IBM HARDWARE MANAGEMENT CONSOLE (HMC) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

27 April 2023

Developed by DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The IBM Hardware Management Console (HMC) Overview provides guidance for secure configuration and usage of the IBM HMC Licensed Internal Code application to manage System z resources. “HMC Application” will be used to reference the licensed Internal Code application for the remainder of this document. The HMC is a closed platform. Specifically, this means that the customer is not given access to the underlying operating platform and is not allowed to install and run other applications on the HMC. All configuration of the HMC is accomplished using tasks provided by the HMC Application as it is the only user interface (UI) available to HMC. This document covers HMC Versions 2.9.2 and 2.10.0.

The HMC is required to be a network-attached device since this is the path HMC uses to communicate with various System z resources. This overview will describe the functions of the HMC and the Support Element. It will briefly cover the security and configuration settings of the HMC Application and how it is utilized to control the HMC/Support Element.

This document applies to all DOD-administered or -managed data center networks, assets, and security domains. The requirements set forth in this document are designed to assist Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and System Administrators (SAs) in support of protecting DOD network infrastructures and resources.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances

and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. TECHNOLOGY OVERVIEW

This section provides background information on the HMC/Support Element and discusses general security considerations involved with using the HMC Application.

2.1 What is a Hardware Management Console (HMC)?

HMC is used to manage System z machines, including partitions, input/output (I/O) channels, and other resources in the System z hardware. It includes features for problem analysis, automatic real-time notification of system events, and automatic reconfiguration and repair. The HMC also provides views of system resources and provides capabilities for system administration, including real-time monitoring, backup, and recovery. The HMC is a management solution that helps you to manage your server resources in an efficient and effective way. The HMC is much more than just a console; it is also a hardware platform interface that provides:

- An expert system that performs analysis of system-level failures—besides server-level failures—determines the root cause and automatically notifies the customer and IBM Service provider of the problem, the impact of the problem, the fix, and the impact of the fix.
- Automatic backup and restore of configuration and customization data for the system's hardware components.
- Automatic and autonomic firmware change management for the servers, which includes automatic monitoring of firmware levels, updates, backups, retrieval, and concurrent application of updates without any customer effort or involvement.
- A highly reliable *call home* server with automatic failover.
- Weekly information about the performance and use of systems in the field. This data is used, in part, to support On-Demand software billing.

CNSSI 1253 defines the required controls for DOD systems, based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

A single HMC can be used to manage all System z and zServers that any customer has, while simultaneously allowing complete redundancy for up to 32 HMCs without additional customer management requirements. The HMC communicates with each server through the server's Support Element (SE). When tasks are performed at the HMC, the commands are sent to one or more SEs that, in turn, issue commands to their servers. Servers can be grouped at the HMC so that a single command can be passed along to as many as all of the servers that are defined to the HMC. One HMC can control up to 100 SEs, and one SE can be controlled by up to 32 HMCs.

The HMC UI provides the functions that you need through an object-oriented UI. Through this design, you can directly manipulate the objects that are defined to the HMC and be made aware of changes to hardware status as they are detected. The main functions are:

- Single system image and single point-of-control for multiple systems. One single HMC can manage all System z systems.
- Exception driven with color/pattern support to illustrate problems to end-user.
- Up to 32 HMCs can simultaneously manage any given system.
- Full replication support among HMCs, which allows any HMC to control any System z.
- Support for complete remote operation.
- Transmission Control Protocol/Internet Protocol (TCP/IP) Simple Network Management Protocol (SNMP) agent and Application Programming Interface (API) that provides the ability to build automation routines or collect and forward information using management APIs in REXX, Java, or C/C++ running on z/OS, Windows®, OS/2, and Linux.
- Single object operations to the System z SEs, which eliminates the need for working near the machine.
- Interface for console integration.
- Primary Interface for Human for Hardware Operation:
    - Drag-and-drop for functions, such as Initial Program Load (IPL), RESET, and LOAD.
    - Classic object-oriented workplace UI.
    - Tivoli® Converged "Tree" style UI.
    - Web-browser based.

