Sharp Imaging and Information Company of America

IEEE-2600™ - 2008

HARDCOPY DEVICE AND SYSTEM SECURITY

Sharp Assures Full Compliance with IEEE-2600-2008 MFP Security Standard

December 2008

Executive Summary

This white paper describes how Sharp MFPs [1] comply, meet and exceed the IEEE-2600-2008 Security Standard Requirements

The Industry Leader in MFP Security

As the office equipment industry transitioned from analog to digital imaging, Sharp recognized the urgent need to address vulnerabilities inherent in network-connected multifunctional devices (MFPs). In doing so, Sharp led the industry with the first Common Criteria-validated security solution, and to this day remains the only manufacturer with an encryption and data overwrite product validated at the highest commercial level.

The Sharp Approach

Sharp takes a comprehensive approach to security by protecting every step in the document lifecycle, from the initial scan or print to final output and distribution. Fully scalable, Sharp's Security Suite enables Information Technology (IT) personnel to confidently safeguard their infrastructure and MFP installed base, without affecting network traffic or workgroup productivity. Specifically, Sharp MFPs (Segment 2 and up, including color) can be customized to meet unique requirements, help optimizing data confidentiality and integrity. For example, Sharp MFPs support:

- **User and device authentication**
- **Data encryption**
- **Memory clearing and sanitization**
- **Access control, user authorization and restrictions**
- **Architecture that virtually eliminates virus vulnerabilities and provides resistance to denial of service (DoS) attacks**
- **Activity monitoring (compliance auditing)**
- **Port management and filtering**

IEEE-2600-2008 Background

The IEEE-2600-2800 defines security requirements (all aspects of security including, but not limited to, authentication, authorization, privacy, integrity, device management, physical security, and information security) for manufacturers, users, and others on the selection, installation, configuration, and usage of hardcopy devices (HCDs) and systems, including printers, copiers, and multifunction devices (MFDs), and the computer systems that support these devices.

This standard identifies security exposures for these HCDs and systems, instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems, and instructs users on appropriate ways to use these security capabilities.

The standard is intended to apply to many different kinds of organizations, but it defines four generalized classes of operational Environments. (A, B, C, D) –see the next table [2] for security requirements examples.

	Effect on security requirements			
Operational Environment	**A**	**B**	**C**	**D**
Element of security				
Value of asset	High	Moderate	Moderate–Low	Low
Physical security	High	Moderate	Low	Low
Network protection	High	Moderate	Moderate	Low
Laws and regulations (see Note)	High	Moderate–Low	Low	Low
Personnel trust	High	Moderate	Low	Low
NOTE—Laws and regulations include privacy and governance laws, industry-specific standards, etc.				

The standard was developed by the P2600 Hardcopy Device and System Security Working Group which is an approved standards project sponsored by the IEEE Information Assurance Standards Committee of the IEEE Computer Society. Sharp and other vendors participated in the P2600 working group and developed this standard.

For more information, please visit http://standards.ieee.org/

(1) MX-2600/3100 series, MX-C311/C401 series [3], MX-4100/4101/5001 series [3] and MX-M363N/M453/M503 series [3]
(2) From IEEE Std.2600-2008 Copyright 2008, by IEEE. All rights reserved.
(3) Q1/Q2-2009

The following identifies how Sharp MFPs (Hard Copy Device- *HCD*[4]) meet or exceed each of the IEEE-2600-2008 Security Objective (Requirements) in reference to all of the standard's identified operational environments (A, B, C, D)

1.1 Protecting HCD software from unauthorized modification (IEEE-2600-2008 section 8.1.1.1 [5])

- *HCD Requirement:*
  - The HCD shall provide procedures to verify that the currently installed software in the HCD is consistent with the authorized, installed HCD software.
- *Sharp Mitigations:*
  - The Sharp MFPs with the Optional Data Security Kit (DSK) automatically perform a set of operations (System Check) when the HCD boots up to assure safe MFP functions including the validity of the installed firmware and the proper encryption operation.

