds the subordinate directories in which Tivoli software is installed.
- $DBDIR - the high level directory structure on other managed nodes that holds the subordinate directory in which Tivoli Enterprise Console database files.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Server	**$DBDIR**/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../generic_unix	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../../msg_cat	[privileged]	[privileged]	755	B.3.10

B.7.3.2 Tivoli Enterprise Console User Interface Server

B.7.3.2.1 UNIX File Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- $BINDIR - the high-level directory structure that holds the subordinate directories in which Tivoli software is installed.
- $DBDIR - the high level directory structure on other managed nodes that holds the subordinate directory in which Tivoli Enterprise Console database files.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Server	**$DBDIR**/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../	[privileged]	[privileged]	755	B.3.10

B.7.3.3 Tivoli Enterprise Console Java Console

B.7.3.3.1 UNIX File Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- $BINDIR - the high level directory structure that holds the subordinate directories in which Tivoli Enterprise Console Java software is installed.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Desktop	**$BINDIR**/../	[privileged]	[privileged]	755	B.3.10

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Desktop	**$BINDIR/..**/generic_unix/../	[privileged]	[privileged]	755	B.3.10

B.7.3.4 Tivoli Enterprise Console Sample Event Information

B.7.3.4.1 UNIX File Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- $BINDIR - the high level directory structure that holds the subordinate directories in which Tivoli Enterprise Console software is installed.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Desktop	**$BINDIR**/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Desktop	**$BINDIR**/../generic_unix/	[privileged]	[privileged]	755	B.3.10

B.7.3.5 ACF

B.7.3.5.1 UNIX File Permissions (Server)

The following system variables may be established during the installation and may be part of the paths in the table below.

- $BINDIR - the high level directory structure that holds the subordinate directories in which Tivoli Enterprise Console Java software is installed.

- $DBDIR - the high level directory structure on other managed nodes that holds the subordinate directory in which Tivoli ACF database files.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Server	**$DBDIR**/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$DBDIR**/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../generic_unix/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../../msg_cat/../	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$LIBDIR**	[privileged]	[privileged]	755	B.3.10

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Server	**$BINDIR**/../lcf_bundle/bin/ **$INTERP**	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$BINDIR**/../lcf_bundle/bin/ **$INTERP**/TME	[privileged]	[privileged]	755	B.3.10

B.7.3.5.2 Windows File and Directory Permissions

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Tivoli Enterprise Console	Server	%**BINDIR%**\..\lcf_bundle\bin**%INTERP%**	TMR Administrators Policy Region Administrator SSO Platform SA Users	Full Control Full Control Full Control Full Control Read & Execute	B.3.10
Tivoli Enterprise Console	Server	**%BINDIR%**\..\lcf_bundle\bin**%INTERP%** \TME\	TMR Administrators Policy Region Administrator SSO Platform SA Users	Full Control Full Control Full Control Full Control Read & Execute	B.3.10

B.7.3.5.3 UNIX File Permissions (Server)

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Tivoli Enterprise Console	Server	**$ORACLE_HOME**/	[privileged]	[privileged]	755	B.3.10
Tivoli Enterprise Console	Server	**$ORACLE_HOME**/bin	[privileged]	[privileged]	755	B.3.10

B.7.3.5.4 Windows File and Directory Permissions

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Tivoli Enterprise Console	Server	**%ORACLE_HOME%**\	TMR Administrators Policy Region Administrator SSO Platform SA Users	Full Control Full Control Full Control Full Control Read & Execute	B.3.10
Tivoli Enterprise Console	Server	**%ORACLE_HOME%**\bin	TMR Administrators Policy Region Administrator SSO Platform SA Users	Full Control Full Control Full Control Full Control Read & Execute	B.3.10

B.7.4 IBM Tivoli Monitoring

B.7.4.1 UNIX File and Directory Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- **$LCF_DATDIR -** the high level directory structure on endpoints that holds the subordinate directory in which the config file is stored.
- **$LCF_BINDIR -** the high level directory structure on endpoints that holds the subordinate directory in which software is installed.
- **$LCF_CATDIR -** the high level directory structure on endpoints that holds the subordinate directory in which message files are located.
- **$LCFROOT -** the high level root directory.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
ITM for Business Integration	TMR Server Gateways	**$LIBDIR**/../	[privileged]	[privileged]	755	B.4.7
ITM for Business Integration	Endpoints	**$LCF_DATDIR**/../../	[privileged]	[privileged]	755	B.4.7
ITM for Business Integration	Endpoints	**$LCF_BINDIR**/../	[privileged]	[privileged]	755	B.4.7
ITM for Business Integration	Endpoints	**$LCF_LIBDIR**/../	[privileged]	[privileged]	755	B.4.7
ITM for Business Integration	TMR Server Gateway Endpoints	**$LCF_CATDIR**	[privileged]	[privileged]	755	B.4.7

B.7.4.2 Windows File and Directory Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- **%LCF_DATDIR% -** the high level directory structure on endpoints that holds the subordinate directory in which the config file is stored.
- **%LCF_BINDIR% -** the high level directory structure on endpoints that holds the subordinate directory in which software is installed.
- **%LCF_CATDIR% -** the high level directory structure on endpoints that holds the subordinate directory in which message files are located.
- **%LCFROOT% -** the high level root directory.
- **[Tivoli Users]** - a group containing accounts for non-administrative users of Tivoli
- **[Tivoli Admins]** – Policy RegionAdministrators/individual accounts or a group with responsibility for administration of Tivoli on the platform.

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
ITM for Business Integration	TMR Server Gateways Endpoints	**%LCF_DATDIR%**\..\..\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.4.7
ITM for Business Integration	TMR Server Gateway Endpoints	**%LCF_BINDIR%\..**\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.4.7
ITM for Business Integration	TMR Server Gateway Endpoints	**%LCF_LIBDIR%\..**\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.4.7
ITM for Business Integration	TMR Server Gateway Endpoints	**%LCF_CATDIR%**	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.4.7

B.7.5 IBM Tivoli Configuration Manager

B.7.5.1 UNIX File and Directory Permissions

The following notation is used in this section:

- $ORACLE_HOME – the high level directory structure that holds the subordinate directories in which the Oracle RDBMS client software resides
- $BINDIR – the high level directory structure that holds the subordinate directories in which Tivoli software resides
- $INTERP – the interpreter type, an OS-specific identifier that is used to separate files required to support different operating systems
- $DBDIR – the high level directory structure on other managed nodes that holds the subordinate directories in which Tivoli scanner software and output resides
- $OID – the Tivoli object ID of the node
- $LCF_BASE_DIR – the high level directory structure on endpoints that holds the subordinate directories in which Tivoli scanner software and output resides.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Configuration Manager	RIM Host	**$ORACLE_HOME**/	[privileged]	[privileged]	755	B.5.9
Configuration Manager	RIM Host	**$ORACLE_HOME**/bin	[privileged]	[privileged]	751	B.5.9
Configuration Manager	Server	**$BINDIR**/TME/INVENTORY	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Server	**$BINDIR**/../generic/TME/INVENTORY	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Server	**$BINDIR**/../generic/HTTPd/Inventory	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Server	**$BINDIR**/../generic/HTTPd/Inv	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Server	**$BINDIR**/../generic/HTTPd/UserLink	[privileged]	[privileged]	755	B.5.9

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Configuration Manager	Server	**$BINDIR**/TAS/HTTPd/cgi-bin/Inventory	[privileged]	[privileged]	751	B.5.9
Configuration Manager	Server	**$BINDIR**/TAS/HTTPd/cgi-bin/Inv	[privileged]	[privileged]	751	B.5.9
Configuration Manager	Server	**$BINDIR**/TAS/HTTPd/cgi-bin/UserLink	[privileged]	[privileged]	751	B.5.9
Configuration Manager	Gateway	**$BINDIR**/../lcf_bundle/bin/**$INTERP** /inv	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Gateway	**$BINDIR**/../lcf_bundle/bin/**$INTERP** /TME/INVENTORY	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Scanner	**$DBDIR**/inventory	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Scanner	**$DBDIR**/inventory/**$OID**	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Scanner	**$LCF_BASE_DIR**/inv	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Scanner	**$LCF_BASE_DIR**/inv/SCANNER	[privileged]	[privileged]	751	B.5.9
Configuration Manager	UserLink	…/UserLink.htm | …/userlink.htm	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Server	**$BINDIR**/TME/COURIER	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Server	**$BINDIR**/../generic/TME/COURIER	[privileged]	[privileged]	755	B.5.9
Configuration Manager	Server	**$BINDIR**/TAS/HTTPd/cgi-bin/Courier	[privileged]	[privileged]	751	B.5.9
Configuration Manager	Gateway	**$BINDIR**/../lcf_bundle/bin/**$INTERP** /TME/COURIER	[privileged]	[privileged]	755	B.5.9
Configuration Manager	TEC Integration	…/tecad_sd.conf	[privileged]	[privileged]	750	B.5.9

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
Configuration Manager	TEC Integration	…/tecad_sd.baroc	[privileged]	[privileged]	750	B.5.9
Configuration Manager	Extension API	[Software Distribution Extension API directory]	[privileged]	[privileged]	750	B.5.9
Configuration Manager	Historical DB	**$BINDIR**//TME/COURIER/SCRIPTS	[privileged]	[privileged]	750	B.5.9
Configuration Manager	UserLink	…/UserLink.htm | …/userlink.htm	[privileged]	[privileged]	755	B.5.9

B.7.5.2 Windows File and Directory Permissions

The following notation is used in this section:

- %ORACLE_HOME% - the high level directory structure that holds the subordinate directories in which the Oracle RDBMS client software resides
- %BINDIR% - the high level directory structure that holds the subordinate directories in which Tivoli software is installed
- %INTERP% - the interpreter type, an OS-specific identifier that is used to separate files required to support different operating systems
- %SCANDIR% - the high level directory structure on PC managed nodes that holds the subordinate directories in which Tivoli scanner software and output resides
- %DBDIR% - the high level directory structure on other managed nodes that holds the subordinate directories in which Tivoli scanner software and output resides
- %OID% - the Tivoli object ID of the node
- %LCF_BASE_DIR% - the high level directory structure on endpoints that holds the subordinate directories in which Tivoli scanner software and output resides
- [Tivoli DB account] – account used by the RIM Host to access the Inventory Oracle database
- [Tivoli Users] – a group containing accounts for non-administrative users of Tivoli
- [Tivoli Admins] – individual accounts or a group with responsibility for administration of Tivoli on the platform.

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Configuration Manager	RIM Host	**%ORACLE_HOME%**\	Administrators SYSTEM [Tivoli Admins] [Tivoli DB account]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	RIM Host	**%ORACLE_HOME%**\bin	Administrators SYSTEM [Tivoli Admins] [Tivoli DB account]	Full Control Full Control Full Control Traverse / Execute	B.5.9
Configuration Manager	Server	%**BINDIR%**\TME\INVENTORY	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Server	%**BINDIR%**\..\generic\TME\INVENTORY	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Server	%**BINDIR%**\..\generic\HTTPd\Inventory	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Server	%**BINDIR%**\..\generic\HTTPd\Inv	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Server	%**BINDIR%**\..\generic\HTTPd\UserLink	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Configuration Manager	Server	%**BINDIR%**\TAS\HTTPd\cgi-bin\Inventory	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Traverse / Execute	B.5.9
Configuration Manager	Server	%**BINDIR%**\TAS\HTTPd\cgi-bin\Inv	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Traverse / Execute	B.5.9
Configuration Manager	Server	%**BINDIR%**\TAS\HTTPd\cgi-bin\UserLink	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Traverse / Execute	B.5.9
Configuration Manager	Gateway	%**BINDIR%**\..\lcf_bundle\bin**%INTERP%**\inv	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Gateway	**%BINDIR%**\..\lcf_bundle\bin**%INTERP%**\TME\INVENTORY	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Scanner	**%SCANDIR%**	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Scanner	**%SCANDIR%**\OUTPUT	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Modify	B.5.9

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Configuration Manager	Scanner	**%DBDIR%**\inventory	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Scanner	**%DBDIR%**\inventory**%OID%**	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Modify	B.5.9
Configuration Manager	Scanner	**%LCF_BASE_DIR%**\inv	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Scanner	**%LCF_BASE_DIR%**\inv\SCANNER	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Modify	B.5.9
Configuration Manager	UserLink	…\UserLink.htm | …\userlink.htm	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read	B.5.9
Configuration Manager	Server	**%BINDIR%**\TME\COURIER	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	Server	**%BINDIR%**\..\generic\TME\COURIER	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Configuration Manager	Server	**%BINDIR%**\TAS\HTTPd\cgi-bin\Courier	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Traverse / Execute	B.5.9
Configuration Manager	Gateway	**%BINDIR%**\..\lcf_bundle\bin**%INTERP%**\TME\COURIER	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	TEC Integration	…/tecad_sd.conf	Administrators SYSTEM [Tivoli Admins]	Full Control Full Control Full Control	B.5.9
Configuration Manager	TEC Integration	…/tecad_sd.baroc	Administrators SYSTEM [Tivoli Admins]	Full Control Full Control Full Control	B.5.9
Configuration Manager	Extension API	[Software Distribution Extension API directory]	Administrators SYSTEM [Tivoli Admins]	Full Control Full Control Full Control	B.5.9
Configuration Manager	Historical DB	**%BINDIR%**\TME\COURIER\SCRIPTS	Administrators SYSTEM [Tivoli Admins]	Full Control Full Control Full Control	B.5.9
Configuration Manager	AutoPack Agent	…/**wsyschg.exe**	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.5.9
Configuration Manager	UserLink	…/UserLink.htm | …/userlink.htm	Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read	B.5.9

B.7.5.3 Windows Registry Permissions

The following notation is used in this section:
- [Tivoli DB account] – account used by the RIM Host to access the Inventory Oracle database
- [Tivoli Admins] – individual accounts or a group with responsibility for administration of Tivoli on the platform.