The HMC provides the platform and UI that controls and monitors the status of the System z system using the two redundant SEs that are installed in each System z. System z implements two fully redundant interfaces, known as the Power Service Control Network (PSCN), between the two SEs and the Central Processor Complex (CPC). Error detection and automatic switch-over between the two redundant SEs provide enhanced reliability and availability.

When tasks are performed at the HMC, the commands are sent to one or more SEs, which then issues commands to their CPCs. The CPCs can be grouped at the HMC so that a single command can be passed along to as many as all of the CPCs that are defined to the HMC.

While an HMC is a physical personal computer (PC) machine, when used as the term HMC, it represents the underlying technology of the HMC. So, when referencing HMC Version 2.10.0, we are talking about the HMC system as a whole, including the current version of its UI.

To ensure the integrity and security of the environment, the HMC and SE operate on a closed platform, which means that the customer is not provided access to the underlying operating platform and is not permitted to install or run additional applications on the underlying operating platform that the HMC or SE are using. The sole purpose of HMC and SE is to provide a platform for the execution of the HMC application.

2.2 What is a Support Element (SE)?

The HMC communicates to each CPC through the SE. An SE is a dedicated ThinkPad that is used to monitor and operate a system. The IBM System z has an *integrated SE*; that is, the SE is located inside of the same frame that the CPC is located. An alternate SE is also provided for the option to automatically failover and switch from the primary SE to the alternate SE if a hardware problem occurs.

The SE, plus an alternate SE, is supplied with each server to provide a *local* console to monitor and operate the system. The SE is usually used by service personnel to perform maintenance operations on the system. Using the communication path through the SE, the HMC can perform numerous operations and tasks to assist in the maintenance and operations of the CPC, logical partitions, I/O, and other physical and logical entities on the system.

The firmware that is responsible for executing system management tasks runs on different system components: the processor module itself, the cage controller, and the SE.

The SE is connected to the cage controllers through a redundant service network, which is an Ethernet network. The cage controllers in the CPC cage are connected to the processor modules through the XMsg-engine[1] hardware in the clock chip. When firmware components that reside on the SE must communicate with firmware components that run on the processors, they communicate to the firmware on the cage controller.

2.3 What is the HMC Application?

One of the primary roles of the HMC Application is to provide a secure access to the HMC. The web-based graphical user interface (GUI) allows for the management and control of the various System z® resources. The main UI provided to the end user allows for the execution of a variety of tasks, some that affect the HMC itself while others target System z® resources. It is this UI that provides access to all of the features of the HMC *Licensed Internal Code* application. Additionally, this UI is the only access provided for customer use.

The web-based UI provided locally on the HMC is provided using a browser. This design point makes it technically straight forward to provide the same UI to a remote browser via the network. Although technically straightforward, there are security aspects to allowing remote access that should be considered.

2.3.1 Remote User Access

For the web-based GUI of the HMC to be accessed from a remote browser, the ***Customize Console Services*** task needs to be used to enable remote access. Enabling remote user access

1 The XMsg engine is a hardware interface on the clock chip that connects the cage controller to the CEC. The XMsg engine contains read/write first-in first-out (FIFO) registers for data exchange as well as several control lines, among them two high-priority reset lines for resetting the communication interface in case of errors. It is connected to the cage controller using the serial support interface (SSI) and is also accessible by millicode.

allows for incoming requests to be accepted by the HMC. By default, the HMC blocks all incoming Hypertext Transfer Protocol (HTTP) requests at the network level. Enabling this feature will only result in the HMC accepting secure, secure sockets layer (SSL)-based, HTTP requests.

2.3.2 Web Server Certificates

All remote user access to the HMC is performed using SSL-encrypted connections. When first started, the HMC will create a self-signed certificate that can be used for encrypting data for remote user connections. In many cases, this is sufficient for the customer and nothing further needs to be done by the SA.

