DRAFT

PERIPHERAL
SECURITY TECHNICAL IMPLEMENTATION GUIDE
Version 1, Release 0

29 OCTOBER 2004

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF FIGURES

APPENDICES

LIST OF FIGURES

SUMMARY OF CHANGES

This is a new document and there are no changes from previous releases.

This page is intentionally left blank.

1. INTRODUCTION

This *Peripheral Security Technical Implementation Guide* (*STIG*) provides the technical security policies, requirements, and implementation details for applying security concepts to Commercial-Off-The-Shelf (COTS) hardware peripheral devices. For this STIG peripheral will mean, "any device that allows communication between a system and itself, but is not directly operated by the system"[1]. However, this document does not deal with devices found wholly contained within the main cabinet of the computer or, with the exception of AB switches, those devices connected via legacy parallel and serial interfaces.

1.1 Background

Peripheral devices are commonly used within the Information Technology (IT) community and some, if not all, of the technologies addressed within this STIG are found at any Department of Defense (DOD) location. Unfortunately, this presence also brings dependence and vulnerabilities. Malicious or mischievous individuals will try to exploit vulnerabilities and uninformed individuals will inadvertently but invariably expose the infrastructure to new vulnerabilities. Because many of these devices need to interoperate with multiple information systems (ISs), their default configuration settings often are not sufficient for strong security posture. In other cases these devices have no user configurable settings and it is the handling of the device that provides the security. This STIG will provide the guidelines to deploy these devices in a secure manner.

The vast numbers of devices that fall into the category of peripherals preclude the inclusion of specific configuration settings for all devices made by all manufactures. Therefore, this document will provide general guidelines. Appendices have been added to provide product specific requirements.

It should be noted that 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 ISs 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 unclassified but sensitive information.

[1] *Dictionary of Computing, Fourth Edition, ISBN:1901659461.*

1.3 Scope

The requirements and recommendations set forth in this document will assist Information Assurance Officers (IAOs) and Information Assurance Manager (IAMs) in securely deploying these peripherals on ISs in all DOD locations hereafter referred to as sites. Since new peripheral devices are introduced at an ever-increasing rate, sites should be proactive in adopting these guidelines to secure future devices not waiting for them to be specifically covered by updates of this STIG. It is a more secure posture to temporarily restrict a new technology than to ignore the use of it until the technology is address within a STIG. The responsible Configuration Control Board (CCB) will approve revisions to site systems that could have a security impact. Therefore, before implementing Peripheral Device security measures, the IAO will submit a change notice to the CCB for review and approval.

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**" implies 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 will make 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**" is considered 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 have 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.

1.6 DISA 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@ritchie.disa.mil**.

1.8 Document Revisions

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

This page is intentionally left blank.

2. SAN DISK SYSTEMS

2.1 Introduction

According to the Storage Networking Industry Association, a storage area network (SAN) is any high-performance network whose primary purpose is to enable storage devices to communicate with computer systems and with each other. This definition applies regardless of the interconnect technology used (Fibre Channel, Ethernet, or other). However, since most SAN implementations use Fibre Channel switch fabrics for interconnectivity, this initial version of the Peripheral STIG will focus on securing Fibre Channel SANs.

Storage networks use various storage devices such as disk and tape drives, RAID subsystems, robotic libraries, and file servers. A network connected storage environment increases the availability, improves LAN bandwidth usage, and increases accessibility of DOD data by linking multiple storage devices on a dedicated storage network and making the storage space available to distributed application servers and clients. However, as is often the case, the needs of the user for faster and more accessibility, can conflict with the need to keep DOD data secure.

SANs are becoming a viable and even preferred solution for data management on the networks. SANs are an excellent way of centralizing data to provide high performing and easy to manage data access. Managing a storage area network not only involves providing highly-available data access and optimal performance, it is essential that all data on the SAN be completely secure at all times. The storage industry is witnessing a rapid increase in servers and storage considerations within SANs. Greater storage accessibility means that more access points to the data will exist. This includes LAN, Campus, MAN, WAN, and wireless access to the stored data. More access points mean that more attention must be paid to protecting information from unauthorized access.

Attaching a network to a set of storage resources presents security risks, which are not present when storage was simply connected to a server. A key component to protecting the SAN is to enable the highest security settings available in the server. However, with a SAN, storage can be directly attached to and extended over a public network, such as the Internet, thus circumventing traditional operating system settings. It is then critical to ensure the integrity and confidentiality of the data by other means. Network security policies must consider protection of data while in storage and during transmission.

2.2 Components of the SAN

This section discusses the typical components of the SAN architecture. SANs vary in complexity. Smaller SANs may not use all the components listed while larger scaled installations may use a complex network for interconnecting multiple storage devices and server systems. Components may have both physical (e.g. port connections) and logical (e.g. zones) relationships to one another.

The network connected storage environment may include some or all of the following components:

- SAN fabric (Usually Fibre Channel switches)

- SAN fabric configuration management and monitoring software
- SAN fabric Security and Access Control Software
- Storage devices (disk arrays, tape devices, etc)
- Hosts (application servers and client-level hosts)
- Host bus adapters (HBAs) which attach the hosts to the fabric switch
- Network interface cards (NICs)
- Connection cabling, connectors, and optical to electrical signal converters (GBIC)
- Remote mirroring and replication storage applications
- Backup and recovery software

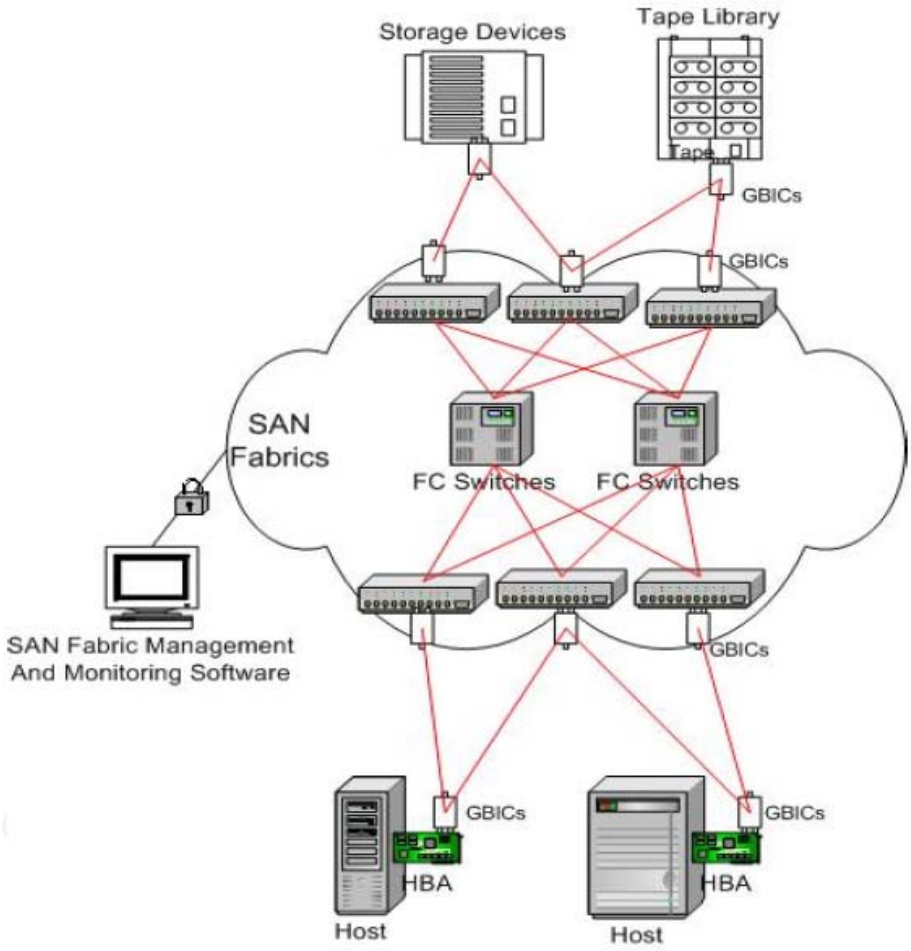

Figure 2-1 Sample SAN Architecture

Since the Fibre Channel Switches or SAN fabric form the intelligent foundation of the SAN, it is vital that the switches are chosen with security of the DOD environment in mind. The following areas will impact the sites ability to secure the SAN and thus, should be carefully considered prior to purchasing a SAN fabric.