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
Configuration Manager	RIM Host	HKLM\SOFTWARE\ORACLE (include all subkeys)	Administrators SYSTEM [Tivoli Admins] [Tivoli DB account]	Full Control Full Control Full Control Read	B.5.3.2.1

B.7.6 IBM Tivoli Monitoring for Business Integration

B.7.6.1 UNIX File and Directory Permissions

The following system variables may be established during the installation and may be used as part of the paths in the table below.

- **$BINDIR** – the high level directory structure that holds the subordinate directories in which Tivoli software is installed
- **$INTERP** – the interpreter type, an OS-specific identifier that is used to separate files required to support different operating systems.
- **$DBDIR** – the high level directory structure on other managed nodes that holds the subordinate directory in which ITM database files are located.
- **$LIBDIR** – the high level directory structure holds directory of the interpreter type.
- **$LCF_DATDIR –** the high level directory structure on endpoints that holds the subordinate directory in which config and log files are stored.
- **$LCF_BINDIR –** the high level directory structure on endpoints that holds the subordinate directory in which software is installed.
- **$LCF_CATDIR –** the high level directory structure on endpoints that holds the subordinate directory in which message files are located.
- **$LCFROOT –** the high level root directory.

Tivoli Product	Component	Object	Owner	Group	Permissions	STIG Reference
ITM for Business Integration	TMR Server	**$DBDIR**/../	[privileged]	[privileged]	755	B.7.5
ITM for Business Integration	TMR Server Gateways	**$BINDIR**/../	[privileged]	[privileged]	755	B.7.5
ITM for Business Integration	TMR Server Gateways	**$LIBDIR**/../	[privileged]	[privileged]	755	B.7.5
ITM for Business Integration	Endpoints	**$LCF_DATDIR**/../	[privileged]	[privileged]	755	B.7.5
ITM for Business Integration	Endpoints	**$LCF_BINDIR**/../	[privileged]	[privileged]	755	B.7.5
ITM for Business Integration	Endpoints	**$LCF_LIBDIR**/../	[privileged]	[privileged]	755	B.7.5
ITM for Business Integration	TMR Server Gateway Endpoints	**$LCF_CATDIR**	[privileged]	[privileged]	755	B.7.5

B.7.6.2 Windows File and Directory Permissions

The following system variables may be established during the installation and may be part of the paths in the table below.

- **%BINDIR%** - the high level directory structure that holds the subordinate directories in which Tivoli software is installed
- **%INTERP%** - the interpreter type, an OS-specific identifier that is used to separate files required to support different operating systems.
- **%DBDIR%** - the high level directory structure on other managed nodes that holds the subordinate directory in which the TMF database files resides.
- **%LIBDIR%** – the high level directory structure holds directory of the interpreter type.
- **%LCF_DATDIR% -** the high level directory structure on endpoints that holds the subordinate directory in which _____ are stored.
- **%LCF_BINDIR% -** the high level directory structure on endpoints that holds the subordinate directory in which software is installed.
- **%LCF_CATDIR% -** the high level directory structure on endpoints that holds the subordinate directory in which message files are located.
- **%LCFROOT% -** the high level root directory.
- **[Tivoli Users]** – a group containing accounts for non-administrative users of Tivoli.
- **[Tivoli Admins]** – Policy RegionAdministrators/individual accounts or a group with responsibility for administration of Tivoli on the platform.

Tivoli Product	Component	Object	Account Assignment	Permissions	STIG Reference
ITM for Business Integration	TMR Server	**%DBDIR%**\..\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.7.5
Tivoli Management Framework	TMR Server, Managed Node Gateway	**%BINDIR%\..**	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.7.5
ITM for Business Integration	TMR Server Managed Node Gateway	**%DBDIR%\..**	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.7.5
ITM for Business Integration	Endpoints	**%LCF_DATDIR%**\..\	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.7.5
ITM for Business Integration	Endpoints	**%LCF_BINDIR%\..**	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.7.5
ITM for Business Integration	Endpoints	**%LCF_LIBDIR/%\..**	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.7.5
ITM for Business Integration	Endpoints	**%LCF_CATDIR%**	TMR Administrators SYSTEM [Tivoli Admins] [Tivoli Users]	Full Control Full Control Full Control Read & Execute	B.7.5

This page is intentionally left blank.

APPENDIX C. MICROSOFT SYSTEMS MANAGEMENT SERVER

C.1 Systems Management Server Overview

Microsoft's Systems Management Server (SMS) is software that addresses the configuration management functions of Enterprise System Management for Windows-based environments. Limited support for some network infrastructure such as switches and routers is included and third-party support for non-Windows hosts is available. SMS is part of Microsoft's infrastructure management product group that includes the Microsoft Operations Manager (MOM) product and the Application Center product.

The following information provides an overview of SMS functions, its architecture, ESM elements it implements, and the industry standards used in the product. A brief summary of similar Microsoft products and the relevant product release are noted to put this discussion in proper context.

Microsoft describes the functions that SMS performs in terms of four areas:

- Inventory includes the collection of hardware and software data for managed systems.
- Provisioning includes capabilities to deploy and update software as well as perform configuration changes.
- Troubleshooting includes remote viewing and manipulation of client systems.
- Reporting includes the capability to generate and view detailed reports based on vendor-supplied and locally developed report specifications.

SMS is based on a flexible architecture that supports distributed server functions, with a logical site as the organizing unit. Complex hierarchies that include primary and secondary sites and parent and child sites can be designed to reflect the operating environment. However, as the complexity of the server distribution and hierarchy implementation increases, the need for careful security configuration and procedures increases as well.

The SMS implementation maps well to the elements discussed in *Section 2.1.2, ESM Implementation Elements*. The correspondence can be described as:

- Manager – ESM manager functions are primarily implemented in SMS through applications that run as Windows Services on SMS server machines. The SMS Executive service is the primary element that fulfills this role.

- Agent – ESM agent functions are implemented in SMS through applications that run as Windows Services on SMS client machines. The SMS Advanced Client implements this role through the SMS Agent Host service.

- Console – The ESM console function is implemented in SMS through the SMS Administrator Console; it is built on the Microsoft Management Console (MMC) framework. The SMS Administrator Console is always installed on the SMS Site Server and can be installed on other server or client machines.

- Management Data Repository – The ESM management data repository is implemented in SMS through the SMS Site Database. This database service is provided by the Microsoft SQL Server product and typically runs on the server machine identified as the SMS Site Server.

SMS employs technologies based on common industry standards:

- SMS inventory functions can optionally use SNMP to gather information from Windows clients that are running an SNMP agent.

- SMS relies heavily on the use of Windows Management Instrumentation (WMI) that is implemented in current versions of Windows operating systems. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) standards set. SMS uses WMI capabilities to communicate with and manage clients, as well as a way to provide a standard interface to its own methods and data.

Microsoft offers other product components and technologies that provide a subset of the configuration management functions found in SMS. Some brief notes on these components helps to put SMS into perspective.

Windows Update is a public, Internet-based web service hosted by Microsoft. It is intended to allow individual clients to download patches, updates, and service packs for certain Windows operating system versions from a public Microsoft web site. Windows Update does not provide features such as selective targeting, network use optimization, distribution control, reporting, or deployment planning.

Software Update Services (SUS) and its announced successor, Windows Update Services (WUS), are optional components for current Windows server operating systems. These components allow administrators to enable deployment of updates from their own servers to clients within their infrastructure. SUS provides the ability to deploy critical updates, security patches, and service packs for current Windows operating systems. WUS will expand on this by offering the capability to update other Microsoft products such as Office, SQL Server, and Exchange. Software…successor, Windows Server Update Services (WSUS), are optional … These components allow administrators to fully manage and distribute updates, that are released through Microsoft Update, from their own (upstream) servers to clients and other servers within their infrastructure. WSUS gives administrators full control over the update management process, eliminating the need for client computers to retrieve updates directly from Microsoft Update. WSUS administrators can specify the types of updates to download, create target groups of computers to receive updates, and determine which computers require updates before deployment. Administrators can approve updates for deployment automatically, uninstall updates, and generate reports to monitor update activity.

In contrast to Windows Update and SUS\WUS, the SMS product is intended as an enterprise-class solution to system management issues including and beyond deploying updates. SMS provides many additional features and an extensible architecture that allows administrators to use the tools to perform functions not supported by the other solutions.

Please note that this document is based on SMS 2003. While the information may be applicable to earlier releases of SMS, it has not been verified for those releases. The primary source for this information is the *Microsoft Systems Management Server 2003 Concepts, Planning, and Deployment Guide*, the *Microsoft Systems Management Server 2003 Operations Guide*, and the *Scenarios and Procedures for Microsoft Systems Management Server 2003: Security* document. Refer to *Appendix A, Related Publications*, for additional documentation and the addresses of web sites with more information.

C.1.1 SMS Component Overview

SMS is a complex software product with a number of components and an architecture that allows it to be implemented in a variety of configurations. This section will describe some of the basic parts and concepts that should be understood in order to configure SMS and to understand the security issues.

A *site* can be thought of as the basic logical unit in the hierarchy of an SMS implementation. A site is related to the span of control in SMS. Different types of sites can be created:

- Primary site – Every SMS implementation must have at least one primary site. A primary site includes a site database that holds information for the site and the child sites that report to it. A primary site can report to another primary site.

- Secondary site – An SMS implementation may have one or more secondary sites. A secondary site does not have its own database; the site forwards its information to, and is administered from, the primary site to which it reports.

- Central site – A central site is the primary site at the top of the SMS hierarchy. All other sites report directly or indirectly to it.

- Parent site – A parent site is a site that has one or more child sites that report to it. A parent site must be a primary site.

- Child site – A child site is a site that reports to another site. A child site may be a primary or a secondary site.

At the time an SMS site is created, it must be assigned a three-character site code. This code identifies the site and is used in the names of Windows accounts that SMS automatically creates. The SMS site code is also used as a way of indicating the site to which a specific client is assigned.

Each site must be configured with boundaries that specify the span of control. Site boundaries are specified in terms of IP subnets and / or Active Directory sites. A site manages the clients within its site boundaries. When Advanced Clients are used, roaming boundaries are specified to control the Distribution Point servers to which a roaming client is allowed to connect.

Each SMS site is created by the installation of SMS software on one or more Windows server machines. Specific terminology is used to describe the SMS servers and functions:

- Site server – A site server is the principal server machine and could be the only server within the site on which the SMS server software is installed. Some or all of the SMS server functions or roles are performed on the site server.

- Site system – A site system is a server machine within the site on which some of the SMS server functions or roles are performed.