For DOD sites, the SA needs to make use of the ***Certificate Management*** task to create a certificate that meets the needs of the DOD requirements. This task provides a full complement of -related functions from creating a self-signed certificate to providing all the tools needed to allow for the use of a DOD-authorized Certificate Authority certificate.

2.3.3 User IDS

Before the UI or tasks can be accessed, either remotely or locally, a user must first be authenticated by the HMC. This is accomplished by logging into the HMC using a user ID and password. By default, the HMC is shipped with a set of five default user IDs. These five user IDs align with a set of traditional user classifications for the HMC. The default user IDs and their classifications are shown in Table 2-1.

Table 2-1: Default HMC User IDs and Their Classifications

User ID	Classification
OPERATOR	Basic operator
ADVANCED	Advanced operator
SYSPROG	System programmer
ACSADMIN	Access administrator
SERVICE	Service personnel

These default user IDs provided illustrate how different user IDs can be used to allow for the operational control of the System z® resources by operations, administrative, and service personnel, with a variety of levels of expertise and needs. In order for the HMC to be secured, these default user IDs need to be removed from the HMC or, at a minimum, the passwords for these default user IDs must be changed. In addition, for security and auditing purposes, it is important for each user of the HMC to have his/her own user ID. User IDs for the HMC must not be shared among multiple people to provide a more secure HMC. The SA can use the User Profiles task to manage the user IDs for the HMC. In addition to providing the expected functions of adding, removing, and altering user IDs, this task also allows for the following characteristics of a user ID to be controlled:

- The password rule to be used for the user ID.

- The roles the user ID is associated with:
  - The password to be used for the user ID.
  - The ability to temporarily disable a user ID.
  - The ability to force the password for a user ID to be changed at the next login.
  - The ability for the user ID to remotely access the HMC.
  - The number of incorrect login attempts allowed before the user ID becomes temporarily disabled, along with the amount of time the user ID is to be temporarily disabled.
  - Control of how long before, and if, a user ID is to be disabled due to lack of activity (e.g., not used for login).
- Various timeouts for the user ID, such as:
  - the minimum time between password changes;
  - the time period before the user ID is automatically disconnected due to inactivity;
  - the time period before the user ID is forced to verify the login session by, specifying the correct password; and
  - the time period before the user ID is automatically disconnected due to the correct password not being used for verification.

2.3.4 Passwords

Keeping passwords non-trivial is an important aspect to the security of any computer system. There is no set of "rules" that would work for all customers; for this reason, the HMC allows for the definition and enforcement of user-supplied custom password "rules". As shipped, the HMC provides three default password "rules" as defined in Table 2-2.

Table 2-2: Default HMC Password Rules

Rule Name	Description
Basic	Simple rule that allows for alphabetic and numeric characters and defines a minimum length of four (4) and a maximum length of eight (8). This rule is provided mainly to allow for the traditional password of the default user IDs to continue to be used. **Note**: This is the default rule for newly created user IDs. For a more secure HMC, new users should be modified to use a rule that meets security requirements for the company.
Strict	Defines a minimum length of six (6) and a maximum length of eight (8), allowing alphabetic and numeric characters, and requiring the password to start and end with an alphabetic character. The rule also prevents the password from having the same character more than two (2) times in a row and causes the password to expire in 180 days.
Standard	Defines a minimum length of six (6) and a maximum length of 30 and allowing

Rule Name	Description
	for alphabetic, numeric, and special characters. The password must start and end with an alphabetic or special character and must have at least one alphabetic character in between. The rule also prevents the password from having the same character more than two (2) times in a row and causes the password to expire in 186 days. In addition, the password cannot be the same as one of the last four (4) passwords for the user and cannot be similar in more than three (3) characters with the last password for the user.