- Choose switches that support open industry standard should be used whenever possible
- Switches must be configurable for use in a fully redundant architecture

- Management and Monitoring Software should be robust, easy to use, and should support security protocols for secure configuration from a management server.
- Switch must have access control capabilities such as passwords and configurable guards against configuration changes.
- Application Program Interface (API) so that security applications from authorized DOD sources may be integrated into the SAN

2.3 SAN Security Concepts

Fibre Channel continues to grow as the architecture of choice for providing high-speed, robust, and scalable interconnects for SANs. Fibre Channel enables the separation of storage and server, unlike the small computer system interface (SCSI), where the interconnect scheme is confined to the servers' cabinetry. A host of new security challenges consists of the exposure of critical business data to increased distances, greater availability, heterogeneous implementations, automatic re-configuration, increased services and changes in strong model administration.

Without security, clients and application servers could see and use all devices attached to the SAN across the network connection making the devices more vulnerable to an attack. The administrator must make sure that users are only accessing and aware of the files to which they are authorized access. The two most common methods of providing access control security at this level in a SAN environment are zoning and Logical Unit (LUN) masking.

2.3.1 Zoning

Zoning separates the SAN into subnetworks. The concept is similar to virtual local area networks (VLANs) in the way they establish a "virtual SAN" within a SAN. The system administrator (SA) uses zoning to group each host and storage device, then associates security and access policies to each group, thus preventing groups of devices from seeing or interacting with each other. Zoning may be used to group devices according to operating system, application, function, physical location, or other criteria as needed. SAN architectures provide port-to-port connections among servers and storage devices through bridges, switches, and hubs. Zoning is an efficient method of managing, partitioning, and controlling pathways to and from storage devices on the SAN fabric; as a result, storage resources are maximized, and data integrity and data security are maintained.

- *(N/A: CAT I) The IAO will ensure that zoning is used to protect the SAN.*

- *(N/A: CAT II) The IAO will ensure that hard zoning is used to protect the SAN.*

- *(N/A: CAT II) The IAO will ensure that the default zone visibility setting for the SAN is set to "none".*

There are two methods of zoning, soft zoning, which is controlled by software, and hard zoning, which is controlled by hardware. The following sections discuss these two zoning methods.

2.3.1.1 Hard Zoning

Hard zoning is accomplished by linking ports on the fabric through use of hardware and software. For a specific zone, hard zoning uses only World Wide Port Names (WWPN) to specify each device. Fabric switches and host bus adapters store and maintain copies of the zone's access control lists (ACLs) to verify access and routing prior to data transfers. Hard zoning requires each device pass through the switch's route table. For example, if two ports are not authorized to communicate with each other, the address will not appear in the route table and communication between those ports is blocked. The devices are physically unable to communicate with devices in another hard zone.

The exact details of how hard zoning is accomplished can differ significantly by vendor. Multi-vendor environments containing switches from different vendors will also impact zoning implementation. Rigorous testing must be employed to ensure that zoning works as intended, with repeated testing of all zones after adding or deleting switches.

The zoning process uses the ACL in the switch as the primary source of port numbers and worldwide names for each hard zone. The ACL is updated and propagated to other switches within the zone when changes are made to the zone. However, the HBA on the initiating devices also store a copy of the ACL. It is possible for the zoning information stored on the HBA to include old addresses, which are no longer allowed in the newly established zoning rules. The HBA's memory is non-persistent, thus a good practice is to force a state change update in the affected HBAs immediately after making zoning changes.

Zoning by ports is easier to implement, but less flexible than zoning by World Wide Name (WWN). Hard zoning does not allow zones to overlap or "follow" a zone member (device) that has its switch port changed. In other words, the zones need to be reconfigured whenever a Fibre Channel device in the SAN changes its switch port when hard zoning is used. When soft zoning is moved from one port to another, soft zoning remains associated with the device.

- *(N/A: CAT III) The IAO will ensure that hard zoning, using World Wide Port Names (WWPN), is used to protect the SAN.*

- *(N/A: CAT I) The IAO will ensure that the zoning tables on all affected HBAs are reset (force a state change update) after making zoning changes.*

2.3.1.2 Soft Zoning

Zoning can also be implemented through software (Simple Name Server (SNS)) that runs inside the fabric switch. By using the WWNN and the WWPN, soft zoning allows members of the zone to be defined. When a host logs into the SAN and requests available storage devices, the SNS will check the zoning table for all storage devices available for that host and the host will only see those devices that have been defined in the zoning table. However, it may be possible with certain operating systems for an attacker to bypass the SNS and go directly to the storage device thus soft zoning may present a potential security issue.

2.3.1.3 Configuring Zoning Components

Zone configurations are based on either the WWN of the device or the physical port that the device plugs into. Zoning components include zones, zone members, and zone sets.

A zone is made up of servers and storage arrays on the SAN fabric that can access each other through managed port-to-port connections. Devices in the same zone can recognize and communicate with each other, but not necessarily with devices in other zones, unless a device in that zone is configured for multiple zones.

Zone members are devices within the same assigned zone. Zone member devices are restricted to intra-zone communications, meaning that these devices can only interact with members within their assigned zone. Unless a device is configured for multiple zones, a zone member interacting with devices outside its assigned zone is not permitted.

Zone members are recognized by port number or WWN; A WWN is a 64-bit number that uniquely identifies zone members.

- *(N/A: CAT III) The IAO will ensure that soft zoning is not used to protect access to SANs used to store sensitive DOD data.*

2.3.2 LUN Masking

Many administrators use LUN masking to limit access to storage devices to further protect the SAN. LUN masking is a method of masking the unit number associated with the disk array. It is configured at the server console using the masking utility provided with the HBA driver. A single large disk array device can be sub-divided to serve a number of different hosts that are attached to the disk array through the SAN fabric. However, unlike zoning, the system administrator can also limit access to each individual LUN inside the disk array by assigning specific LUNs to specific server(s).

LUN masking can be done either behind the disk array port or at the server HBA. It is more secure to mask LUNs at the disk array device, but not all disk array devices have LUN masking capability.

By filtering access to certain storage resources on the SAN, LUN masking goes one step beyond zoning alone. Also, by using a piece of code residing on each host connected to the SAN, LUN masking can be provided through hardware (i.e. intelligent bridges, routers, or storage controllers) or software. LUN masking effectively masks off the LUNs that are not assigned to the application server, allowing only the assigned LUNs to appear to the application server's operating system.

Managing paths by LUN masking is a reasonable solution for smaller SANs, however, this method requires an extensive amount of configuration and maintenance and is not recommended for larger SANs with large number of hosts or LUNs on the storage array. The complexity of maintaining this method of access control may itself present a security issue, as it is unlikely that the administrator will maintain the configuration for a large SAN.

2.4 Network and Host Security

This section contains general security policies, which apply to SAN network devices in the enclave and represent general best practices in any data-networking environment.

- *(N/A: CAT III) The IAO will ensure that SAN devices are added to the site System Security Authorization Agreements (SSAAs).*

- *(N/A: CAT II) The IAO will ensure that SANs are compliant with overall network security architecture, appropriate enclave, and data center security requirements in the Network Infrastructure STIG and the Enclave STIG.*

- *(N/A: CAT II) The IAO will ensure that prior to installing SAN components (servers switches, and management stations) onto the DOD network infrastructure, components are configured to meet the applicable STIG requirements.*

- *(N/A: CAT II) The NSO will ensure that servers and other hosts are compliant with applicable Operating System (OS) STIG requirements.*

- *(N/A: CAT I) The IAO will ensure that vendor supported, DOD approved, anti-virus software is installed and configured on all SAN hosts (servers) in accordance with the Desktop Application STIG on SAN servers and management devices and kept up-to-date with the most recent virus definition tables.*

- *(N/A: CAT II) The NSO will maintain a current drawing of the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment.*

- *(N/A: CAT II) The NSO will ensure that all the network level devices interconnected to the SAN are located in a secure room with limited access.*

2.4.1 Securing the Fabric Switch to Switch Connection

This section discusses policies for securing the interconnection between fabric switches. A switch may attempt to illegally join a fabric or change the fabric topology. This is usually accomplished by having physical access to the SAN fabric. However, a management interface may enable this as well from a remote location. An unauthenticated switch may be able to change the layout of the environment or cause denial of resource access to legitimate users.