- Site system role – A site system role is a specific function that a site system performs for that site. The roles defined in SMS include: site server, site database (or SQL) server, SMS Provider, Client Access Point (CAP), Distribution Point, Management Point, Server Locator Point, and Reporting Point. Site system roles can be distributed across multiple server machines.

Some important points to note about SMS servers include the following:

- The site server and site database server roles are commonly implemented on the same physical machine. There are performance and security advantages to this configuration.

- The Management Point, Server Locator Point, and Reporting Point roles require Internet Information Services (IIS) to be installed and operational on the server. Separating these roles to run on a different machine than the site server is recommended for this reason.

The goal of implementing an SMS site is to establish the capability to manage clients. SMS 2003 supports the definition of two types of clients: Legacy Clients and Advanced Clients.

Legacy Clients have the following characteristics:

- Legacy Clients are carried over from earlier releases of SMS and support older Windows operating systems including Windows 9x and Windows NT.

- Legacy Clients require more and more highly privileged Windows application accounts to be defined.

- Microsoft has announced their intent to drop support for Legacy Clients in a future release of SMS.

Advanced Clients have the following characteristics:

- Advanced Clients run on Windows 2000 and later operating systems.

- Advanced Clients require fewer Windows application accounts.

- Advanced Clients support transmission integrity through digital signature checks on SMS policy and content.

- Advanced Clients support the concept of roaming, which is the ability to move a client machine from one IP subnet or Active Directory site to another. This can decrease the complexity of managing mobile machines.

- Advanced Clients support the use of the Background Intelligent Transfer Service (BITS). This simplifies firewall port configuration and provides greater efficiency in receiving file distributions.

Figure C-1 depicts how a simple SMS site using Advanced Clients could be configured.

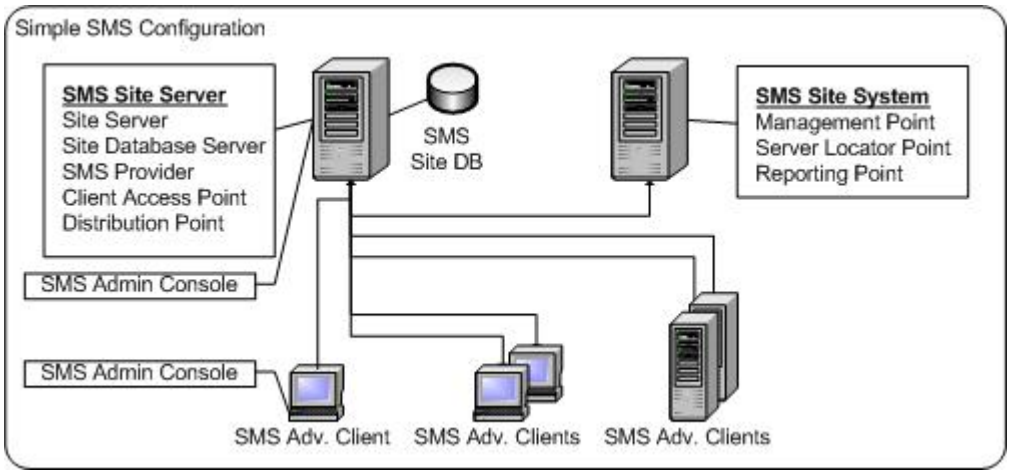

Figure C-3. Simple SMS Site

SMS capabilities are implemented through functions that interact with the server and client components. A basic understanding of the following functions helps to understand SMS security issues: resource discovery, the SMS status system, logging, maintenance tasks, and the use of WMI.

Resource discovery consists of methods that SMS uses to capture and maintain basic data about objects within a site's boundaries. The types of SMS Discovery fit roughly into three categories:

- Discovery can gather information from Windows domain controller repositories such as Active Directory containers.

- Discovery can query individual machines using Windows function calls relating to file sharing capabilities.

- Discovery can gather information through standard TCP/IP network facilities such as the Internet Control Message Protocol (ICMP), Dynamic Host Configuration Protocol (DHCP), or SNMP.

The SMS status system provides the primary tool for determining the operational condition of SMS server components. Status messages are generated by individual SMS components and stored in the site database. Status filter rules control retention, reporting, replication, and external program actions. Status summarizer components use status messages and other site database information to create summaries of the operational state of the SMS hierarchy. Status messages are identified as one of three types: milestone, detail, or audit.

Many SMS components include a logging capability that collects detailed data about SMS activities. The status, location, and size of a component's log are configurable. While most of the component logging might be enabled only for detail-level troubleshooting, logging for the SMS Site Backup would be considered routine.

SMS maintenance tasks provide a method to automate a schedule of routine actions needed to keep SMS operating normally. The product comes with several pre-defined tasks. The most notable of these is the Backup SMS Site Server task.

The use of WMI by SMS deserves note because WMI is supplied as a component of current Windows operating systems, but SMS depends heavily on it to gather and manage information. As noted earlier, WMI is an implementation of the WBEM standards set. As such WMI incorporates methods and data structures related to system management. Therefore access to WMI methods and data is a security concern for SMS.

WMI data is stored in logical structures known as namespaces. Namespaces are organized hierarchically, expressed as parent and child namespaces. Certain namespaces are defined and populated by the Windows OS. When an SMS server or client component is installed on a machine, additional namespaces are created. Access is controlled at the namespace level, with support for the concept of inheriting namespace access permissions from parent to child. The WMI Control, a plug-in to the Microsoft Management Console, provides access to WMI namespace access settings.

A choice of security modes in which to operate was added in SMS 2003. Standard security mode is essentially the same as the only security option in SMS 2.0. Advanced security mode was added to address the complexity and administrative effort associated with Windows application account definitions in the older SMS security mode. The subject of security modes is addressed in the next section, but some important issues should be noted:

- Advanced security mode requires the implementation of Windows Active Directory for all SMS servers within a site and at all network locations.

- While it is possible to operate a hierarchy of SMS sites with a mixture of security modes, certain sites in the hierarchy (parents of other Advanced security mode sites) would be required to operate in Advanced security mode.

Although it is not a component that currently comes with the basic SMS installation materials, the SMS Toolkit should be considered required for SMS at all installations. The toolkit can be downloaded from Microsoft at the web site noted in *Appendix A, Related Publications*. Four elements in the Toolkit are necessities:

- The SMS Trace tool is a viewer for the component log files. While the files are text files that can be viewed using other applications, the SMS Trace tool provides formatting, filtering, and highlighting that are essential to efficiently finding information in the logs.

- The IIS Lockdown Template is used to configure the Windows IIS component more securely. The SMS Toolkit version is specifically tailored for SMS environments.

- The URLScan Template is also used to increase IIS security in terms of file filtering. This Toolkit version is also specifically tailored for SMS servers.

- The Management Point Spy verifies that management points and proxy management points are obtaining policies from the primary site.

C.1.2 General Security Considerations

Enhancing the security of SMS configurations requires the application of a number of known best practices for information systems. This task is made somewhat simpler because the components run on a homogenous platform base, Microsoft Windows operating systems. At the same time, the distributed nature of SMS, the potential for different hierarchical deployments, and various product options complicate an attempt to provide straightforward security guidance.

As a preface to the next section in this document, the following paragraphs discuss these general security considerations for SMS:

- Security Policy Implementation
- Risk Sensitivity or Analysis
- SMS server roles and server partitioning
- SMS configuration options: security mode and client type
- Database and web server software
- OS accounts required by SMS
- SMS program and data files
- SMS object access control
- WMI namespace access control
- SMS Feature components
- Status and logging mechanisms
- Network issues
- Installation issues
- Backup and recovery issues

Putting Systems Management Server (SMS) security in place is critical to maximize the integrity of your computer infrastructure, and putting SMS security in place properly is crucial to the successful operation of SMS. In order to maintain SMS security and react to security issues when

they arise, you must be vigilant. You must routinely review your security (and enhance it where appropriate), and take advantage of new security options when they become available.

Risk sensitivity or analysis is essentially the process of identifying risks and deciding what to do about them. You must identify the potential source of the risk, assess the probability of that risk occurring, prioritize the risk based on impact to your business priorities, and then plan to minimize that probability. All risks are not equally damaging. The most serious risk from SMS is that its functionality could be hijacked by an unauthorized user who could then distribute software to all SMS clients.

It was noted in *Section C.1.1, SMS Component Overview*, that SMS server functions are defined in terms of site system roles. This is relevant to security because some of the roles have specific software and OS account requirements that, if combined in certain machine configurations, could degrade overall security. As a result certain server partitioning requirements and recommendations apply.

SMS 2003 offers two security modes: Standard and Advanced. The choice of mode directly impacts security because it results in significant differences in the types of OS accounts required for SMS to operate. Standard security employs typical administrator-defined user accounts; Advanced security uses Windows LocalSystem and computer accounts.

SMS 2003 offers two types of clients: Legacy and Advanced. There are a number of security considerations for this choice and Microsoft documentation explicitly states that the Legacy Client "…is not considered a secure environment."

SMS requires the use of the Microsoft SQL Server database product and the Windows IIS web server component. These software packages must be configured to comply with other applicable security implementation guides.

SMS permits flexibility in the OS accounts that it uses for access between servers and clients. Exposure can be reduced by following requirements for more accounts, but with the least privilege principle applied to each.

As with the implementation of all software packages, there are program files and data files for which access protection must be controlled in order to maintain the desired confidentiality, integrity, and availability characteristics of SMS.

Use of SMS administrative privileges is controlled through SMS object access definitions. In anything but the simplest administrative environments, an access control strategy must be employed to ensure that separation of duties is maintained.

The use of WMI namespaces by SMS was briefly described earlier. Limiting access to those namespaces is needed to maintain SMS availability and integrity.

Microsoft identifies some of the SMS product components as SMS Features. This includes Reporting, Remote Tools, Software Distribution, and Inventory Collection. The current

coverage in this document of security considerations for the SMS Features is limited. However, due to identified security vulnerabilities in the Remote Tools feature, a specific requirement covering that feature is necessary.

SMS offers status and logging capabilities that are directly related to maintaining SMS availability. In addition, the use of certain status features is needed to maintain an audit trail of activity.

The distributed architecture of SMS and its management mission cannot be implemented without the use of networks for communication. The TCP/IP ports used by SMS are subject to other security guidance that restricts their use outside of enclave boundaries. The data being transported is also subject to confidentiality and integrity requirements.

During the installation phases of SMS, issues can arise from the setup and configuration options that are selected. Although the results of undesirable choices can be corrected later, the better choices can eliminate windows of vulnerability during installation:

- The SMS setup process defines two types: express and custom. Microsoft characterizes express setup as "appropriate for setting up evaluation sites on an isolated network" because it enables SMS configuration options that could cause serious negative impact to a production environment. Specifically, the SMS Discovery methods, client installation types, or Remote Tools feature that are enabled by express setup could negatively impact the integrity and availability of the environment.

- When SMS setup is executed, access to some administrative privileges is automatically granted to the Windows account used to perform the installation. An administrative account strategy can help to ensure that this access is appropriately granted.

- Early implementation steps for SMS can include the use of Network Discovery to detect assets. Without adequate planning and coordination, the generated network activity might be interpreted incorrectly as a form of network attack.

An instance of reduced availability of the SMS system could lead to further, more serious security problems. For example, the inability to deploy a critical security patch could allow many unprotected client systems to be compromised. This is one of the reasons why backup and recovery must be considered even more important for SMS server systems than for some other categories of servers.

C.2 SMS Specific Configuration Guidance

The following subsections describe considerations and requirements for securing SMS configurations. The information is organized according to the subject areas defined in DODI 8500.2 and corresponds to the organization of *Section 3, Enterprise System Management Security,* in this document.

When reviewing the requirements, the following must be noted:

- The specific file and directory names referenced in the requirements and specified in the appendix reflect defaults indicated in vendor documentation. If a site or organization deploying SMS chooses other names, the requirements apply to the site-specific names.

- The term Site Server refers to machines on which the SMS site server role executes. The term Site System refers to machines running Client Access Point (CAP), Distribution Point, Management Point, Server Locator Point, and Reporting Point roles.