Each customer will review the default set of password rules, with respect to STIG guidance, and change, delete, or add to these rules so that s/he adheres to the STIG. The ***Password Profiles*** task can be used by the SA to manage the password rules for the HMC. This task provides the ability for the following set of characteristics to be defined for these password "rules":

- Minimum length.
- Maximum length.
- Number of days before the password expires.
- Maximum number of times a character can be used consecutively within a password.
- Number of times a password must be changed before a previous password can be re-used.
- If the password is to be treated in a case sensitive manner or not.
- Specific rules as to the types of characters that can be used, and in which positions, for a password.

2.3.5 User Roles

There are two types of HMC "roles": task roles and managed resource roles. Task roles are used to group tasks into sets that make sense for specific classifications of users. Likewise, managed resource roles are used to group either specific types and/or specific instances of System z® resources that are allowed to be managed by a specific class of users. The HMC ships the following default "roles" as defined in Table 2-3.

Table 2-3: Default HMC User Roles

Managed Resource Role	Description
All Directors/Timers Managed Objects	Allows access to both defined and undefined Director/Timer managed resources.
All Fiber Saver Managed Objects	Allows access to both defined and undefined Fiber Saver managed resources.
All Managed Objects	Allows access to all Defined CPC, Undefined CPC, CPC Image, and Coupling Facility managed resources.
Defined Directors/Timers Managed Objects	Allows access to defined Director/Timer managed resources.
Defined Fiber Saver Managed Objects	Allows access to defined Fiber Saver managed resources.

Managed Resource Role	Description
Limited Managed Objects	Allows access to all Defined CPC, CPC Image, and Coupling Facility managed resources.
z/VM Virtual Machine Objects	Allows access to all defined z/VM virtual machine objects.

Task Role	Description
Access Administrator Director/Timer Tasks	Administrative tasks for Director/timer managed resources.
Access Administrator Fiber Saver tasks	Administrative tasks for Fiber Saver managed resources.
Access Administrator Tasks	Administrative tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
Advanced Operator Tasks	Advanced operational tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
Operator Tasks	Operational tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
Service Fiber Saver Tasks	Service-related tasks for Fiber Saver managed resources.
Service Representative Director/Timer Tasks	Service-related tasks for Director/Timer managed resources.
Service Representative Tasks	Service-related tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
System Programmer Tasks	System Programmer tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
Universal Director/Timer Tasks	Director/Timer tasks allowed for all users.
Universal Fiber Saver Tasks	Fiber Saver tasks allowed for all users.
z/VM Virtual Machine Tasks	All tasks relating to z/VM virtual machine images.

The SAs can use the ***Customize User Controls*** tasks to define new task or managed resource roles that make sense in their environment. Likewise, as previously mentioned, the ***User Profiles*** task can be used to associate one or more roles with a specific user ID.

2.3.6 Data Replication

The HMC Application provides many different configuration options for controlling end user operation controls. This along with the fact that most customers have multiple HMCs for redundancy indicates that this configuration needs to be performed separately at each HMC. There is nothing to stop this mode of operation; the data replication feature of the HMC is provided to help in large installations with many HMCs.

The SA can use the ***Configure Data Replication*** task to configure a master HMC that is used to configure all of the user ID-related characteristics for that HMC and a set of other “slave” HMCs. To avoid data being compromised, all data sent between HMCs is encrypted.

2.3.7 Service and Support

The HMC Application is used by IBM service personnel to perform service-related tasks to the HMC and the associated System z® resources being managed by the HMC. Differing customer needs result in a wide range of controls put in place for the service personnel, ranging from being treated like any other HMC user to being completely locked out of the HMC. The HMC provides the customer with the controls needed to control access for service personnel to the HMC.

2.3.8 Service and Support Access

This default setup provides IBM service personnel with all the tasks needed to service the HMC and its associated System z® resources. This user ID is just like every other HMC user ID; it can be altered or deleted to meet the security needs of the customer. Of course, making radical changes in this area can affect IBM's ability to service the HMC and the associated System z® resources, so any changes made should be reviewed with IBM service personnel for their awareness.