- *(N/A: CAT III) The NSO will configure all fabric switches to use FIPS 140-1/2 validated encryption algorithm to protect Switch to switch communications.*

- *(N/A: CAT III) The NSO will ensure that fabric switches are protected by encryption and DOD PKI and that the manufacturer's default keys are changed prior to attaching to the SAN Fabric.*

- *(N/A: CAT II) The NSO will disable all network management ports on the SAN fabric switches except those needed to support the operational commitments of the sites.*

- *(N/A: CAT II) The NSO will ensure that SAN management is accomplished using the out-of-band or direct connection method.*

2.4.2 Securing the Management Interface

To ensure that a trusted and secure management console-to-fabric communications layer exists, management-to-fabric technologies can use PKI and other encryption technologies. PKI and other encryption help ensure that the management console or framework used to control the fabric is authentic and authorized. In addition, encryption methodologies can restrict the number of switches on the fabric from which management and configuration changes are propagated to the rest of the fabric.

- *(N/A: CAT III) The NSO will ensure that communications from the management console to the SAN fabric are protected using DOD PKI.*

- *(N/A: CAT III) The NSO will ensure that the manufacturer's default PKI keys are changed prior to attaching the switch to the SAN Fabric.*

- *(N/A: CAT III) The SA will configure the SAN to use FIPS 140-1/2 validated encryption algorithm to protect management to fabric communications.*

- *(N/A: CAT I) The NSO will ensure that all SAN management consoles and ports are password protected and that all manufacturer default passwords are changed.*

- *(N/A: CAT I) The NSO will ensure that all SAN management consoles and ports are password protected with a strong (two-factor) password.*

- *(N/A: CAT I) The NSO will ensure that the manufacturer's default passwords are changed for all SAN management software.*

2.4.3 Securing the Host to Fabric Connection

This section addresses security policies and technologies associated with the connection between the host servers (via the associated HBA) and the fabric switches. The goal is to secure this type of connection by explicitly allowing only authorized Fibre Channel HBAs of authorized hosts. All other HBAs are denied from attaching to the port by default. Host to fabric security technologies ACLs the same way that router ports use ACLs. Security concepts, which apply to ACLs in the router arena should also be applied in securing the SAN environment. Enforcement of access control on each port by using ACLs, prevents unauthorized and intruder hosts from attaching to the fabric via any port. These restrictions may also be based on the source and destination addresses of the IP packet as well as the service type (e.g., Simple Mail Transfer Protocol (SMTP), e-mail, Telnet, and Hypertext Transfer Protocol (HTTP)).

- *(N/A: CAT I) The NSO will ensure SAN fabric ACLs and firewall rules are based on a policy of Deny-by-Default with blocks on all services and protocols not required on the given port or by the site.*

- *(N/A: CAT III) The NSO will ensure that that all attempts to any port, protocol, or service that is denied is logged.*

- *(N/A: CAT I) The NSO will ensure that only authorized IP addresses are allowed SNMP access to the SAN devices.*

- *(N/A: CAT II) The NSO will ensure IP addresses of the hosts that are permitted SNMP access to the SAN management devices belong to the internal network.*

- *(N/A: CAT II) The NSO will ensure SNMP is enabled in the read only mode; Read/Write will not be enabled unless approved by the NSO.*

- *(N/A: CAT III) The NSO will ensure that hard zoning rather than soft zoning is used to provide access control to the SAN.*

Typically, network facilities based on traditional networks provide connectivity between end-user platforms and server system components. It is also possible to connect end-user platforms directly to the Fibre Channel network, allowing the client host to directly access storage devices.

- *(N/A: CAT III) The IAO will ensure that end-user platforms are not directly attached to the Fibre Channel network and may not access storage devices directly*

2.5 Data Backup and Disaster Recovery

In most scenarios, data back up to onsite or offsite storage devices is dependent on the use of the common LAN or WAN infrastructure and its associated traffic characteristics. With a SAN, these operations take place independent of the primary network, increasing the operational performance. Backup and recovery procedures are critical to the security and availability of the SAN system. If a system is compromised, shut down, or otherwise not available for service, this could hinder the availability of resources to the warfighter.

Traditionally, disasters involving data loss were handled using recovery from tape. The use of SANs allows for various methods of automated data backup and “warm” availability of this data in the event of a loss of the primary data image. Efficiently maintaining a redundant data image requires a low latency, high availability network infrastructure, for which today’s storage networks are suitable. Total connectivity for the loss of the primary site would result in an image backup site emerging as the active image site. Recovery of the primary site is met with it being updated by the current active image and a decision whether to fall back to the original primary image server.

- *(N/A: CAT II) The IAM will ensure that a written disaster plan exists that provides for the resumption of mission or business essential functions in accordance with local policy and the requirements of DODD 8500.2.*

- *(N/A: CAT II) The IAO will ensure that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with the operational software.*

- *(N/A: CAT II) The IAO will ensure that data backup is performed in accordance with the requirements of DODD 8500.2 and the sites local policy.*

This page is intentionally left blank.

3. KEYBOARD, VIDEO, AND MOUSE SWITCHES (KVM)

This section will address KVM switches and A/B switches. KVM switches are used to connect a single keyboard, video monitor, and mouse to multiple ISs saving space and equipment. They are commonly found within testing laboratories, server rooms, and with the advent of small inexpensive switches, on desktops to reduce clutter. A/B switches switch a single peripheral between multiple ISs or multiple peripheral devices on a single interface for a single IS. Switch(es) will refer to both KVM and A/B switches unless otherwise noted.

The KVM switches are considered to be one of three categories demarked by their physical characteristics and intended use. These classifications are single user KVM switch, multi user analog KVM switch, and a multi user network attached KVM switch. Each switch will be defined within its own section. To simplify the reading of this document, duplicate requirements within the three categories will be presented within the section for each category rather than being consolidated in a general switch section referred to by each separate section. The requirements for a single user KVM switch are found within its section.

Analog KVM switches are switches that are directly connected to a single set of human interface hardware, keyboard, monitor, and mouse, that function as the only set of interface hardware for each system attached to the KVM switch. It has no remote access properties or network properties.

Network attached KVM switches may have analog components attached but also have the ability to be accessed via client software either over a network or via dialup remote access. The client software may be either a proprietary software client supplied by the switch manufacturer or a web browser. The network protocol may be a standard protocol like TCP/IP or may be proprietary. The switch may allow any combination of connections; single user to any single IS, multiple users to a single IS, or multiple users to multiple but different ISs.

3.1 Single User KVM Switch

A single user KVM switch is a simple analog KVM switch attached to four or fewer ISs of the same classification level located within a single user's work area for the purpose of consolidating multiple sets of keyboards, video monitors, and mice for a single user to one set. These switches will be manually operated and have minimal programmable menus or features. The single user KVM switch definition and policies will only apply if the classification level of all ISs involved is unclassified. In all other cases either the multi user analog KVM switch or multi user network attached KVM switch definitions or policies will apply.

The reason for these switches being restricted to unclassified ISs are to allow for their use with a minimal amount of documentation. With classified ISs the DAA for all ISs attached to the KVM switch would have to approve the attachment.

3.1.1 Administrative Requirements

To ensure that the users have been advised of their responsibility when using switches the IAO will maintain a written user agreement. Additionally, the IAO will ensure that documentation

explaining the users responsibilities when using a switch and the correct operation of the switch is supplied to the users in either a section of the Security Features Users Guide (SFUG) or a separate document. It should, at a minimum, describe the correct switching procedures and include these steps.

1. Logging onto an IS.
    a. Identify the classification of the IS currently selected.
    b. Use the login and passwords appropriate for that IS.
    c. Verify the classification of the present IS by checking the classification label/banner.
    d. Begin processing.
2. Switching between ISs.
    a. Screen lock the IS you are currently working on if the IS supports this capability.
    b. Select the desired IS with the switch.
    c. Enter your user identifier and password to deactivate the screen lock on the newly selected IS.
    d. Verify the classification of the present IS by checking the classification label/banner.
    e. Begin processing.