C.2.1 Security Design and Configuration

This section describes the specific considerations and requirements for SMS that are related to the IA controls in the Security Design and Configuration subject area. The following information is addressed:

- Cryptographic algorithms
- Protection of SMS software and limits on privileged program use
- Software release maintenance
- Application partitioning
- Network port usage

SMS can use encryption, hashing, and signing algorithms for some data transfer operations. However, there are no individual SMS controls that allow the selection of specific FIPS 140-compliant algorithms. This issue is addressed by following the requirements in the *Windows NT\2000\XP Addendum* and the associated NSA guides that address OS security configuration.

SMS software resides in directories and files that are installed on server and client systems. The assignment of directory and file access permissions for the SMS software is restricted in accordance with the DODI 8500.2 System Library Management Controls. Access permissions must be assigned only to process and user accounts that require the associated access to perform designated functions. Privileged system accounts used for administrative functions are allowed full access. Non-privileged accounts, such as the accounts used by the SMS clients, are allowed execute access to program files and read access to other objects.

- *(EMS.0010: CAT II) The SA will ensure access to SMS server software libraries (including executable and configuration files) is restricted in accordance with the permissions in Appendix C.3.*

- *(EMS.0020: CAT III) The SA will ensure access to SMS client software libraries (including executable and configuration files) is restricted in accordance with the permissions in Appendix C.3.*

The SMS server software libraries include tools that are used for special maintenance tasks. These tools have the capability to significantly impact the operation of an SMS site and clients. Included in these tools are the following:

- The ACL Reset tool (ACLreset.exe) is primarily used during recovery operations to synchronize directory permissions with Windows application accounts that are being redefined.

- The Hierarchy Maintenance tool (PreInst.exe) is a multi-purpose utility used for diagnosis, repair, recovery, and key management tasks. Its use may be required in the event disaster recovery must be performed.

- The Remote Tools command line program (Remote.exe) enables Remote Tools to be run outside of the Administrator console.

Access to the ACL Reset and Hierarchy Maintenance programs is appropriate only for administrators with responsibility for SMS site maintenance because of the powerful functions they perform. Access to the Remote Tools program must be closely restricted because of the security issues associated with the Remote Tools feature. Additional information on Remote Tools is found in *Section C.2.3.2, Account Management*.

- *(EMS.0030: CAT II) The SA will ensure access to the SMS ACL Reset, Hierarchy Maintenance, and Remote Tools programs is restricted in accordance with the permissions in Appendix C.3.*

As Microsoft has continued development of the SMS product, new releases have been made available. In conjunction with the Microsoft Support Lifecycle policy, there are limits to the length of time a product release remains supported. At the end of this period, security updates are no longer provided. As of the publishing date of this document, Microsoft has stated the following concerning end of support:

- Support for SMS 2003 with no Service Pack applied will be retired as of 10 Sep 2005.

- Support for SMS 2003 with Service Pack 1 will be retired as of 31 Jan 2014 or twelve months after the next Service Pack is released, whichever comes first.

Information on SMS support dates is available at Microsoft's web sites at http://support.microsoft.com/gp/lifesrvr and http://support.microsoft.com/gp/lifesupsps.

To prevent situations in which an organization becomes vulnerable to a security problem that the vendor will not repair or confirm, requirements for the use of supported products and for migration planning are necessary.

- *(EGA.0110: CAT I) The IAO will ensure SMS software is removed or upgraded prior to the vendor dropping support for the installed release.*

- *(EGA.0120: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading SMS software prior to the date the vendor drops security patch support.*

The architecture of SMS allows it to be installed in a number of server configurations. It is possible to combine all the server functions on a single machine or distribute the system roles among a number of network-connected machines. This offers flexibility, but can also create security vulnerabilities. The following items must be considered:

- The Windows account under which the primary SMS server service (SMS Executive) runs must be a member of the Administrators group for the machine on which it runs. Because of the account structure on Windows domain controller machines, the SMS server software would gain domain-wide Administrator privileges if installed on a domain controller.

- The supporting software required for SMS servers includes MS SQL Server and IIS. Installing or enabling these components on a Windows domain controller has negative security implications.

- The SMS Site Server stores most of its data on the Site Database Server. The nature and amount of data transferred between these logical roles, the network port requirements, the authentication activity, and the availability requirement are factors in determining the best configuration of these two server roles.

- The Management Point, Server Locator Point, Reporting Point, and optionally the Distribution Point require that IIS be installed. The use of the Windows LocalSystem account and the access that might be assigned to it on SMS Site Servers can cause concern when IIS also uses this account.

- In an SMS single site configuration using Advanced Clients, but without the Active Directory extensions, the clients authenticate the Site Server using data on the Management Point. If the Site Server and Management Point are combined on a single machine and that machine fails, clients may be unable to authenticate the rebuilt Site Server.

In consideration of these items, there are a number of SMS server configuration requirements related to partitioning the SMS application.

- *(EMS.0040: CAT II) The SMS Administrator will ensure the SMS Site Server, Site Database Server, and any other Site Systems are not installed on Windows domain controllers.*

- *(EMS.0050: CAT II) The SMS Administrator will ensure the instance of SQL Server on the SMS Site Database Server is dedicated to SMS.*

- *(EMS.0060: CAT III) The SMS Administrator will ensure SMS Site System roles require IIS are not enabled on the Site Server machine.*

- *(EMS.0070: CAT II) The SMS Administrator will ensure single site environments with Advanced Clients and without the Active Directory extensions, the SMS Management Point is not enabled on the Site Server machine.*

In addition to the preceding requirements, the following recommendation is noted:

- The SMS Site Database Server should be installed on the same machine as the Site Server. This varies from normal application partitioning guidance, but the SMS application is an acknowledged exception. Combining these roles reduces exposure of SMS data on the network, reduces authentication transactions, and simplifies security administration.

SMS components use a variety of network ports for communicating among the servers and clients. Microsoft documentation (including Knowledge Base article 826852) provides the following information about TCP/IP port usage by SMS:

Port	Component
80*	Advanced Client to Management Point
135	Administrator Console to servers and clients
137	Remote Control to clients
138	Remote Control to clients
139	Remote Control to clients
389	Site Server to Site Database Server Site Server to child site Proxy Management Point to Site Database Server Advanced Client to Management Point
445	Site Server to Site Database Server Site Server to child site
636	Site Server to Site Database Server Site Server to child site Proxy Management Point to Site Database Server Advanced Client to Management Point
1433	Management Point to Site Database Server
1723	RAS Sender
2701	Remote Tools to Advanced Client
2702	Remote Tools to Advanced Client
2703	Remote Tools to Advanced Client
2704	Remote Tools to Advanced Client
3268	Advanced Client to Management Point

Table C-1. SMS Port Use

NOTE: Service Pack 1 for SMS 2003 allows the port used for communications from an Advanced Client to Management Points, Server Locator Points, and BITS-enabled Distribution Points to be changed.

In addition to these, some Windows OS services used by SMS require the following ports to be enabled: 53 (DNS), 67 (DHCP), 135 (RPC), 138 (WINS, NetBIOS), and 139 (NetBIOS). Specific port usage depends on the local network configuration and the SMS components used.

One example of port usage involves Advanced Clients in SMS environments without the Active Directory extensions. In this environment, WINS must be enabled in order for clients to find the Server Locator Point (SLP). Advanced Clients use the SLP to find their assigned Management Point.

As indicated above, Service Pack 1 for SMS 2003 makes it possible to alter the TCP/IP port used by the Advanced Client. This may be desirable for the purpose of administrative traffic management. However, there are two considerations that make this undesirable. The first is that some other, non-well-known port would have to be selected and this might conflict with other applications. The second consideration is that SMS client traffic across firewall boundaries might then require an additional port to be opened on the firewall. For these reasons, the port used by the Advanced Client should usually not be changed. If a compelling reason for changing the port is defined, the following port management requirements would apply to the newly selected port.

The requirements specified under DoD Instruction 8551.1, *Ports, Protocols, and Services Management (PPSM),* designate several of the ports utilized by SMS components as RED or YELLOW. As described in *Section 3.2.3, Network Access,* specific action is required for applications using these ports across enclave boundaries.

- *(EMS.0080: CAT II) If an SMS configuration is deployed across DoD enclave boundaries and the deployed components utilize PPSM-designated RED or YELLOW ports, the IAO will ensure specific SMS configuration is approved by the Defense Information System Network (DISN) DAAs.*

C.2.2 Identification and Authentication

This section describes the specific considerations and requirements for SMS that are related to the IA controls in the Identification and Authentication subject area. The following information is addressed:

- Unique SMS administrator and user accounts
- SMS server and client application account options
- Default SMS application accounts

The functions performed by SMS are controlled by the actions of SMS administrators. An SMS administrator is someone authorized for privileged access to the SMS servers, software, and data. Because SMS has broad capabilities to affect the configuration and availability of potentially a large number of client systems, best security practices related to least privilege and separation of duties must be applied to SMS administrator accounts.

Access to some SMS functions may not be privileged. For example, an organization may allow some users to access SMS reporting capabilities. This type of access can be referred to as SMS

user access. However, because SMS data could be sensitive, control of SMS user accounts is still required.

In accordance with DODI 8500.2 IA control Individual Identification and Authentication, access to the SMS systems must be gained through an individual identifier.

- *(EGB.0010: CAT II) The IAO will ensure each SMS administrator or user account is associated with an individual identifier and password.*

SMS does not perform user I&A services itself, but relies primarily on services provided by the Windows operating system. Therefore the ESM requirements for applications providing I&A, described in *Section 3.3, Identification and Authentication*, do not apply to SMS.

However, when SMS is configured to use Standard security mode, there is an issue for Windows account password guidance that needs to be addressed for SMS to operate reliably. The following information summarizes this issue:

- Accounts used by the SMS software to access server and client machines are considered to be application accounts.

- *Windows NT/2000/XP Addendum* security guidance requires domains to be configured with an account lockout policy. In some circumstances SMS could trigger this policy, resulting in degraded SMS availability.

- To avoid lockouts, the SMS application accounts should be configured with the *Password never expires* option.

- Passwords for accounts that are automatically created by SMS do not have to be changed by an administrator. The potential risk from this practice is mitigated by the strong password generation capability and the site reset function used by SMS. These accounts are identified in *Section C.2.3.2, Account Management*.

- Passwords for SMS application accounts created by the System Administrator must conform to the yearly change requirement for application accounts.

Although the primary access points to SMS functions and data use I&A services in the Windows OS logon interface, the Report Viewer web application does not. Refer to *Section C.2.3.5, Network Access*, for more information on this interface and the password transmission issue. In accordance with the DODI 8500.2 IA control for Individual Identification and Authentication, passwords must be encrypted for transmission.

- *(EMS.0090: CAT II) The SMS administrator will ensure the Reporting Point server is configured to use the HyperText Transfer Protocol Secure (HTTPS) protocol or an alternate network encryption mechanism is used for user connections to the Report Viewer application.*

SMS maintains elements of a Public Key Infrastructure (PKI) to perform host authentication. Advanced Clients use these elements to authenticate data from a Management Point. Refer to the certificate infrastructure and certificate management topics in the Microsoft document, *Scenarios and Procedures for Microsoft Systems Management Server 2003: Security*, for information. It is not possible to utilize the DoD PKI for this facility and there are no SMS options to control it.

Configured in Standard security mode, SMS uses several application accounts to access server and client machines. The DODI 8500.2 IA control entitled Individual Identification and Authentication requires that factory-set, default, or standard user IDs be removed or changed. Although SMS does not permit the names of all its accounts to be changed from the defaults, it is possible to change the most important account used on the Site Server.

The Windows account under which the primary SMS server service (SMS Executive) executes is named SMSService by default. By defining the account before SMS installation and supplying the name to the installation procedure, it is possible to easily avoid using this default.

- *(EMS.0100: CAT III) The SMS Administrator will ensure the Windows account used for the SMS Executive service is not named SMSService.*

It was noted above that SMS uses some PKI elements for host authentication. As with that PKI implementation, key management within SMS cannot utilize an external Key Management Infrastructure (KMI) and there are no SMS options to control key management.