There is a special HMC user ID that can be used by IBM Product Engineering to perform in-depth problem determination. This user ID, PEMODE, differs from other HMC user IDs in several ways:

- This user ID cannot be altered or deleted by the customer.
- The password for this user ID is unique to each HMC and changes on a daily basis.

This user ID cannot be managed by the SA like other user IDs; the HMC does provide controls for this user ID to be disabled by the customer. This can be done using the ***Customize Product Engineering Access*** task. By disabling product engineering access, this user ID becomes completely unusable and prevents any access to the HMC by product engineering.

Note: The product engineering user ID is not enabled for remote access and requires the user to revalidate the password every 2 hours while it is being used.

2.3.9 Remote Support

One of the most important roles the HMC plays is its role as the connectivity point for communicating with IBM. One or more HMCs can be configured to act as this connectivity point for redundancy. There are many reasons an HMC may need to communicate with IBM and some of them are to:

- Report problems detected by the HMC or one or more of the System z® resources being managed.
- Transmit additional data needed by IBM support personnel for problem analysis.
- Download firmware fixes for the HMC and/or System z® resources being managed.
- Report hardware inventory, system configuration, and system availability data.

- Process On-Demand orders to update System z® server capacity.

The HMC can use various methods for communicating back to IBM to match different customer environments and requirements. The methods are through the Internet or through a modem.

2.3.10 Internet Connectivity

With Internet Connectivity, the HMC uses a client-provided Internet connection to connect to IBM support personnel. All the communications are handled through TCP sockets (which always originate from the HMC) and use SSL to encrypt the data that is being sent back and forth.

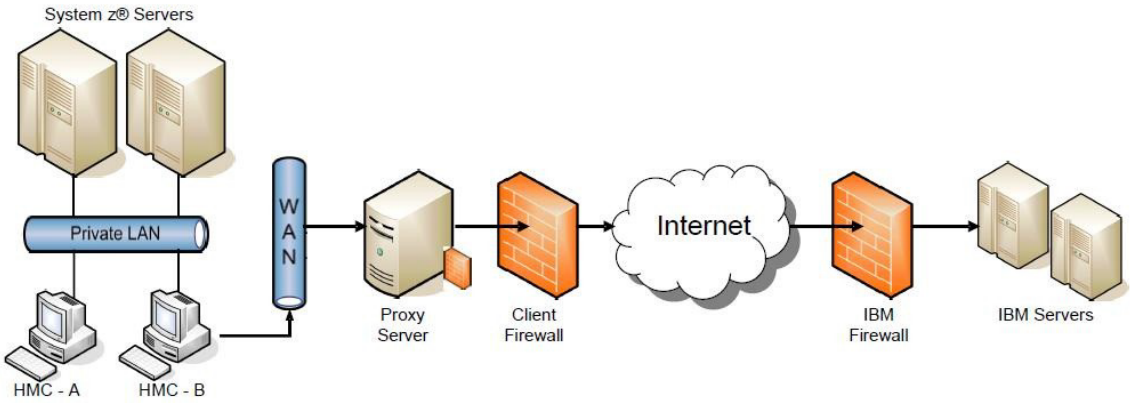
The network interface of the HMC used to provide this Internet connectivity should not be the same one used for connectivity to the System z® resources being managed. This is easily accomplished since the HMC provides multiple network interfaces, one of which can be used for Internet connectivity and another which can be used for managing the System z® resources.

The HMC for security purposes will connect to the Internet through a client-configured proxy server.

2.3.11 Internet Connectivity with a Proxy Server

Figure 2-1 shows the HMC connecting to IBM using a client-provided proxy server.

Figure 2-1: Internet Connectivity Using Proxy Server



To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC #2616) and the CONNECT method. For security purposes, basic proxy authentication (RFC #2617) will be configured so that the HMC authenticates before attempting to forward sockets through the proxy server. For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. The proxy server will also limit the specific IP addresses to which the HMC can connect.