- *(KVM01.001.00: CAT IV) The IAO will maintain written user agreements for all users authorized to use the KVM or A/B switch.*

- *(KVM01.002.00: CAT III) The IAO will maintain and distribute to the users a SFUG that describes the correct uses of the switch and the users responsibilities.*

3.1.2 Physical Requirements

Although the KVM switch itself is considered an unclassified object, it must be protected in a manner suitable for the IS with the highest classification to which it is connected. For example, if the switch is connected to a sensitive but unclassified system and an unclassified system then it will be protected in the same manner as the sensitive but unclassified system. This also means that physical access to the KVM switch will be restricted to individuals that are allowed physical access to all ISs attached to the switch.

A smart (intelligent or programmable) keyboard will not be attached to a KVM switch. These keyboards present the possibility of data being transferred between ISs of different classifications.

NOTE: This includes keyboards with smart card readers, USB ports, and removable media drives.

Any wireless keyboards or mice used with a KVM switch will be compliant with the requirements set forward in the current version of the Wireless STIG.

To avoid inadvertent compromise of and IS attached to a KVM switch the following steps need to be taken.

1. The desktop backgrounds will display classification banners at the top and bottom of the screen.
2. These banners will state the overall classification level of the IS in large bold type.
3. These banners will have a solid background color assigned using the following scheme:
   Yellow for SCI,
   Orange for TS,
   Red for Secret,
   Blue for Confidential,
   and Green for Unclassified.
   When ISs have similar classification levels but require separation for other reasons, the use of unique colors for different ISs or networks is permissible.
4. These banners will identify the IS if space is available.

Further the screen lock (or screen saver) application present on all IS connected to the KVM switch will display the maximum classification level of the IS and identify the IS using the same banners as described in the paragraph dealing with desktop background banners above. The screen lock application will require re-authentication of the user before releasing its lock on the keyboard and video.

All KVM switches will be labeled as required for all government owned equipment. Additionally all switch positions, cables, and connecters will be labeled with the identity and security classification of the IS to which they are attached. Any unused port/connector on a KVM switch will be blocked with tamper resistant seals.

- *(KVM01.003.00: CAT 1) The IAO or SA will ensure that the KVM switch is physically protected in accordance with the requirements of the highest classification for any IS connected to the KVM switch.*

- *(KVM01.004.00: CAT II) The IAO or SA will ensure that no smart (intelligent or programmable) keyboard is used in conjunction with a KVM switch.*

- *(KVM01.005.00: CAT II) The IAO or SA will ensure that any wireless keyboards or mice attached to KVM switches are in compliance with the current Wireless STIG.*

- *(KVM01.006.00: CAT III) The IAO or SA will ensure that the desktop backgrounds of ISs attached to a KVM switch are labeled with banners in accordance with this STIG.*

3.1.3 Configuration Requirements

A single user analog KVM switch should not be configurable. Though it is desirable to have a single user analog switch that has minimal configurable features. Switches that are configurable will comply with the following security measures.

If the KVM switch is configurable the configuration will be locked from unauthorized modification. This lock will be either a DOD compliant password or PKI authentication. If the configuration is not lockable or is not locked then all required configuration settings are considered findings regardless of their settings. If the KVM switch is capable of automatically toggling between ISs this feature will be disabled. This feature can lead to the inadvertent display and compromise of information.

Many KVM switches have "hot key" features where a specific key sequence or combinations of keys pressed simultaneously will cause a specific action to be taken by the KVM switch. Examples of these actions could be, toggle to the next available system, turn on/off auto toggling between connected ISs, and other actions. The only "hot key" feature that is allowed with a KVM switch is one that brings up a menu of ISs attached to the KVM switch allowing the user to select the IS they wish to use in lieu of pushing the manual switch button. All other "hot key" features, including the feature to manually toggle between ISs, will be disabled within the lockable configuration. The following "hot key" feature(s) are specifically forbidden and will be disabled within the lockable configuration.

If the KVM switch has a configuration, the IAO or SA will maintain a backup of the configuration. If a machine-readable backup is not possible then a document describing the settings selected will be maintained.

- *(KVM01.009.00: CAT II) If the KVM switch has configurable features, the IAO or SA will ensure that the configuration is protected from modification with a DOD compliant password. PKI authentication is acceptable and preferred to password authentication.*

- *(KVM01.010.00: CAT II) The IAO or SA will ensure that the feature for automatically toggling between ISs is disabled.*

- *(KVM01.011.00: CAT III) The IAO or SA will ensure that the only "hot key" feature enabled is the menu feature that allows the user to select the IS to be used from the displayed menu.*

- *(KVM01.012.00: CAT II) The IAO or SA will ensure that the "hot key" feature that toggles to the next available system is disabled.*

- *(KVM01.013.00: CAT III) The IAO or SA will ensure that a machine-readable or a paper-document backup is maintained for the configuration of the KVM switch.*

3.2 Multi User Analog KVM Switch

Multi user analog KVM switches are analog KVM switches found in any environment that do not meet the requirements for single user analog KVM switches. Most often this would be a server area where there are many separate servers each of which needs occasional administrative access. A KVM switch can save both space and money by allowing a single set of hardware support all of the servers. However, these multi user switches are not restricted to a single set of hardware provided that there is no network component involved. Another environment where these switches would commonly be found is the laboratory environment where there are many test ISs.

3.2.1 Administrative Requirements

In addition to administrative requirements of single user switches the IAO is required to meet the following requirement. The IAO will maintain a written description of all KVM switches used. This description will contain the manufacturer, model number, version number, and serial number. The description will also describe all ISs connected to the KVM switch, the IS's classification levels, and the location of the KVM switch.

- *(KVM02.003.00: CAT III) The IAO will maintain a written description of the KVM switch, the ISs attached to the KVM switch and the classification level of each IS attached to the KVM switch.*

3.2.2 Physical Requirements

The Physical requirements for a multi user analog KVM switch are the same as the physical requirement for the single user KVM switch found is section 3.1.2.

3.2.3 Configuration Requirements

There are analog KVM switches that fill the whole gambit from being controlled by mechanical switches, with no configurable features, to touch sensitive switches that are fully configurable with menus, multiple colors and "hot key" triggered scripts. If the switch is configurable, it should be able to allow for user identification with userids and user authentication with either passwords or PKI. The KVM switch should restrict the IS access by users. An example of this type of restriction would be user A is allowed access to systems 1 and 2 but not 3, user B is allowed access to system 3 but not 1 and 2, and user C is allowed access to all systems.

These requirements will be followed in addition to those listed in the single user analog KVM switch found in section 3.1.3.

If the KVM switch supports any of the above functions, it will be configured to use that functionality. If the KVM switch does not support the previous functionality it must cares should be given in restricting access to the switch to only users that need to access the IS attached.

Since the knowledge of the configuration password would allow a user to change the security profile of the KVM switch, the password will expire and be changed every 90 days or when an administrator who knows the password no longer has need for access to the configuration. If the KVM switch has the ability to expire the password this feature will be used otherwise there will be a written procedure requiring the IAO or SA to change the password every 90 days and documenting the change.

No analog KVM switch will be connected in a manner that supports remote access via a dialup modem. These devices are not designed to be network communications devices and do not supply as robust security either in authentication or encryption of transmitted data as would be found in a freestanding dedicated Remote Access Server (RAS) server. If this feature exists on the KVM switch it will be disabled and the connectors that support this feature will be blocked with a tamper resistant seal.

- *(KVM02.010.00: CAT I) The IAO will ensure, if the KVM switch supports separate userids and passwords for each user, that the KVM switch is configured to require the user to login to the KVM switch to access the ISs attached. PKI authentication is acceptable and preferred to password authentication.*

- *(KVM02.011.00: CAT I) The IAO will ensure, if the KVM switch supports the enforcement of DOD compliant passwords, that the KVM switch is configured to require DOD compliant passwords.*

- *(KVM02.014.00: CAT II) The IAO will ensure the KVM switch is configured to force the change of the configuration password every 90 days or that there is a policy and procedure in place to change the configuration password every 90 days.*

- *(KVM02.018.00: CAT I) The IAO will ensure that if the KVM switch as the ability to support a RAS connection, that this feature be disabled and the connectors on the KVM switch supporting this feature are blocked with a tamper resistant seal.*

3.2.4 Requirements for Spanning Classification Levels

KVM switches should not be able to directly transfer information from one IS to another. However information could inadvertently be transferred between IS by a user entering data on one IS while thinking that he is accessing another IS attached to the same KVM switch. Therefore, prior to an analog KVM switch being attached to any IS the DAA for that IS must acknowledge and approve the connection. These approvals will be maintained by the IAM.