C.2.3 Enclave and Computing Environment

This section describes the specific considerations and requirements for SMS that are related to the IA controls in the Enclave and Computing Environment subject area. Because of the extent of the information in this area, it is organized in the following subsections:

- Data protection
- Account management
- Application Customization
- Auditing
- Network Access

C.2.3.1 Data Protection

During installation and operation, SMS software creates directories and files on server and client machines. The assignment of directory and file access permissions for the SMS data is restricted in accordance with the DODI 8500.2 IA controls Access for Need-to-Know and Changes to Data. Access permissions must be assigned only to process and user accounts that require the associated access to perform designated functions. Privileged system accounts used for administrative functions are allowed full access. Non-privileged accounts, such as the accounts used by SMS users, are allowed execute access to program files and read access to other objects.

- *(EMS.0110: CAT II) The SA will ensure access to the SMS server data directories and files is restricted in accordance with the permissions in Appendix C.3.*

- *(EMS.0120: CAT III) The SA will ensure access to the SMS client data directories and files is restricted in accordance with the permissions in Appendix C.3.*

During installation, SMS software configures some directories on server machines as shared folders. As a defense-in-depth measure, the shared folder permissions are restricted as a supplement to the standard directory and file security. Accounts requiring access are allowed change permission.

- *(EMS.0130: CAT III) The SA will ensure access to shared SMS folders on SMS servers is restricted in accordance with the permissions in Appendix C.3.*

In *Section C.1.1, SMS Component Overview*, the use of namespaces to store WMI data was briefly discussed. All Windows systems on which the WMI services are active store WMI data in namespaces. SMS uses this Windows data as well as using WMI services to store additional SMS-specific data. WMI namespaces are organized hierarchically, with the Root namespace at the top. When SMS is installed, the Root\SMS and Root\NetworkModel namespaces are created on the Site Server and the Root\CCM namespace is created on Site Systems and Advanced Clients.

In addition to the security provided for the WMI files by Windows, an additional layer of security is used to protect namespaces at each level in the hierarchy. As with Windows directory security, namespace security can be inherited down through the hierarchy. The possible namespace access privileges include: Execute Methods, Full Write, Partial Write, Provider Write, Enable Account, Remote Enable, Read Security, and Edit Security.

In order to maintain the integrity of Windows and SMS namespace data, access to the WMI namespaces must be restricted. All accounts are allowed Execute Methods, Provider Write, and Enable Account access; the SMS administrators group is also allowed Remote Enable access; and privileged system accounts used for administrative functions are allowed all access privileges.

- *(EMS.0140: CAT II) The SA will ensure access to WMI namespaces on SMS servers and clients is restricted in accordance with the permissions in Appendix C.3.*

According to the DODI 8500.2 IA control for Changes to Data, logging access and changes to SMS data is required for some environments. Logging can be accomplished through two facilities:

- Current Windows operating systems have the capability for file and directory auditing. The generated data specifically identifies the data access attempted. *Windows NT/2000/XP Addendum* security guidance has requirements that address file and directory access logging. Implementation of that guidance is assumed.

- SMS client and server components record process information in individual log files. Although this information is not intended to be a data access log, elements of it can be used for that purpose.

Because SMS component logging is designed as a troubleshooting tool and the output can be voluminous as a result, there are no specific requirements related to data access logging at this time. Organizations implementing SMS should evaluate and enable logging appropriate to their environment.

By virtue of the client/server architecture of SMS, it is given that data will traverse one or more networks as it is collected and processed. When this data reflects detailed configuration information, such as the output of a hardware or software inventory process, that data assumes the sensitivity characteristics of the systems from which it is derived.

The network configuration in which SMS is implemented, combined with the sensitivity of the SMS data, can generate the need for protective measures. The DODI 8500.2 IA control for Encryption for Confidentiality (Data in Transit) specifies the relevant circumstances.

SMS does not provide for encryption of all data in transit. Therefore an organization deploying SMS is required to take steps such as the implementation of a VPN to provide encryption when appropriate to the data classification.

- *(EGC.0030: CAT II) The IAO will ensure SMS data includes unclassified, sensitive information (including system hardware or software configuration data) traverses a commercial or wireless network is encrypted, at a minimum, using NIST-certified cryptography.*

- *(EGC.0040: CAT II) The IAO will ensure SMS data includes classified systems' hardware or software configuration data traverses a network cleared to a lower level than the SMS data is encrypted using NSA-approved cryptography.*

C.2.3.2 Account Management

Account management spans a number of issues related to the definition of accounts and the assignment of privileges to those accounts. In this section, the following issues and related requirements are addressed:

- Application, administrator, and user accounts
- Account groups
- SMS objects
- SMS Features.

The complex nature of SMS is reflected in the Windows account structure used in SMS operations. The accounts can be grouped in three categories:

- The SMS application accounts are used for server-to-server, server-to-client, and client-to-server access.

- Individuals responsible for some set of installation, operation, and maintenance tasks use SMS administrator accounts for SMS.

- SMS user accounts are used by individuals designated to receive some level of non-privileged access to SMS features such as reporting.

It must be noted that the applicability of this information varies by product release. The information in this section is based on SMS 2003.

The usage of SMS application accounts is highly dependent on two key options selected for the deployment of SMS. These options were discussed briefly in *Section C.1.1, SMS Component Overview*; the important points are:

- The choice of security mode, Standard or Advanced, has significant impact. In Standard mode, Windows user accounts are used to run services and access other systems. In Advanced mode, SMS services run under the Windows LocalSystem security context and access between systems is done using Windows computer accounts.

- The type of clients, Legacy or Advanced, has some impact on account usage. Legacy Clients use privileged Windows user accounts for key tasks such as installing software on clients. Advanced Clients use the Windows LocalSystem security context and the computer account for the same tasks. It must also be noted that, as of the implementation of SMS 2003 Service Pack 1, Microsoft does not support use of the Legacy Client on Windows 2000, Windows XP, or Windows Server 2003.

Managing Windows application accounts is an administrative burden and potential source of vulnerability. If an application account is assigned a weak password and the account is compromised, the confidentiality, integrity, and availability of the application could be negatively impacted. When the account is privileged, entire platforms can be affected. For an ESM application such as SMS, this could be the enabling factor in a major security incident.

If account password maintenance is not carefully coordinated with application execution, the use of an invalid password could quickly trigger the Windows account lockout policy and some function of the application would be disabled. For SMS this could result in the inability to distribute a critical security patch, resulting in a large number of client machines becoming vulnerable to an attack.

In addition to the Windows account management issues and the Microsoft support statement, Legacy Clients do not include the support found in the Advanced Client to authenticate SMS

data using digital signatures. These factors make the use of the Legacy Client a poor security practice.

- *(EMS.0150: CAT II) The SMS Administrator will ensure the SMS Legacy Client is not installed.*

Guidance for the selection of security mode is a more difficult issue. Although Advanced security reduces the number of required accounts, there is a significant prerequisite to its use. Advanced security mode requires that all SMS server machines within a site are in Active Directory and Active Directory is available at all network locations. Because of the planning and coordination required to correctly implement Active Directory, many organizations have not yet fully enabled this technology.

Because of the Active Directory prerequisite, a specific security mode is not required at this time. However, to take advantage of the improved security, organizations should deploy SMS using Advanced security mode when they are able.

Other issues related to SMS application accounts necessitate a discussion of how the accounts are used. The following table describes the accounts used for SMS server connections in a configuration using Standard mode security with Advanced clients.

Windows Account [Default Name]	**Function Notes**
SMS Service [SMSService]	- Used as identity for SMS services on site server - Used to access the site database when it resides on the site server - Used instead of the Site Address and Site System Connection accounts if they are not defined - Creates files and directories on site server
Server Connection [SMSServer_*sc*]	- Used by site system(s) to access the site server - Created by default during site server installation - Multiple accounts could be created by administrator
Site Address	- Used in multi-site configurations for communication between sites - If not defined, SMS Service is used
Site System Database [SMS_SQL_RX_*sc*]	- Used by the site system(s) (Server Locator, Management Point) to access the site database server - Created by default during site server installation
Site System Connection	- Used by the site server to access site system(s) - Not created by default - If not defined, SMS Service is used - Creates files and directories on site system(s)
Remote Service [SMSSvc_*sc.*…]	- Used as identity for SMS services on site system(s) - Created when site system role is assigned

Table C-2. SMS Server\Server Application Accounts

NOTE: The letters *sc* represents the assigned SMS site code.

It is important to note that the SMS software does not require Site Address and Site System Connection accounts. When they are not defined, the SMS Service account is used instead.

To ensure that privileges are appropriately assigned, attention to some details of how these accounts are defined must be considered. These details include:

- The location of the security database where the accounts are defined impacts the scope of the assigned privileges. Accounts defined in Windows Administrator groups on domain controllers have privileges over all the systems within the domain.

- The Windows user groups assigned to the accounts also impact the assigned privileges. Several SMS accounts must be assigned to the Windows Administrators group on specific machines, but others do not require this privilege.

- Some accounts require specific Windows user rights to be assigned.

- An administrator should not change passwords for SMS application accounts that are automatically created and maintained by SMS.

The following table summarizes this information for each account.

Windows Account [Default Name]	**Where Defined**	**Privilege Notes**
SMS Service [SMSService]	Domain	Group membership: - local Administrators – site server Rights: - Log on as a service – site server
Server Connection [SMSServer_*sc*]	Local - site server	Group membership: - Site System to Site Server Connection Passwords: - Not to be changed by administrator – only default accounts
Site Address	Local - site servers	Group membership: Site to Site Connection
Site System Database [SMS_SQL_RX_*sc*]	Local - site database server	Group membership: - Site System to SQL Server Connection Password: - Not to be changed by administrator
Site System Connection	Local - site system	Group membership: - local Administrators – site system

Windows Account [Default Name]	**Where Defined**	**Privilege Notes**
Remote Service [SMSSvc_*sc*…]	Local - site system	Group membership: - local Administrators – site system Rights: - Log on as a service – site system Password: - Not to be changed by administrator

Table C-3. SMS Server\Server Application Account Privileges

NOTE: The letters *sc* represents the assigned SMS site code.

As indicated in the table, most of the SMS accounts can be defined on local systems where they are used. This helps to further reduce the attack surface that is presented by these accounts. The notable exception to this strategy is the SMS Service account. This account is used in several contexts (such as SMS Discovery) that require Windows domain access.

In consideration of this information and to ensure that the DODI 8500.2 IA control for Least Privilege is followed, requirements to reduce the access privileges of SMS application accounts are defined.

- *(EMS.0160: CAT II) The SA will ensure none of the following SMS accounts are defined in any Windows administrator-level group on a domain controller: SMS Service, Server Connection, Site Address, Site System Database, Site System Connection, and Remote Service.*

- *(EMS.0170: CAT II) The SMS Administrator will ensure for supported functions, Site System Connection and Site Address accounts are used instead of the SMS Service account.*

In addition to the SMS application accounts for server connections already discussed, there are two accounts for communication between servers and Advanced Clients. The following table describes these accounts.

Windows Account	**Function Notes**
Advanced Client Network Access	- Used by clients to access shares on non-SMS servers - Used for Client Push installation in NT domains
Client Push Installation	- Used by the Client Push installation method to install software on clients - If not defined, SMS Service is used.

Table C-4. SMS Server\Client Application Accounts

The need for these accounts depends on the environment and the configuration of the Windows clients. The Advanced Client Network Access account would not be needed where the user accounts utilized on clients already have access to any required network shares. It may be required if SMS Roaming is being utilized. The Client Push Installation account would not be

needed if Client Push Installation is not used, users already have administrative rights, or a different strategy is used to manage the privileges required for product installations.

For the same reasons noted for the other SMS application accounts, the location where the accounts are defined and the Windows user group membership impact the privileges assigned. The following table summarizes some of the account definition details for these accounts.

Windows Account	Where Defined	Privilege Notes
Advanced Client Network Access	Domain	Group membership: - Domain Users
Client Push Installation	Domain or Local – client	Group membership: - Domain Admins or - [local] Administrators – client

Table C-5. SMS Server\Client Application Account Privileges

It is important to note that the Client Push Installation account may have Windows administrator-level privileges over a wide span of clients. To mitigate the risk associated with this definition, organizations should consider a plan to selectively disable this account for periods when it is not being used.

In consideration of this information and to ensure that the DODI 8500.2 IA control for Least Privilege is followed, the following requirements to reduce the access privileges of SMS application accounts are defined.