2.3.12 Modem Connectivity

The HMC uses one of several configured phone numbers to dial the modem to connect to the AT&T Global Network. After the modem connects, the HMC authenticates itself and establishes a Point-to-Point Protocol (PPP) session between the two modems. After the PPP session has finished, AT&T allows IP connections through a "Fenced Internet". This completes the network between the HMC and the IBM service delivery center.

All the communications between the HMC and the IBM servers are handled through TCP sockets. These sockets always originate from the HMC and use SSL to encrypt the data that is being sent back and forth. The "Fenced Internet" connection uses a firewall to limit access between the HMC and the Internet. Specifically, it limits communication to HMC-initiated connections to the authorized IBM IP addresses needed to connect to the IBM service delivery center.

2.4 Securing Access to the HMC

While the HMC provides a complete set of controls for the customer to manage user access and capabilities, none of this matters if the HMC is left logged on in a non-secure location or if the HMC can easily be attacked via the network. For these reasons, both physical and network security are critical to the security of the HMC.

2.4.1 Physical Security

The physical location of the HMC can play a large role in how the HMC is treated from a security perspective. Many times, the HMC is located in a secure room which, of course, provides the best security. However, securing physical access to the HMC does not negate the need to make use of the other security features of the HMC, such as automatically disconnecting inactive user IDs, employing strict password rules, etc.

In addition to the security features provided by the HMC *Licensed Internal Code* application, the PC platform of the HMC also provides some features that can provide additional physical protection to prevent the PC from being booted using code other than that installed on the PC hard drive. These functions are mainly provided as part of the Basic Input Output System (BIOS) in the PC:

- Change the startup device settings in BIOS to prevent the booting of removable media, such as a compact disc (CD) or diskette.

  Note: If this level of security is used, this setting will need to be disabled for several, infrequent processes used by IBM service personnel, such as hard disk restore and Engineer Change EC upgrades.
- A power-on password can be set in BIOS to prevent unauthorized changes to BIOS settings.
- Unattended start mode can be set in BIOS to allow the HMC to reboot without the power-on password following restoration of power after an unplanned outage. However, the

keyboard and mouse at the HMC will remain locked until the power-on password is entered.

2.4.2 Network Security

The HMC must be attached to a network so that it can manage the System z® resources associated with it. In some cases, for HMCs located close to the System z® servers it is managing, this network is a "private" network that is fully contained on a single raised floor. However, when a customer has multiple data centers or attaches the HMC to its corporate Intranet to allow for remote access, network security is of utmost importance.

Since the HMC can be a multi-homed machine (e.g., it has multiple network interfaces), it can be connected to a "private" network containing the System z® resources and the corporate Intranet at the same time. In fact, this is a very prevalent customer configuration since it provides a level of physical separation for the System z® resources while, at the same time, allowing for the use of advanced HMC capabilities such as remote access and Internet connectivity for remote support.

The HMC Application includes a full-function firewall that is used to control network access to the HMC. As previously described, by default, the HMC allows for virtually no inbound network traffic. As different features of the HMC are enabled (e.g., remote access, SNMP-based automation, etc.), additional inbound network traffic is allowed. The HMC utilizes a set of TCP/IP ports to allow the inbound network traffic.

In addition to these inbound requests, the HMC also initiates requests to the System z® resources that it is managing as well as to other HMCs. The HMC utilizes a set of TCP/IP ports to allow the outbound network traffic.

2.4.2.1 Communications

From a network perspective, the HMC uses TCP/IP for all of its communications. Both Internet Protocol, Version 4 (IPv4) and Internet Protocol, Version 6 (IPv6) are fully supported by the HMC. When using inbound or outbound functions, it may be necessary to define rules in customer-owned firewall roles and the use of both IPv4 and IPv6 protocols may require rules to be defined for each of these protocols. Additionally, even though the HMC is a management focal point for various System z® resources, the HMC does not provide any IP forwarding capabilities.