The IAO will ensure that only approved switches are used. A list of approved switches can be found on one of the following lists.

a. The National Information Assurance Partnership (NIAP) National Information Assurance Certification and Accreditation Process (NIACAP) List
b. The Defense Intelligence Agency (DIA) Standard Products List

c. NSA NES Approved Products List as approved by the DISN DAAs
(The SIPRNet Connection Approval Office (SCAO) will maintain a DISN Approved Products List.)

Cascaded KVM switches can easily lead to a user accessing a different IS than intended because of the multiple switch positions needed to be set to correctly access a specific IS. Therefore, KVM switches will not be cascaded either with another KVM switch or any other switch. The KVM switch will have tamper resistant seals to verify that it has not been opened, rewired, or modified. All unused connectors for ISs will be blocked with tamper resistant seals. All cable connections will be marked with tamper resistant seals that allow visual confirmation that the configuration of the cable has not been modified.

There is a new feature appearing on KVM switches where a peripheral device other than a keyboard, video monitor, or mouse can be switched along with the normal KVM devices from IS to IS. This is essentially A/B switch functionality. The first implementation of this feature was to switch speakers with the KVM devices but it has now been expanded to switch a USB port in at least one case. Since the use of A/B switches connecting peripherals to ISs of different classification levels is prohibited, KVM switches that are attached to ISs of different classification levels will have this feature disabled in the configuration if possible. Regardless of whether it can be disabled, no peripheral devices other than the keyboard, video, and mouse will be connected to the KVM switch users will be instructed not to attach any devices other than a keyboard, video monitor, or mouse to the KVM switch. Additionally, the connectors used for this feature will be blocked with tamper resistant seals.

- *(KVM02.020.00: CAT III) The IAM will maintain written permission from all DAAs responsible for all ISs that are connected to a KVM switch.*

- *(KVM02.021.00: CAT II) The IAO will ensure that only approved KVM or A/B switches are used.*

- *(KVM02.022.00: CAT III) The IAO or SA will ensure that no KVM switches are cascaded.*

- *(KVM02.023.00: CAT II) The IAO or SA will ensure that tamper resistant seals are attached to the KVM switch and all IS cables at their attachment points.*

- *(KVM02.024.00: CAT I) The IAO or SA will ensure, if the KVM switch has the ability to switch peripheral devices other than the keyboard, video, and mouse, that this feature is disabled.*

- *(KVM02.025.00: CAT I) The IAO, the SA and the user will ensure that no peripheral other than the keyboard, video, or mouse is connected to the KVM.*

- *(KVM02.026.00: CAT II) The IAO or SA will ensure that the connectors for additional peripherals are blocked with tamper resistant seals.*

3.3 Multi User Network Attached KVM Switch

Multi user network attached KVM switches will be found in the same environments where one would find a multi user analog KVM switch. Because of their additional cost, they are generally only used if there is a requirement for remote administration of the ISs such as a "lights out" server environment where there would normally not be administrative personnel. In a laboratory environment consideration should be given the use of an "out-of-band" or private network to segregate the traffic from the functional traffic for both security and performance reasons. However, if this network attached KVM switch is used to administer ISs the switches will be attached to an "out-of-band" network. Additionally, KVM switches will only be attached to a network of the same classification level. Because of the network access these switches support some of the features that were optional on an analog KVM switch are required for a network attached KVM switch

- *(KVM03.001.00: CAT I) The IAO or SA will ensure a network attached KVM switch to administer ISs that connected to an "out-of-band" network of the same classification level as all systems attached to the KVM switch.*

- *(KVM03.002.00: CAT I) The IAO will ensure that network attached KVM switches will only be connected to a network that is at the same classification level.*

3.3.1 Administrative Requirements

The Administrative Requirements are the same as the requirements for the single user analog switches found in sections 3.1.1 or 3.2.1.

3.3.2 Physical Requirements

Although the KVM switch itself is considered an unclassified object, it must be protected in a manner suitable for the IS with the highest classification to which it is connected. For example, if the switch is connected to a sensitive but unclassified system and an unclassified system then it will be protected in the same manner as the sensitive but unclassified system. This also means that physical access to the KVM switch will be restricted to individuals that are allowed physical access to all ISs attached to the switch.

All KVM switches will be labeled as required by all government owned equipment. Additionally all switch positions, cables and connecters will be labeled with the identity and security classification of the IS that they are attached.

The network-facing component of a network attached KVM switch will be compliant with the Network Infrastructure STIG.

The following requirement must be used in addition to those requirements listed in section 3.1.2 and 3.2.2 of this STIG.

- *(KVM03.012.00: CAT I) The IAO or SA will ensure that the network-facing component of a Network Attached KVM switch is compliant with the current Network STIG.*

3.3.3 Configuration Requirements

Network attached KVM switches will have an identification and authentication component that will meet all DOD requirements for password authentication or PKI authentication. In accordance with *DODI 8500.2*, group or shared authentication will not be allowed.

The KVM switch will restrict the IS access by user. An example, of this type of restriction would be user A is allowed access to systems 1 and 2 but not 3, user B is allowed access to system 3 but not 1 and 2, and user C is allowed access to all systems.

During the identification and authentication process (login) an Electronic Notice and Consent Banner compliant with the requirements found in CJCSM 6500.01 Enclosure C Appendix C will be displayed. In summary, the banner must contain the following 5 requirements. It will be displayed prior to the login solicitation and if possible will be displayed after a successful log-on and will remain displayed on the user's screen until a keystroke is entered. This serves as an auditable event that the banner was read.

a. The system is a DOD system.
b. The system is subject to monitoring.
c. 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.
d. Use of the system constitutes consent to monitoring.
e. This system is for authorized US government use only.

The KVM switch configuration will be locked from unauthorized modification. This lock will be either a DOD compliant password or PKI authentication. If modification of the configuration is a privilege that is granted to a user, the initial authentication of the user will be adequate.

Because all administrative traffic must be encrypted to protect it from interception, the KVM switch will be configured to require encryption for all communications via the network. NIST FIPS 140-1/2 validated cryptography will be used.

Some network attached KVM switches have the ability to encapsulate and forward USB protocol between the attached ISs and the client connected via the network. With this functionality the possibility exists to boot an IS, attached to the KVM switch IS, over the network from a USB attached device. Because of the extreme consequences that would arise from a compromised KVM switch, this feature will be disabled on the KVM switch and any IS attached to the KVM switch. If there is no need for a USB connection between an IS and the KVM switch, the USB ports will be blocked with tamper resistant seals.

NOTE: If the ISs is attached to the KVM switch to support a keyboard, video, or a mouse over USB, this connection could also support boot if the KVM switch and IS were configured to allow this functionality, even if it is disabled. Though it will be documented and approved by the IAM for all ISs attached to the KVM.

A more common feature of KVM switch is the ability to directly control the power supplied to the attached ISs. With this feature a client attached to a network attached KVM switch can interrupt the power to an IS effectively shutting it down. Because a compromised KVM switch could shut down all of the ISs using this feature without the need to access the operating systems of the attached ISs, this feature will not be used.

The IAO or SA responsible for the ISs the KVM switch is attached to will maintain a backup of the KVM configuration. This backup will include the userid/password file(s) that exist on the system. If the userid/password files are stored elsewhere on the network, the IAO or SA responsible for the ISs will ensure backup procedures exist for the remote userids/password file(s).