- *(EMS.0180: CAT II) The SA will ensure the SMS Advanced Client Network Access account is not defined in any Windows administrator-level group on a domain controller.*

- *(EMS.0190: CAT II) The SMS Administrator will ensure for supported functions, a Client Push Installation account is used instead of the SMS Service account.*

Based on other requirements, there are certain SMS application accounts that are prohibited. The source of these considerations is:

  - The *Database STIG* requires the use of Windows authentication for Microsoft SQL Server.

  - An earlier requirement in this section prohibits the use of the Legacy Client.

- *(EMS.0200: CAT II) The SMS Administrator will ensure internal Microsoft SQL Server accounts (such as the SA pseudo database account) are not used as an SMS Site Database account.*

- *(EMS.0210: CAT III) The SA will ensure the following SMS Legacy Client accounts are not defined or are disabled: Client Connection, Client Services (DC), Client Services (non-DC), Client User Token (DC), Client User Token (non-DC), CCM Boot Loader (DC), CCM Boot Loader (non-DC), and Legacy Client Software Installation.*

NOTE: The letters DC represent domain controller.

It should be noted that the Client Connection account is automatically created during SMS installation and must be manually deleted or disabled.

The second category of Windows accounts defined for SMS are SMS administrator accounts. Because of the level of control that SMS has over client machines, SMS administrators are effectively SAs for all the clients. This fact underscores the need to document and control the assignment of SMS administrator privileges.

The following considerations should be noted concerning the Windows account used during SMS installation:

- This account requires local Windows Administrator privileges on the site server.
- This account automatically becomes an SMS administrator that is granted control over all SMS objects.

The final category of Windows accounts defined for SMS are SMS user accounts. As noted earlier, an SMS user account is an account used by individuals for non-privileged access to an SMS feature such as reporting. Although this level of access does not imply control over SMS, it does imply access to SMS data. As such, this access must also be documented and controlled.

Guidelines are necessary in order to manage SMS access privileges for all three of the SMS account types: application, administrator, and user. While any processes that implement these guidelines do not have to be specific to SMS accounts, the nature of SMS makes it particularly important to ensure these guidelines are followed to manage those accounts.

- *(EGC.0080: CAT II) The IAM will ensure a process is documented and implemented for the management of SMS accounts.*

- *(EGC.0090: CAT II) The IAM will maintain documentation of the assignment of SMS administrator and user accounts.*

- *(EGC.0050: CAT II) The IAO will ensure SMS application accounts are assigned the minimum privileges required.*

- *(EGC.0050: CAT II) The IAO will ensure SMS administrator accounts are assigned the minimum privileges required for the user's job function, as indicated in the local account documentation.*

- *(EGC.0060: CAT III) The IAO will ensure SMS administrator accounts are not used for non-privileged functions.*

During the installation of SMS, some Windows user groups are automatically created. Access to SMS privileges and data can be assigned to groups that represent roles associated with SMS operations. Using these groups in a role based access control strategy can be more efficient and secure than assigning access rights to individual accounts. The following table describes these groups.

Windows Group [Default Name]	**Function Notes**
SMS Administrators [SMS Admins]	- Used for SMS administrator accounts - The account used during the installation of SMS on the site server is placed in this group by default.
Site System to Site Server Connection [SMS_SiteSystemToSite ServerConnection_*sc*]	- Used for Server Connection account(s) - The default Server Connection account, SMSServer_*sc*, is placed in this group by default.
Site System to SQL Server Connection [SMS_SiteSystemToSQL Connection_ *sc*]	- Used for Site System Database account(s) - The default Site System Database account, SMS_SQL_RX_*sc*, is placed in this group by default.
Site to Site Connection [SMS_SiteToSite Connection_*sc*]	- Used for Site Address account(s)
Reporting Users [SMS Reporting Users]	- Used for users authorized to access SMS reporting

Table C-6. SMS Groups

NOTE: The letters *sc* represents the assigned SMS site code.

The location where these groups are defined and the members in the group are security considerations. The following table describes some of the definition details for these groups:

Windows Group [Default Name]	**Where Defined**	**Group Members**
SMS Administrators [SMS Admins]	Local - site server	Group members: - Users with SMS administrative privileges
Site System to Site Server Connection [SMS_SiteSystemTo SiteServerConnection_*sc*]	Local - site server	Group members: - Server Connection account(s) - Site Server (except Distribution Point) computer account(s)
Site System to SQL Server Connection [SMS_SiteSystemTo SQLConnection_ *sc*]	Local - site database server	Group members: - Site System Database account(s)
Site to Site Connection [SMS_SiteToSite Connection_*sc*]	Local - site servers	Group members: - Site Address account(s)

Windows Group [Default Name]	Where Defined	Group Members
Reporting Users [SMS Reporting Users]	Local - Reporting Point	Group members: - Non-privileged users with SMS reporting privileges

Table C-7. SMS Group Membership

Because membership in a Windows user group implicitly provides some type of access, the members of the group must be controlled.

- *(EMS.0220: CAT II) The IAO will ensure only documented SMS administrator accounts are members of the SMS Administrator group.*

- *(EMS.0230: CAT II) The SA will ensure only SMS application accounts or SMS server computer accounts are members of the Site System to Site Server Connection, Site System to SQL Server Connection, and Site-to-Site Connection Windows groups.*

- *(EMS.0240: CAT II) The SA will ensure only accounts of documented SMS reporting users are members of the Reporting Users group.*

Based on the earlier requirement in this section that prohibits the use of the Legacy Client, there is a Windows group that is not needed and is therefore also prohibited.

- *(EMS.0250: CAT III) The SA will ensure the Legacy Clients Internal Client Group Windows group is not defined.*

SMS objects represent logical elements used in the course of SMS operations. As with other technologies that use object-oriented design, SMS defines specific object classes. An object instance is an individual item that is a member of an object class. A consequence of this design is that actions on an object can be controlled using the context of a class or instance. For example, an SMS administrator may be permitted access to change configuration options for all SMS Collections or only for specific Collections.

The following object classes are defined in SMS:

- Advertisement
- Collection
- Package
- Query
- Report
- Site
- Software Metering Rule
- Status Message

SMS allows objects to be secured through the definition of object security rights. An object right represents the ability to perform certain actions on an object. For most SMS objects, rights can be controlled at both the class and instance level. So it is possible to permit a user or group of users the right to perform a certain action on all the objects in a class or only on certain object instances. This architecture enables a role based access control strategy to be applied to object permissions.

The following table summarizes the SMS object rights and the object classes to which they apply.

Object Right	Adver-tisement	Collec-tion	Packge	Query	Report	Site	Software Metering Rule	Status Msg
Administer	X	X	X	X	X	X	X	X
Advertise		X						
Create	X	X	X	X	X	X	X	X
Delegate	X	X	X	X	X	X	X	
Delete	X	X	X	X	X	X	X	X
Delete Resource		X						
Distribute			X					
Manage SQL Commands						X		
Manage Status Filters						X		
Meter						X		
Modify	X	X	X	X	X	X	X	
Modify Resource		X						
Read	X	X	X	X	X	X	X	X
Read Resource		X						
Use Remote Tools		X						
View Collected Files		X						

Table C-8. SMS Object Rights and Classes

Please refer to the *Microsoft Systems Management Server 2003 Concepts, Planning, and Deployment Guide,* for detailed information on SMS objects and object rights.

An example of Collection object security shows how SMS object security can be used. One instance of an SMS Collection object might be a group of client machines that are related by user organization. All client machines that belong to the Johnson Logistics group could be in a Collection named JHN-Log. By defining instance security for the JHN-Log Collection, a System Administrator for that group could be allowed to control SMS functions for only that group of clients.

The following characteristics apply to SMS object security:

- The SMS Administrator Console is the primary tool used to assign SMS object permissions.

- Class-level rights apply to all object types within the class.

- Instance-level rights apply to specific instances of an object type.

- Windows accounts that have object security rights must also have access to the related SMS WMI namespace.

- The account used to install SMS and the LocalSystem security context on the site server are granted permissions to all SMS objects by default.

Assigning SMS object access permissions to specific Windows accounts or groups represents a privilege assignment that must be documented and controlled to ensure that it remains limited.

- *(EGC.0090: CAT II) The IAM will maintain documentation of the assignment of SMS object rights.*

- *(EGC.0050: CAT II) The IAO will ensure only documented SMS object rights are assigned to SMS administrators.*

Because SMS implementation can vary significantly, it would be unrealistic to mandate requirements for all the object rights in every environment. However, the following specific considerations are relevant:

- There must always be at least one account with the class-level Administer right for an object class.

- Users who create an instance of an object are automatically assigned Read, Modify, and Delete rights for that object.

- Creating local Collection objects and applying instance security provides a way to scope administrative span of control.

- The Delegate object right allows a user or group to grant rights to other users for the objects that the first user or group creates.

- The Delete object right for Status Message objects could allow a user or group to prematurely delete audit data.

- The Manage SQL Commands object right allows SQL Server commands to be created through the SMS Administrator console. These commands have complete privileges to the SMS site database.

In view of these considerations, the following guidance is recommended with respect to assigning SMS object rights:

- Rights should be assigned at the instance level when possible. This is particularly desirable for Collection objects.

- The Delegate right should be assigned on a limited basis.

- The Delete right for Status Message objects should be assigned on a limited basis and at the individual account rather than group level.

- The Manage SQL Commands right should be assigned on a limited basis and at the individual account rather than group level.

There is one object right for which a specific requirement is necessary. The Use Remote Tools right controls the right to use the SMS Remote Tools feature on the Collection object class and instances. Because Remote Tools is a significant issue from the security perspective, some brief comments are required.

Remote Tools is an SMS feature composed of several tools designed for help desk assistance and troubleshooting support. The tools provide full control over the client machine, allowing an administrator to perform operations remotely as if they were physically present at the machine. The Remote Tools suite consists of: Remote Control, Remote Reboot, Remote Chat, Remote File Transfer, Remote Execute, SMS Client Diagnostics, and Ping Test.

Although Remote Tools offers a powerful capability, there are security issues in the implementation that make the use of the feature unacceptable. The problems include:

- Control of Windows administrative privileges may be bypassed for the tools user. The Microsoft *Scenarios and Procedures for Microsoft Systems Management Server 2003: Security* document states, "SMS Remote Tools also allow a non-administrator to execute programs in an administrative context, if they have sufficient permission to remote tools."

- Control of Windows administrative privileges may be bypassed for the client user. The *Microsoft Systems Management Server 2003 Operations Guide* states, "When an administrator uses Remote Execute to perform operations on the client, the user who is logged on to the client will also have elevated permissions and can then gain access to the same directories and files as the administrator." To aggravate this problem, if a network session failure occurs, this privilege elevation would not be terminated.

- SMS Collection security may be bypassed. The Remote.exe tool used to establish a Remote Tools connection includes a command line option (SMS:NOSQL). This option allows a connection to the client without accessing the SMS Site Database.

In view of these serious security issues, the use of Remote Tools must be prohibited. Access to the tools via the Remote.exe program is addressed through the file permission requirement specified in *Section C.2.1, Security Design and Configuration*. The following requirement addresses the Use Remote Tools object right.

- *(EGC.0050: CAT II) The SMS administrator will ensure the Use Remote Tools right is not granted to any account.*

C.2.3.3 Application Customization

Even though SMS is a highly configurable product, there may be instances in which an organization determines that the way in which a specific component functions does not meet the needs of the organization. In this case, a decision might be made to modify SMS functions by replacing or adding programs.

Microsoft offers an SMS software development kit (SDK) that includes "…documentation and sample applications for developing SMS applications that integrate with, or use, the SMS Administrator Console, SMS Provider (server-side applications), and client-side applications." This SDK provides tools to assist in modifying the designed function of SMS.

Because of the elevated privileges used during many SMS operations, the installation and propagation of improperly modified SMS functions could cause serious compromises of the confidentiality, integrity, or availability of a single server or a large number of client machines. Adherence to a configuration management process can help to mitigate this risk.

- *(EGC.0110: CAT III) The IAO will ensure any modified or added programs installed in an SMS configuration and used by a user or process with elevated privileges has been processed through a documented configuration management (CM) process.*

C.2.3.4 Auditing

Auditing for an information system is defined as a way to assess the adequacy of system controls and the degree of compliance with policies and procedures. To enable auditing, data must be continually collected. Because of the possible impact of SMS operations on the security posture of many client systems, maintaining audit data for SMS is essential.