The management of the various System z® resources requires network communications between the HMC and the resources. It is important for this communications to be secure. There are different types of network communications for each of the System z® resources.

2.5 Logging and Audit Trails

Even when the security characteristics of a computer system like the HMC is understood and trusted, there needs to be facilities in place so that the security of the system can be monitored and audited to ensure that it is performing as it should. For this reason, the HMC uses its *security log* to log important security-related events. The customer can use the ***View Security Log*** task to view these security events and also the ***Format Security Logs to DVD-RAM*** task to offload security logs for storage.

The security log contains entries for security-related events. The following is a short list illustrating the types of events contained in the security log:

- User logon/logout.
- Failed logon attempts.
- Password changes.
- Creation, deletion, alteration of user IDs.
- Creation, deletion, alteration of user roles.
- Creation, deletion, alteration of System z® server activation profiles.
- Execution of disruptive commands.
- Change management activity.
- Remote support calls.
- Network traffic blocked by the firewall.

The security log is intended to be used by the customer to determine when events occur that have altered the security characteristics of the HMC or that indicate an action was taken that could have security implications to the HMC and/or the System z® resources that it is managing.

2.6 Classified Systems Configuration Requirements

In some data centers, requirements exist for setting up classified systems. This section describes this type of an environment.

A Strict Separation Virtual Machine Monitor (SVMM) restricts the allocation of resources so that there is absolutely no sharing of objects amongst their clients. Although Processor Resource/System Manager (PR/SM) may be configured as a SVMM, it may also be configured to run in a mode where sharing of some resources is permitted. To be used as a classified system SSVMM, PR/SM must be configured in the following manner:

1. Devices must be configured so that no device is accessible by more than one partition (although they may be accessible by more than one channel path).
2. Each I/O (physical) control unit must be allocated to a single partition in the current configuration.
3. The Security Administrator must not reconfigure a channel path unless all attached devices and control units are attached to that path only.

4. The Security Administrator must ensure that all devices and control units on a reconfigurable path are reset before the path is allocated to another partition.
5. No channel paths must be shared between partitions.
6. The amount of reserved storage for a partition must be zero.
7. The SA must ensure that the number of processors and co-processors dedicated to activated partitions is less than the total number available.
8. Dynamic I/O configuration changes must be disabled (i.e., changes require a power-on reset). Note: This does not apply if the classified system is the only LPAR on the system.
9. I/O Priority Queuing must be disabled.
10. Workload Manager must be disabled so that the central processing unit (CPU) and I/O resources are not managed across partitions.
11. No partition must be configured to enable HiperSockets (Internal Queued Direct I/O).
12. Partitions must be prevented from receiving performance data from resources that are not allocated to them (no partition should have global performance data control authority).
13. At most, one partition can have I/O configuration control authority (i.e., no more than one partition must be able to update any Input-Output Configuration Data Set (IOCDS) and this partition must be administered by a trustworthy administrator (i.e., the administrator of this partition is considered a SA of the classified system.
14. The Security Administrator must ensure that write access is disabled for each IOCDS, unless that IOCDS is to be updated (the current IOCDS must not be updated).
15. The Security Administrator must verify any changed IOCDS after a power-on reset with that IOCDS before any partitions have been activated (the Security Administrator may determine whether the IOCDS has been changed by inspecting the date of the IOCDS).
16. No partition should have cross-partition control authority (i.e., no partition should be able to reset or deactivate another partition).
17. No partition must have coupling facility channels that would allow communication to a Coupling Facility partition.[2]
18. Replication of HMC Customizable Data must be disabled.

2 The coupling facility provides shared storage and shared storage management functions for the sysplex (for example, high speed caching, list processing, and locking functions). Applications running on z/OS and OS/390 images in the sysplex define the shared structures used in the coupling facility. These images efficiently share data so that a transaction processing workload can be processed in parallel across the sysplex.