- *(KVM03.013.00: CAT I) The IAO will ensure that the KVM switch is configured to require the user to login to the KVM switch to access the ISs attached. PKI authentication is acceptable and preferred to password authentication.*

- *(KVM03.014.00: CAT I) The IAO will ensure that the KVM switch is configured to require DOD compliant passwords.*

- *(KVM03.016.00: CAT II) The IAO will ensure that group or shared userids are not used.*

- *(KVM03.017.00: CAT III) The IAO will ensure that the KVM switch be configured to restrict users access only to the systems they require.*

- *(KVM03.018.00: CAT III) The IAO or the SA will ensure that the Network attached KVM switch displays an Electronic Notice and Consent Banner complaint with requirements of CJSCM 6500.01.*

- *(KVM03:021.00: CAT I) The IAO or SA will ensure that the KVM switch is configured to only use encrypted communications using FIPS 140-1/2 validated cryptography.*

- *(KVM03.026.00: CAT I) The IAO or SA will ensure that the KVM switch will not be configured to encapsulate and send USB connections other than KVM connections.*

- *(KVM03.027.00: CAT II) The IAO will ensure that the USB ports on the KVM switch are blocked with tamper resistant seals if no USB connections are made to a KVM switch that can encapsulate and send the USB protocol over the network to the client.*

- *(KVM03.029.00: CAT II) The IAO will ensure that any feature that allows the KVM switch to directly control the power supplied to the ISs will not be configured or used and that any connectors on the KVM switch used to support this feature will be blocked with a tamper resistant seal.*

3.3.4 Requirements for Spanning Classification Levels

Because of the problems inherent in the spanning of networks of different classification levels, Network attached KVM switches will not be attached to ISs of different classification levels.

- *(KVM03.031.00: CAT I) The IAO will ensure the network attached KVM switches are not attached to ISs.*

3.4 A/B Switch

An A/B switch is a simple device that switches either a single peripheral device between two or more ISs or, switches multiple devices to a single I/O port on an IS. Whether the switch had two or more switch positions, it is always referred to as an A/B switch. In the past, A/B switches were an inexpensive solution to sharing devices among multiple users without having to power down the ISs and move the cables. The other use was to accommodate multiple devices that are occasionally used on a single system without incurring the expense of adding additional I/O ports. This technology is obsolete and better solutions exist. However, A/B switches are still being used.

A/B switches should only be used to connect multiple peripheral devices to a single system and then only if no other solution can be found. A/B switches should never be used to share peripheral devices between two or more ISs. If an A/B switch is used to share peripheral devices between two or more ISs, the IS, should be intended for a single users use, be within a single users work area, and be visible from all ISs it is attached to.

3.4.1 Administrative Requirements

To ensure that the users are aware of their responsibilities concerning the use of A/B switches, the IAO will maintain a written user agreement for all users authorized to use A/B switches. Additionally, the IAO will ensure that there is a section within the SFUG detailing the proper uses of A/B switches. The proper use should include at a minimum.

1. A/B switches should be used only if there is no other solution.
2. A/B switches should be used only to connect multiple peripheral devices to a single IS.
3. A/B switches should never be used to connect a single peripheral to multiple ISs.
4. If an A/B switch is used to connect to share peripheral devices between two or more ISs, the ISs should be intended for the use of a single user within the users work area, and be visible from all ISs that it is attached.

- *(KVM04.001.00: CAT IV) The IAO will maintain written user agreements for all users authorized to use an A/B switch.*

- *(KVM04.002.00: CAT III) The IAO will maintain and distribute to the users a SFUG that describes the correct uses of the switch and the users responsibilities.*

3.4.2 Physical Requirements

Although the A/B switch itself is considered an unclassified object, it must be protected in a manner suitable for the IS with the highest classification to which it is connected. An example would be, if the switch is connected to a sensitive but unclassified system and an unclassified system, then it will be protected in the same manner as the sensitive but unclassified system. This also means that physical access to the A/B switch will be restricted to individuals that are allowed physical access to all ISs attached to the switch.

Because two people accessing the A/B switch at one time could created situations where a user unaware of the other users intervention may inadvertently write data to the wrong media within a device attached to a A/B switch or might inadvertently transfer data to the wrong IS (as with a scanner) A/B switches will not be used to share devices between two or more users.

All A/B switches will be labeled as required for government owned equipment. Additionally, all switch positions, cables and connecters will be labeled with the identity and security classification of the IS that they are attached.

- *(KVM04.003.00: CAT 1) The IAO or SA will ensure that the A/B switch is physically protected in accordance with the requirements of the highest classification for any IS connected to the A/B switch.*

- *(KVM04.004.00: CAT II) The IAO or SA will ensure that an A/B switch is not used to share a peripheral device between two or more users.*

- *(KVM04.005.00: CAT III) The IAO or SA will ensure that the A/B switch, cables, switch positions, and connectors are labeled in accordance with this STIG.*

3.4.3 Configuration Requirements

Being simple devices, A/B switches usually do not have any configuration requirements. There is a class of A/B switches used to share devices between multiple ISs without the need to manually switch the device. This class of switches often have some configuration settings to determine which IS has preference if simultaneous request are received for the device. Since this does not affect the security posture of the switch it is of no concern here.

3.4.4 Requirements for Spanning Classification Levels

The IAO will ensure that only approved switches are used. A list of approved switches can be found on one of the following lists.

b. The National Information Assurance Partnership (NIAP) National Information Assurance Certification and Accreditation Process (NIACAP) List
c. The Defense Intelligence Agency (DIA) Standard Products List
d. NSA NES Approved Products List as approved by the DISN DAAs (The SIPRNet Connection Approval Office (SCAO) will maintain a DISN Approved Products List.)

The A/B switch will have tamper resistant seals to verify that it has not been opened, rewired or modified. All unused connectors will be blocked with tamper resistant seals. All cable connections will be marked with tamper resistant seals that allow visual confirmation that the cable configuration has not been modified.

Cascaded A/B switches can easily lead to a user accessing a different IS than intended because of the multiple switch positions needed to be set to correctly access a specific IS. Therefore A/B switches will not be cascaded either with another A/B switch or any other switch.

If an A/B switch is connected to two ISs of different classifications, it will not be used to switch a peripheral device that has persistent memory. These devices include, but are not limited to; disk drives and drives for removable media. This could lead to information being compromised by movement between systems of different classification levels. Additionally, input and output devices including but not limited to scanners, printers, and plotters will not be attached to A/B switches that span classification levels.

- *(KVM04.006.00: CAT II) The IAO will ensure that only approved A/B switches are used.*

- *(KVM04.007.00: CAT II) The IAO or SA will ensure that tamper resistant seals are attached to the A/B switch and all IS cables at their attachment points.*

- *(KVM04.008.00: CAT III) The IAO or SA will ensure that A/B switches are not cascaded.*

- *(KVM04.009.00: CAT I) The IAO or SA will ensure that A/B switches are not used to switch a peripheral device that has persistent memory between two or more ISs of different classification levels.*

NOTE: Persistent memory devices include but are not limited to disk drives and devices for removable memory.

- *(KVM04.010.00: CAT I) The IAO will ensure input and output devices including but not limited to scanners, printers or plotters are not attached to A/B switches that span classification levels.*

This page is intentionally left blank.

4. UNIVERSAL SERIAL BUS (USB)

Because of the proliferation of devices that could be attached to a PC it became evident that the legacy serial and parallel interfaces were no longer suited to the task nor fast enough to support the needed data transfer rates. There existed some high-speed interfaces such as SCSI but they were complex to implement. USB is a standard developed to allow easy connection of peripheral devices to a PC without the requirement of complex cabling and a high level of knowledge about the configuration of the interface. The original implementation of USB, level 1.0, was recently superseded by the newest release 2.0. Release 2.0 allows for additional transmission speed, while maintaining backwards compatibility for USB 1.0 devices and systems. Although this section deals specifically with the USB standard, the general principles and policies described here can be applied to any electrically hot swappable dynamically configurable device such as IEEE 1394 (FireWire) or PCMCIA (CardBus) cards. USB allows dynamic software configuration of devices as they are connected without having to restart the operating system.

For the purpose of this STIG, USB devices can be divided into two categories. These categories are differentiated by the memory they contain. There are devices that contain only volatile memory, or no memory at all, and there are devices that contain non-volatile or persistent memory.

Devices that contain volatile memory use the memory for temporary storage such as page buffers in printers, image buffers in scanners, or cache buffers in removable storage devices like Zip drives. Special notice should be made for USB hubs as they contain memory buffers even though it is not obvious. When the power is removed from these devices by unplugging them from the USB port and unplugging them from a separate power supply if one is needed, their memory is erased. Because these devices are designed to withstand minor fluctuations in power they contain some means of maintaining memory for short power interruptions. Users need to ensure that USB devices remain without power for at least 60 seconds when disconnecting them from one IS and connecting to a different IS to make sure enough time passes for all power to dissipate and the memory erased.