To a large extent, SMS relies on the auditing support provided by the Windows operating system on which the SMS components execute. The application, security, and system logs maintained by Windows, when configured according the Windows OS security guidance, enable auditing of SMS account and data access.

The SMS software includes a Status System with features that supplement the audit functions in Windows. The Status System monitors SMS activity for a site and generates status messages.

The following characteristics are relevant to security:

- Status System messages are identified with a message severity level of error, warning, or informational.

- Status System messages are identified with a message type of milestone, detail, or audit.

- Audit messages provide an audit trail of actions taken in the SMS Administrator console that result in objects being added, modified, or deleted. All audit messages have a severity level of informational.

- Configuration options are available to control how status messages are processed for display and how long they are retained.

- Status filter rules can be configured to determine processing options such as disposition for status messages.

- The system includes status summarizers (Component, Site, Package, Advertisement) that provide a quick method of establishing the operational state of SMS.

- SMS can be configured to replicate status messages, status summaries, both, or neither up in the SMS hierarchy to the parent site.

The SMS Component Status and Site System Status summarizers can be used by administrators to detect of a loss of availability that may be due to a system compromise. For this reason, these components or an effective alternate need to be enabled.

- *(EMS.0260: CAT III) The SMS administrator will ensure the Component Status and Site System Status summarizers are enabled or an alternate on-line monitoring capability is maintained.*

- *(EMS.0270: CAT II) The SMS administrator will ensure the Component Status and Site System Status summarizers or their alternate are regularly reviewed for indications of inappropriate or unusual activity.*

SMS Status System audit data may be instrumental in determining the source of a compromise of the SMS application. In consideration of this fact and to ensure that the DODI 8500.2 IA control for Audit Record Retention is followed, steps must be taken to ensure that audit messages are retained.

- *(EMS.0280: CAT II) The SMS administrator will ensure status filter rules and the Delete Aged Status Messages maintenance task are configured so audit status messages are not deleted until they have been backed up.*

- *(EGC.0130: CAT II) The SMS administrator will ensure SMS audit data is retained for at least one year.*

- *(EGC.0170: CAT II) The SMS administrator will ensure SMS audit data is backed up not less than weekly onto a different system or media than the system on which the SMS server executes.*

C.2.3.5 Network Access

Most SMS functions are performed by interactions of servers and clients over network connections. This access generally occurs in one of the following ways:

- SMS Administrators access administrative controls for the SMS server software.

- SMS Reporting users access an SMS Reporting Point server to review SMS data.

- SMS application software on client machines accesses servers to send or receive status or configuration data.

- SMS application software on server machines accesses other servers to communicate status or configuration data.

It was noted in *Section C.2.2, Identification and Authentication*, that SMS does not perform user I&A services itself, but relies primarily on services provided by the Windows operating system. Therefore the ESM requirements for applications providing I&A, described in *Section 3.4.5, Network Access*, do not apply to SMS.

This section describes the considerations and requirements related to the security of these network access scenarios that are not specifically related to I&A services.

SMS administrators access the SMS server administrative controls through the SMS Administrator console. This client application is installed on the Site Server and on client machines used by SMS administrators. Due to the physical access restrictions for the SMS servers, access using a client machine would be more common. The administrator's access credentials, which would have been authenticated by the Windows OS at logon time, are passed to the Site Server for access.

To access SMS reports, users invoke the web browser on their client machine to access the Report Viewer web application on the SMS Reporting Point site system. The application uses IIS as the web server platform. Users are required to enter their Windows account and password to be authenticated for access.

Access to the web server on the Reporting Point site system could be from any browser client with network connectivity. This connection might represent access to a Government information system from a non-Government client. In consideration of the DODI 8500.2 Warning Messages IA control, privacy and security notices must be displayed to users.

- *(EMS.0290: CAT III) The SMS administrator will ensure the web server on the Reporting Point site system is configured to present a warning banner advising the user:*

  - *The system is a DoD system.*
  - *The system is subject to monitoring, recording, and auditing.*
  - *Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.*
  - *Use of the system constitutes consent to monitoring.*
  - *The system is for authorized US Government use only.*

Until the implementation of Service Pack 1 for SMS 2003, it is not possible to configure web server-based (e.g., SSL) encryption for the Reporting Point. Without such a capability, user passwords are transmitted in the clear when authenticating to the Reporting Point system. Please refer to *Section C.2.2, Identification and Authentication,* for the required action that addresses this issue.

The sensitivity of SMS data transmitted between servers and clients and the detail configuration data retained in the SMS Site Database would generally be classified at a level that reflected the data on the client machines. Although it might be technically possible for SMS to manage clients operating at different classification levels over a controlled interface, this has not been evaluated and has not been determined an acceptable configuration.

There are also potential network security issues when an SMS site hierarchy spans DoD and non-DoD networks. The ability for such SMS configurations to conform to the DODI 8500.2 IA control for Interconnections among DoD Systems and Enclaves has not been established.

- *(EGC.0220: CAT II) The IAM will ensure an SMS site hierarchy is not implemented across DoD information systems operating at different classification levels or across DoD and non-DoD systems or networks.*

As with any application host, the SMS servers are possible targets for attack. Because of the potential damage to the server and possibly a large number of clients that could result from a successful attack, the importance of detecting an attack on an SMS server is high. As described in the *Enclave STIG,* a host-based intrusion detection system (HIDS) provides this support.

- *(EGC.0230: CAT II) The IAO will ensure SMS servers are protected by a host-based intrusion detection system.*

The loss of integrity for SMS data transmitted between servers and clients can result in a number of problems. Data corruption in the SMS Site Database could result in invalid information being used to administer clients. It could be possible for clients to receive malicious code or data that would cause a loss of their confidentiality, integrity, or availability characteristics.

SMS provides mechanisms to help ensure that transmission integrity is maintained. These mechanisms are based on the use of PKI elements that support the use of digital signatures.

- SMS 2003 signs and authenticates data sent between sites using internally managed private/public encryption key pairs. Or environments with mixed SMS 2.0 and 2003 releases, an option exists to reject unsigned data from SMS 2.0 sites.

- Multiple methods are available for transmitting keys between sites. When the automatic method is used, a secure exchange option can be used to ensure the integrity of the keys. The manual method involves the use of the Hierarchy Maintenance tool (PreInst.exe) to unload and reload the keys.

Using the SMS integrity mechanisms helps to prevent data corruption and to deter some types of network attacks. This use conforms to the DODI 8500.2 IA control for Transmission Integrity Controls.

- *(EMS.0300: CAT II) The ESM administrator will ensure the "Do not accept unsigned data from sites running SMS 2.0 SP4 and earlier" Site Properties option is enabled.*

- *(EMS.0310: CAT II) The ESM administrator will ensure the "Require secure key exchange between sites" Site Properties option is enabled.*

Restrictions on access to the Hierarchy Maintenance tool are specified in *Section C.2.1, Security Design and Configuration*.

Another transmission integrity mechanism that SMS can take advantage of is server message block (SMB) signing. This facility ensures that data transferred using the SMB protocol is not altered during transmission. SMB signing is provided by the Windows OS platform and is enabled when the requirements in the *Windows NT\2000\XP Addendum* document and the associated NSA guides that address OS security configuration are followed.

C.2.4 Enclave Boundary Defense

This section describes the specific considerations and requirements for SMS that are related to the IA controls in the Enclave Boundary Defense subject area.

An organization may determine that remote access to administrative functions in SMS is necessary to maintain the availability of the SMS configuration. Remote access would most likely involve the use the SMS Administrator console application. Access to the SMS Report Viewer web application might also be deemed necessary for non-privileged users.

The requirements described in *Section 3.5, Enclave Boundary Defense*, apply to remote access to SMS and there are no unique considerations specific to SMS. The requirements address the DODI 8500.2 IA controls for Remote Access for Privileged Functions, Remote Access for User Functions, and VPN Controls.

- *(EGD.0010: CAT II) The IAO will ensure remote access to SMS applications is secured through the following:*

  - *Use of a managed access control point such as a remote access server in a DMZ*
  - *Session encryption using, according to the data classification, NIST-certified or NSA-approved cryptography*
  - *Strong user authentication resists spoofing, such as a two-factor system.*

- *(EGD.0020: CAT II) The IAO will ensure remote access for SMS administrators uses:*

  - *Session security measures such as a VPN configured in blocking mode to discard all but authorized traffic.*
  - *A process, which creates an audit log for each remote session.*

- *(EGD.0030: CAT II) The IAM/IAO will review the audit log for every remote session of an SMS administrator.*

- *(EGD.0040: CAT II) The IAO will ensure VPN traffic for remote SMS administrator sessions is visible to a network intrusion detection system (IDS).*

C.2.5 Physical and Environmental

This section describes the specific considerations and requirements for SMS that are related to the IA controls in the Physical and Environmental subject area.

The functions performed by SMS applications require elevated privileges to be used during operations. The proper use of some of these functions can have a significant, positive impact on the client machines that are served. A primary example of this impact would be the deployment of vendor security patches or updated antivirus signatures that would enhance the security of the client machines.

An improper use of SMS functions could have a proportional or more significant negative impact on client machines. Compromise of programs or data sent to clients could ultimately lead to a serious loss of the confidentiality, integrity, or availability characteristics of a large number of client machines.

In recognition of these significant possible impacts, attention to physical access restrictions for the SMS servers is more important than for typical application hosts. As a result, access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R. IA control for Access to Computing Facilities is essential.

- *(EGE.0010: CAT II) The IAO will ensure physical access to SMS application hosts is restricted to specifically authorized personnel.*

C.2.6 Continuity

This section describes the specific considerations and requirements for SMS that are related to the DODI 8500.2 IA controls in the Continuity subject area.

SMS can be used to provide business or mission essential functions such as the deployment of vendor security patches or antivirus signature updates. In this case, a loss of SMS availability could be a serious concern because a large number of client machines might be left vulnerable to some form of attack.

To ensure that the availability of SMS is maintained and in accordance with the DODI 8500.2 IA controls for Disaster and Recovery Planning and Identification of Essential Functions, requirements for recovery and restoration planning are needed.

- *(EGF.0010: CAT II) The IAM will ensure the disaster recovery plan for the enclave includes appropriate provision for the continuity of SMS if it is used to provide essential information assurance functions such as security patch management or antivirus signature deployment.*

  - *For SMS applications serving MAC III systems, resumption within five days of activation*
  - *For SMS applications serving MAC II systems, resumption within 24 hours of activation*
  - *For SMS applications serving MAC I systems, transfer to an alternate site for the duration of an event with little or no loss of operational continuity.*

- *(EGF.0020: CAT II) The IAM will ensure any SMS configuration provides essential information assurance functions such as security patch management or antivirus signature deployment is identified for priority restoration planning.*

Having a backup of SMS data is critical whether recovering from ordinary hardware problems, unexpected software errors, or a major computing facility event. The considerations relative to SMS data backup are as follows:

- The strategy and tools used to back up SMS data are directly related to how well an SMS configuration can be recovered. Because SMS data spans a number of individual files as well as tables residing in the Site Database, a specific tool must be used to get properly synchronized data in the backup.

- The frequency with which data is backed up is directly related to the difficulty or sometimes possibility of resuming operations.

The SMS product includes a Backup SMS Site Server task to properly capture SMS data for backup. It is described in the *Microsoft Systems Management Server 2003 Operations Guide*. This tool has the following characteristics:

- It is defined as one of the SMS Maintenance tasks and is disabled by default.

- It executes under the SMS_SITE_BACKUP service and stops basic SMS services on the Site Server while the backup is in progress.
- Its input includes the Site Database, SMS data files, registry keys, and system configuration information.
- Its input does not include data on Site Systems as that data could be re-created by the Site Server.
- Its output is referred to as the backup snapshot, consists of a number of directories and files, and is stored under a parent SMS backup directory specified by the administrator.
- The SMSbkup.ctl file contains site-specific configuration information for the task.
- The AfterBackup.bat file is an optional file that allows an administrator to specify commands to execute when the task completes. This could be used to create an archival copy of the backup data.
- It does not create a complete backup of the Site Server or Site Systems and therefore must be used in conjunction with another backup tool.