Devices with non-volatile memory will maintain the data written to them for an extended time without external power being supplied to the device. With some devices such as hard disk drives and flash memory, the data will be maintained for the life of the device unless actions are taken to erase them. These devices include hard disk drives, flash memory (jump) drives, some MP3 players, battery backed RAM cards, and PDA’s. Additionally, devices such as some digital cameras also contain non-volatile memory. Non-volatile memory devices do not include devices that have removable media like flash card readers, Zip drives, CD writers and DVD writers (all flavors). With these devices it is the media that is of concern not the device. If there is any question about whether a device contains non-volatile memory it should be treated as if it does until proven otherwise.

- *(USB00.0001.00: CAT III) The IAO will ensure that the SFUG requires that all USB devices are be powered off for at least 60 seconds prior to being connected to an IS.*

4.1 Administrative Requirements

In general, this STIG applies to USB devices that contain persistent memory. Camcorders, MP3 devices, and digital cameras are commonly used by private individuals for personal use and represent a risk of being overlooked as storage media, infecting an IS with malicious code, or being used to remove restricted or sensitive material from a location. These devices have limited business purposes and must be approved by the DAA before being connected to a DOD IS.

USB jump drives, small devices that contain flash memory, are considered media and are allowed. However, jump drives that are designed to look like anything other than a jump drive will not be attached to an IS. Additionally, since they could easily be overlooked in a spot search to verify that no restricted or sensitive information is being removed from a location, disguised USB jump drives will be banned from locations containing DOD ISs. There will be a prominently displaced notice describing this ban at all facility entrances and these devices will be confiscated if found.

All devices containing non-volatile memory are to be considered removable media. They will be secured in a manner appropriate for the classification level of the data they contain. They will also be labeled in accordance with the classification level of the data they contain.

DODI 8500.2, requires all sensitive but unclassified data be encrypted using FIPS 40-1/2 validated cryptography while electronically stored unless, the storage of this information in unencrypted form is approved in writing by the data owner. This applies to data stored on USB devices with non-volatile memory. Since these devices are often used to transport data this will protect the data from unauthorized access and disclosure if the device is misplaced or stolen besides protecting the data from unauthorized access while attached to an IS.

The SFUG will include guidance on USB devices maintained by the IAO. All users will be made aware of their responsibilities when using these devices and the proper labeling and storage of USB devices with non-volatile memory.

- *(USB01.0001.00: CAT II) The IAO, SA, and user will ensure that MP3 players, camcorders, or digital cameras are not to be attached to ISs without prior DAA approval.*

- *(USB01.0002.00: CAT II) The IAO, SA, and user will ensure that small flash memory devices that attach directly to a USB port that appear to be something other than a jump drive to the casual observer is not attached to ISs and is not permitted in locations containing DOD ISs.*

- *(USB01.0003.00: CAT II) The IAO will ensure that prominently displayed notices informing everyone of the ban of disguised jump drives are present at all entrances of locations containing DOD ISs.*

- *(USB01.0004.00: CAT II) The IAO, SA, and user will ensure that persistent memory USB devices are treated as removable media and secured in a manner appropriate for the classification level of the data they contain.*

- *(USB01.0005.00: CAT II) The IAO, SA, and user will ensure that the labeling of persistent memory USB devices is in accordance with the classification level of the data they contain.*

- *(USB01.0006.00: CAT II) The IAO, SA, and user will ensure that all sensitive but unclassified data stored on a USB device with persistent memory is encrypted.*

NOTE: This item may be in conflict with the Windows and Unix STIGs.

- *(USB01.007.00: CAT II) The IAO, SA, and user will ensure that USB devices with persistent memory are formatted in a manner to allow the application of Access Controls to files or data stored on the device.*

- *(USB01.0008.00: CAT III) The IAO will ensure that there is a section within the SFUG describing the correct usage and handling of USB technologies.*

- *(USB01.0009.00: CAT III) The IAO will ensure that the USB usage section of the SFUG contains a discussion of the devices that contain persistent non-removable memory.*

4.2 Configuration Requirements

Most USB devices do not have any configuration settings let alone any dealing with security. However, there now exist motherboards with system BIOS settings that allow an IS to be booted from a USB device. Other than during system maintenance, the system BIOS will not be set to allow the system to boot from a USB device. If the BIOS is set to allow this, the data stored on the systems disks and data found on any network attached to the system could be compromised by the booting of a foreign operating system from a USB attached device.

- *(USB02.0001.00: CAT I) The IAO or SA will ensure that no IS has its BIOS set to allow a boot from any USB device.*

5. MULTI FUNCTION DEVICES (MFD) AND NETWORK PRINTERS

5.1 Introduction

The purpose of this section is to discuss and provide guidance for the secure implementation of network attached MFDs and printers. MFDs are gaining popularity in the enterprise because they allow users to print, copy, fax and scan from a single device. The advantages of this are realized in the cost savings, space savings and maintenance compared to the individual devices they replace. Many MFDs offer the user the ability to fax directly from the desktop. Like network attached printers, MFDs are subject to the same network and physical security concerns. Because these devices include an embedded operating system and firmware, network connectivity, and a number of services and protocols, considerable attention is being paid to their secure implementation. As with printers, MFDs may have FTP, telnet, HTTP, HTTPS, SMTP and SNMP services running. MFDs may also have a connection to a phone line for fax functionality. If an attacker gains network access to one of these devices, a wide range of exploits may be possible. If an attacker gains physical access to a device, the programming of the device can be compromised and the potentially sensitive data stored on the hard disk can be recovered.

There are many vendors that manufacture network MFD and printer devices. The intent is not to specify a particular brand or vendor but provide, from a security perspective, things to look for. The following features are required:

1. Ensure the devices firmware is upgradeable by flash.
2. Verify all unneeded services; protocols and features can be disabled.
3. Ensure the device is IP addressable.
4. Ensure the IS can restrict access to the device by IP.
5. Ensure all management services will have the ability to change the default passwords and community strings.
6. Ensure there is a way to physically lock the device to prevent physical tampering including changing the configuration and accessing the hard disk by non-print administrators
7. Verify there are no known security vulnerabilities that cannot be addressed by a flash upgrade.
8. If the device incorporates a hard disk, verify there a method to erase the data once a print\fax\copy\scan job is complete (overwrite hard disk, erase memory, etc).

5.2 Network Protocols

Most MFDs are capable of operating using a number of different network protocols such as IPX/SPX, AppleTalk, DLC/LLC, NetBios/NetBEUI, NetBIOS/IP and TCP/IP. Devices configured to use protocols that are mission required result in reduced security exposure. For Windows, Unix, Linux and Mainframe based systems, TCP/IP is the required protocol. All MFDs and printers need to be assigned a static IP. In addition, all unused protocols need to be disabled.

- *(MFD01.001: CAT II) The SA will ensure the only network protocol used is TCP/IP all others are disabled.*

- *(MFD01.002: CAT II) The SA will ensure all MFDs and Printers are assigned a static IP.*

5.3 Management Services

As the name implies, management services are the services used by the device to allow administrative access to configure and monitor the device. FTP, telnet, HTTP, HTTPS, SMTP, BOOTP, DHCP and SNMP are the most common services. Like their server counterparts, there is a potential for unauthorized access or compromise through these services.

In most cases, FTP and telnet are not needed except for the occasional firmware upgrade. HTTP and HTTPS are used to remotely manage the device through an embedded web server. DHCP are disabled because the device will have a dedicated IP. SMTP is used to inform system administrators of critical errors (low toner, paper jams, low paper). SNMP is used for network monitoring. HTTPS is used instead of HTTP and SNMPv3 is preferred over earlier versions.

The default passwords or community strings on theses services are replaced with a complex password and all unneeded services are disabled. Unless using HTTPS or SNMPv3, services needed for firmware upgrades or device configuration are enabled only when they are needed and disabled all other times. All other management services (DHCP, SMTP, BOOTP, etc) are disabled all other times.

It is recommended that all MFDs and printers be placed on a dedicated network segment or VLAN with a discretionary access list to limit access to IPs of the print spoolers and SAs. With this configuration, users will not be able to directly access the devices but rely on print spoolers and the additional security they provide. If a device does not allow compliance because of an inability to disable services, set passwords, update firmware or passwords and configuration are lost after shutdown (older printers) the vulnerability can be mitigated by at least one of the following:

1. Replace the print server with a new internal or external print server that can be flash upgraded as needed.
2. Place the device behind a switch, router or firewall allowing a discretionary access list to block all traffic to the device except the traffic coming from the print spooler and SAs IP.

- *(MFD02.001: CAT I) The SA will ensure the default passwords and SNMP community strings of all management services are replaced with complex passwords.*

- *(MFD02.002: CAT I) The SA will ensure the MFD maintains its configuration state (passwords, service settings etc) after a power down or reboot.*

- *(MFD02.003: CAT II) The SA will ensure except for HTTPS and SNMPv3, that all management protocols are enabled only when necessary to upgrade firmware or configure the device and disabled all other times. In addition, all other management services such as DHCP, SMTP, and BOOTP are disabled at all times.*

- *(MFD02.004: CAT II) The SA will ensure devices are flash upgradeable and are configured to use the most current firmware available.*

5.4 Print Services

Most modern MFDs and printers are capable of employing a number of print services to include: Port 9100, LPD, IPP and FTP. In most cases, only Port 9100 or LPD are all that are necessary. For Windows based systems using a print spooler, choose Port 9100. Unix, Linux and Mainframe systems employ LPD (port 515).

- *(MFD03.001: CAT III) The SA will ensure print services are restricted to LPD or port 9100.*

NOTE: Only environments where both Windows and non-windows clients need services from the same device can both Port 9100 and LPD be enabled at the same time.

5.4.1 Print Spoolers

Print spoolers, in a Windows environment, most commonly involve using a print spooler; a Windows server to connect to the device and manage the access of clients and their print jobs. The advantages are access control and print prioritization based on Windows groups. When possible, devices are restricted to only a Windows print spooler or Unix\Linux\Mainframe print spooler. By segmenting this way, the device can be restricted to a single print service, port 9100 or LPD. A further advantage, router, firewall or switch ACL's can be employed to limit traffic to the device from only the print spooler and a few SA IPs for management.

- *(MFD04.001: CAT II) The SA will ensure MFDs and printers are configured to receive jobs from only print spoolers, not directly from users.*

NOTE: The configuration is accomplished by restricting access, by IP, to those of the print spooler and SAs. IP restriction is accomplished on the device (if supported) or placing the device behind a firewall, switch or router with an appropriate discretionary access control list.

- *(MFD05.001: CAT II) The SA will ensure print spoolers are configured to only allow authorized users access to MFDs and printers and restrict users to managing their own individual jobs.*

5.4.2 Auditing

Auditing is an important step in the preservation of resources and security. In addition to monitoring of potential "hacking" attempts to the devices, auditing is used to enforce an acceptable use policy for the MFD or printer. To the extent possible, auditing on the device is fully enabled. The servers, acting as print spoolers, will have their printer shares and MFD software configured with a defined access control list with auditing fully enabled. Auditing will include: all administration, configuration changes, user submitted jobs including: username, job type (fax, copy, print etc), and time.

- *(MFD06.001: CAT II) The SA will ensure devices and their spoolers have auditing fully enabled.*

- *(MFD06.002: CAT III) The IAO will ensure implement a MFD\printer security policy to include:*

    - *Acceptable use of device storage and retransmission of data.*
    - *Procedures for scrubbing or disposing of hard disks when devices are sent out for repair or disposal.*
    - *Defined protocols for acceptable key operator codes, administration passwords, user codes, who can change them, how often, format and storage of codes, and passwords.*

- *(MFD06.006: CAT III) The IAO will define a level of auditing to perform to include who reviews the audit logs.*

NOTE: Auditing will include user, key operator and admin codes and passwords, enabled features and services. Any deviation from baseline should be treated as a potential security incident. Ensure operational security controls are in place to ensure servicing of devices by authorized personnel is in accordance with change and configuration protocols.

5.5 Copy/Scan/Fax services

- *(MFD07.001: CAT I) The IAO will ensure MFDs with copy, scan, or fax capability are not allowed on classified networks unless approved by the DAA.*

- *(MFD07.002: CAT II) The SA will ensure the device is configured to clear the hard disk between jobs if scan to hard disk functionality is used.*

- *(MFD07.003: CAT III) The SA will ensure, file shares have the appropriate discretionary access control list in place if scan to a file share is enabled.*

- *(MFD07.004: CAT III) The SA will ensure auditing of user access and fax log is enabled if fax from the network is enabled.*

- *(MFD07.005: CAT II) The SA will ensure devices do not allow scan to SMTP.*

5.6 Physical Security

MFDs and printers share many of the same security concerns as network servers. Servers can and should be located and locked in a secure area away from the general work area; MFDs and printers do not have this same luxury. Every effort should be made to protect these devices from physical tampering. If the device has a hard disk, the device will have a mechanism to lock and prevent access to the hard disk. Where possible, only minimum console functionality is enabled. For repairs to the device by a vender, the controls may be relaxed then put in place after repair. When possible, devices with hard disks, are configured to erase the files stored on the disk after each print, scan, copy or fax job. This measure will minimize the loss of confidential data recovered in the event the hard disk is stolen or the device is otherwise compromised.

- *(MFD08.001: CAT II) The IAO will ensure the device has a mechanism to lock and prevent access to the hard disk.*

- *(MFD08.002: CAT I) The SA will ensure devices are configured to prevent non-printer administrators from altering the global configuration of the device.*

APPENDIX A. RELATED PUBLICATIONS

Department of Defense (DOD) Directive 8500.1, "Information Assurance (IA)" October 24, 2002

Department of Defense (DOD) Instruction 8500.2, "Information Assurance (IA) Implementation" February 6, 2003

Chairman Of The Joint Chiefs Of Staff Manual (CJCSM) 6510.01, "Defense-In-Depth: Information Assurance (IA) And Computer Network Defense (CND)" 25 March 2003

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) 140-2, "Security Requirements For Cryptographic Modules" May 25, 2001 as modified December 3, 2002. This publication may be found on the NIST website http://www.nist.gov.

USB

Universal Serial Bus Specification, Revision 2.0, April 27, 2000. This specification may be found on the web site http://www.usb.org.

APPENDIX B. LIST OF ACRONYMS

Acronym	Plain Text
ACL	Access Control List
CCB	Configuration Control Board
CJCSM	Chairman Of The Joint Chiefs Of Staff Manual
COOP	Continuity of Operations Plan
COTS	Commercial Off-The Shelf
DAA	Designated Approving Authority
DOD	Department of Defense
FIPS	Federal Information Processing Standards Publication
GB	Giga Byte (1,000,000,000 bytes)
HBA	Host Bus Adapter
HTTP	Hyper Text Transfer Protocol
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IEEE	Institute of Electrical and Electronics Engineers, Inc
IS	Information System
KVM	Keyboard, Video, and Mouse
LUN	Logical Unit Number
MB	Mega Byte (1,000,000 bytes)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSO	Network Security Officer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
SAN	Storage Area Network
SCSI	Small Computer Systems Interface
SDID	Short Descriptor Identifier
SMTP	Simple Mail Transfer Protocol
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guide
TASO	Terminal Area Security Offices
USB	Universal Serial Buss

APPENDIX C. DEFINITIONS

Term	Definition
CardBus	See PCMCIA
FireWire	See IEEE 1394
Hot key	A single key entry, a combination of keys simultaneously pressed or sequence of key entries on a computer keyboard that causes a specific action. Sometimes referred to as a shortcut or keyboard shortcut.
IEEE 1394	A dynamically configurable, electronically hot swappable standard for connecting peripheral devices, most notably camcorders, to a computer. Also known as FireWire and ILink.
ILink	See IEEE 1394
Jump Drive	A small flash memory device that connects directly to a USB port and appears to be a disk storage device to the operating system. The typically have storage capacities from 64MB to 2GB.
MP3	Audio compression format, usual found in the name of a audio playback device supporting this format.
PC-Card	See PCMCIA
PCMCIA	A dynamically configurable electronically hot swappable standard for connecting peripheral devices to a computer. Also known as PC-Card or CardBus.
Peripheral (device)	Any device that allows communication between a system and itself, but is not directly operated by the system.
Remote Access Server	A server that allows access to a network via a dialup phone connection connection.