NOTE: As of the publishing date of this document, product testing indicates that there is an issue with implementing the Backup SMS Site Server task in STIG-compliant environments. The *Database STIG* requires that the SQL Server service account not be a member of the Windows Administrators group. When the Site Database Server is configured this way, the Backup SMS Site Server task fails due to insufficient authority to the dynamically created output directory. The workaround to this problem is to change the output destination of the sitedbdump command in the SMSbkup.ctl file. By specifying an existing directory with write permissions for the SQL Server service account, the task is able to complete normally.

The following requirements are designed to ensure that SMS data is backed up properly and that the backup data is protected in accordance with the DODI 8500.2 IA control for Data Backup Procedures.

- *(EGF.0030: CAT II) The SMS Administrator will ensure SMS data is managed appropriately to the MAC of the systems served by the ESM application.*

  - *For SMS configurations managing MAC III client systems, SMS data is backed up at least weekly.*

  - *For SMS configurations managing MAC II client systems, SMS data is backed up daily and the recovery media is stored at an off-site location affords protection in accordance with the mission assurance category and confidentiality level of the data.*

  - *For SMS configurations managing MAC I client systems, SMS data is backed up by maintenance of a redundant secondary system, not collocated, can be activated without loss of data or disruption to the operation.*

- *(EMS.0320: CAT II) The SMS Administrator will enable the Backup SMS Site Server task as part of the backup process for the SMS configuration.*

- *(EMS.0330: CAT II) The SMS Administrator will ensure logging is enabled for the SMS_SITE_BACKUP service.*

- *(EMS.0340: CAT II) The SMS Administrator will ensure the parent SMS backup directory is not located on the same logical drive partition as the parent SMS data directory.*

- *(EMS.0350: CAT II) The SA will ensure access to the SMS backup directories and files is restricted in accordance with the permissions in Appendix C.3.*

Copies of the SMS software could be critical when attempting to continue or resume operations after a disruptive event. If the operational servers and the original SMS installation materials are lost or inaccessible, installation of a backup copy of the software may be the only way to recover in the required timeframe. Protecting this copy is in accordance with the DODI 8500.2 IA control for Backup Copies of Critical Software.

- *(EGF.0040: CAT II) The IAO will ensure backup copies of software for any SMS configuration provides essential information assurance functions such as security patch management or antivirus signature deployment are stored in a fire-rated container or otherwise not collocated with the operational software.*

C.2.7 Vulnerability and Incident Management

This section describes the specific considerations and requirements for SMS that are related to the DODI 8500.2 IA controls in the Vulnerability and Incident Management subject area.

As with any application, it is possible that new vulnerabilities will be discovered in SMS components. Continued vigilance and quick action to implement security patches are the chief means to deter attacks based on the exploitation of product vulnerabilities.

Section 3.8, Vulnerability and Incident Management, describes the need for a vulnerability management process. Requirements that ensure utilization of the process are necessary to comply with the DODI 8500.2 IA control for Vulnerability Management.

- *(EGG.0010: CAT II) The IAM will ensure a vulnerability management process, which encompasses SMS applications and server hardware is documented and implemented.*

- *(EGG.0020: CAT II) The IAO will ensure all security related patches to SMS are applied and the completion is documented for each applicable asset.*

The current security patches applicable to SMS can be researched through Microsoft's Security Bulletin Search web site at http://www.microsoft.com/technet/security/current.aspx.

C.3 Systems Management Server Permissions

C.3.1 Windows Directory and File Permissions

The following notation is used in this section:

- [*SMS Folder*] – the high level directory structure that holds the subordinate directories in which SMS software programs and data reside
- [*SMS Data Folder*] – the high level directory structure that holds the subordinate directories in which the SMS SQL database resides
- [*SMS Toolkit Folder*] – the directory in which the SMS Toolkit software is installed
- [SITE_BACKUP_DESTINATION] – the directory in which the SMS_SITE_BACKUP service places SMS data backup files for the Site Server and the Site Database Server
- %SystemRoot% - the directory in which Windows is installed, e.g. C:\winnt
- [SMS Limit. Admins] – one or more groups of SMS administrators with a limited scope of authority
- [SQL Server account] – the account under which SQL Server executes
- [anonymous web account] – the account set up for anonymous access to IIS – commonly IUSR_*computername*
- [web application account] – the account set up for web applications – commonly IWAM_*computername*
- [*sc*] – the assigned SMS site code.

Object	Account Assignment	Permissions	STIG Reference
…\[*SMS Folder*]	Administrators SYSTEM SMS Admins SMS_SiteSystemTo SiteServerConnection_*sc* [SMS Limit. Admins]	Full Control Full Control Full Control Read & Execute Full Control	C.2.1 C.2.3
…\[*SMS Folder*]\bin\…\ACLreset.exe	Administrators SYSTEM	Full Control Full Control	C.2.1
…\[*SMS Folder*]\bin\…\PreInst.exe	Administrators SYSTEM	Full Control Full Control	C.2.1
…\[*SMS Folder*]\bin\…\Remote.exe	Administrators SYSTEM	Full Control Full Control	C.2.1
…\[*SMS Data Folder*]	Administrators SYSTEM SMS Admins SMS_SiteSystemTo SQLConnection_ *sc* [SQL Server account]	Full Control Full Control Full Control Full Control Full Control	C.2.3
…\[*SMS Toolkit Folder*]	Administrators SYSTEM SMS Admins [SMS Limit. Admins]	Full Control Full Control Full Control Full Control	C.2.1
[SITE_BACKUP_DESTINATION]	Administrators SYSTEM SMS Admins	Full Control Full Control Full Control	C.2.6
…\SMS_CCM	Administrators SYSTEM INTERACTIVE [anonymous web account] [web application account]	Full Control Full Control Read & Execute Read & Execute Read & Execute	C.2.3

Object	Account Assignment	Permissions	STIG Reference
…\SMSADMIN	Administrators SYSTEM SMS Admins [SMS Limit. Admins]	Full Control Full Control Full Control Full Control	C.2.1
…\SMSADMIN\bin\…\Remote.exe	Administrators SYSTEM	Full Control Full Control	C.2.1
…\SMSADMIN\bin\…\PreInst.exe	Administrators SYSTEM	Full Control Full Control	C.2.1
…\SMSADMIN\bin\…\ACLreset.exe	Administrators SYSTEM	Full Control Full Control	C.2.1
%SystemRoot%\system32\ccmcore.dll	Administrators SYSTEM INTERACTIVE [anonymous web account] [web application account]	Full Control Full Control Read & Execute Read & Execute Read & Execute	C.2.1
%SystemRoot%\system32\SMSAccountSetup.ini	Administrators SYSTEM SMS Admins	Full Control Full Control Full Control	C.2.1
%SystemRoot%\system32\CCM	Administrators SYSTEM INTERACTIVE	Full Control Full Control Read & Execute	C.2.1

Table C-9. SMS Directory and File Permissions

C.3.2 Windows Shared Folders Permissions

The following notation is used in this section:

- [*sc*] – the assigned SMS site code.

Object	Account Assignment	Permissions	STIG Reference
CAP_[*sc*] *	Administrators	Full Control	C.2.3
SMS_[*sc*]	Authenticated Users Domain Computers	Change Change	C.2.3
SMS_Site	Authenticated Users Domain Computers	Change Change	C.2.3
SMS_SUIAgent	Authenticated Users Domain Computers	Change Change	C.2.3
SMSClient	Authenticated Users Domain Computers	Change Change	C.2.3

Table C-10. SMS Shared Folder Permissions

* - The CAP_[*sc*] share is not used in SMS configurations having only Advanced Clients.

C.3.3 WMI Namespace Permissions

The following notation is used in this section:

- [all] – all available permissions
- [SMS Limit. Admins] – one or more groups of SMS administrators with a limited scope of authority

Namespace	Account Assignment	Permissions	STIG Reference
Root	Administrators Authenticated Users	[all] Execute Methods Provider Write Enable Account	C.2.3
Root\CCM	Administrators Authenticated Users	[all] Execute Methods Provider Write Enable Account	C.2.3
Root\CIMV2	Administrators Authenticated Users	[all] Execute Methods Provider Write Enable Account	C.2.3
Root\SMS	Administrators Authenticated Users SMS Admins [SMS Limit. Admins]	[all] Execute Methods Provider Write Enable Account Execute Methods Provider Write Enable Account Remote Enable Execute Methods Provider Write Enable Account Remote Enable	C.2.3

Namespace	Account Assignment	Permissions	STIG Reference
Root\NetworkModel	Administrators Authenticated Users	[all] Execute Methods Provider Write Enable Account	C.2.3

Table C-11. SMS WMI Namespace Permissions

This page is intentionally left blank.

APPENDIX D. LIST OF ACRONYMS

ACF	Adapter Configuration Facility
ADE	Application Development Environment
AEF	Application Extension Facility
API	Application Programming Interface
ARF	Application Registration File
BDT	Bulk Data Transfer
BITS	Background Intelligent Transfer Service
C&A	Certification and Accreditation
CAP	Client Access Point
CCB	Configuration Control Board
CCITT	International Telegraph and Telephone Consultative Committee
CDS	Class Definition Statement
CIM	Common Information Model
CIO	Chief Information Officer
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLI	Command Line Interface
CM	Configuration Management
CMIP	Common Management Information Protocol
CMOT	CMIP Over TCP
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CORBA	Common Object Request Broker Architecture
COTS	Commercial-Off-the-Shelf
DAA	Designated Approving Authority
DBMS	Database Management System
DC	Domain Controller
DEN	Directory Enabled Networks
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DM	Distributed Monitoring
DMI	Desktop Management Interface
DMTF	Distributed Management Task Force
DMZ	Demilitarized Zone
DoD	Department of Defense
DODI	DoD Instruction
EIF	Event Integration Facility
EKMS	Electronic Key Management System
ESM	Enterprise System Management

FCAPS	Fault management, Configuration management, Accounting management, Performance management, Security management
FIPS	Federal Information Processing Standard
FSO	Field Security Operations
GEM	Global Enterprise Manager
GID	Group ID
GOTS	Government-Off-the-Shelf
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I&A	Identification and Authentication
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IATF	Information Assurance Technical Framework
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IIS	Internet Information Services
ILT	Instrumentation Library Type
IT	Information Technology
ITM	IBM Tivoli Monitoring
ITU	International Telecommunication Union
JTF-GNO	Joint Task Force - Global Network Operations
KMI	Key Management Infrastructure
LDAP	Lightweight Directory Access Protocol
MAC	Mission Assurance Category
MDist	Multiplexed Distribution
MFA	Management Functional Areas
MIF	Management Information Format
MMC	Microsoft Management Console
MOM	Microsoft Operations Manager

NIAP	National Information Assurance Partnership
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OID	Object Identifier
OOB	Out of Band
ORB	Object Request Broker
OS	Operating System
OSI	Open Systems Interconnection
OSS	Open Source Software
PCIM	Policy Core Information Model
PDI	Potential Discrepancy Item
PKI	Public Key Infrastructure
PM	Program Manager
POC	Point of Contact
PPS	Ports, Protocols, and Services
PPSM	Ports, Protocols, and Services Management
RBAC	Role-Based Access Control
RDBMS	Relational Database Management System
RFC	Request for Comment
RIM	RDBMS Interface Module
RME	Resource Model Engine
S/MIME	Secure Multipurpose Internet Mail Extensions
SA	System Administrator
SDID	Short Description ID
SDK	Software Development Kit
SIPRNet	Secret Internet Protocol Router Network
SLP	Server Locator Point
SMB	Server Message Block
SMS	Systems Management Server
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide
SUS	Software Update Services
TBSM	Tivoli Business Systems Manager
TCP/IP	Transmission Control Protocol / Internet Protocol
TEC	Tivoli Enterprise Console
TMA	Tivoli Management Agent
TME	Tivoli Management Environment

TMF	Tivoli Management Framework
TMR	Tivoli Management Region
TNR	Tivoli Name Registry
UI	User Interface
UID	User ID
URL	Uniform Resource Locator
USM	User-based Security Model
VMS	Vulnerability Management System
VPN	Virtual Private Network
WBEM	Web-Based Enterprise Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
WUS	Windows Update Services
XML	Extensible Markup Language