1.2 User Identification and Authentication (IEEE-2600-2008 section 8.1.1.2[5])

- *HCD Requirement:*
  - The HCD shall identify and authenticate each user who tries to access HCD assets or execute HCD applications
- *Sharp Mitigations:*
  - Sharp takes a comprehensive approach to securing valuable MFP assets by providing device access control to help avoid the risk that resources are misused or abused:
    - **User authentication**: Authentication to the LDAP server, Active Directory, or other authentication servers, identifies the sender and helps ensure that only authorized users (With a valid username/password or access cards such as Proximity card or Common Access Card (CAC)) can access setup, maintenance and/or MFP functions.
    - **Account codes:** Account Codes are a standard feature on all Sharp MFPs that track device usage from the control panel. The user must enter either a valid 5-digit code or user credentials, including a strong password. Each department can have their own code. A report can be generated that includes usage by Account Code.
    - **Password protection:** Using up to 32 alphanumeric characters, including special symbols (e.g., #&*<>), Sharp's strong password protection makes the MFP highly secure. In addition, to add another layer of protection, anyone that enters three invalid admin passwords or document filing passwords can be locked out.

1.3 User Authorization (IEEE-2600-2008 section 8.1.1.3[5])

- *HCD Requirement:*
  - The HCD shall ensure that users are authorized prior to permitting access to HCD assets and performance of HCD functions.
  - The HCD shall also ensure that Unauthorized Users are not permitted to access HCD assets or execute HCD applications including installation or update of firmware, software, and "applet."
- *Sharp Mitigations:*
  - Sharp MFPs provide the ability for the administrator to define and set rules (User/Group profiles) governing permissions given to user or user groups, such as for access to print, scan, fax, or copy functions, access to color printing, or limits on the number of pages that can be processed.
    - User and Group Profiles protect the Sharp MFP from unapproved usage, update and/or possible tampering by specifying functions that can be accessed. For instance, one user and/or group can be limited to copy and fax functions, locking out scan to e-mail and printing. Or to control supply costs, a profile can restrict access to color copying and/or printing.
    - Sharp MFPs have specific credentials only for administrator to do updates.

(4) HCD –Hard Copy Device and MFP used interchangeably with Multi Function Printer/Device

1.4 Offline salvage of deleted or stored User Document Data (IEEE-2600-2008 section 8.1.1.4[(5)])

- *HCD Requirement:*
  - The HCD shall ensure that User Documents that have been logically deleted or released after use cannot be recovered from nonvolatile storage devices that have been removed from the HCD.
- *Sharp Mitigations:*
  - The optional Sharp Data Security Kit automatically overwrites deleted data on the MFP's hard disk using an effective wiping technique, whether immediately after each job or as an automatically scheduled task.

1.5 Protecting User Document Data, User Function Data, HCD Confidential Data, Protected Data, and Software in the HCD

1.5.1 From Disclosure (IEEE-2600-2008 section 8.1.1.5.1[(5)])

- *HCD Requirement:*
  - The HCD shall protect User Document Data and HCD Confidential Data from unauthorized disclosure when such data is in the HCD.
- *Sharp Mitigations:*
  - Sharp's Common Criteria validated Data Security Kit offers multiple layers of security. First, all latent image data within the MFP is encrypted (using an AES algorithm) before being written to the hard drive, RAM or Flash memory. When a document is printed, copied, scanned or faxed, the temporary data stored/buffered in memory is overwritten up to seven (7) times, rendering it unrecoverable. Sharp competitors typically overwrite just three (3) times. It is the combination of encryption and overwrites that sets Sharp apart.
  - Confidential Print and Confidential Fax are standard Sharp features that help prevent users from accessing sensitive documents without appropriate identification (valid job ID, password, or PIN code). The user enters an 8-digit (MX series) or 5-digit (AR series) pin from the control panel before the print/fax file is released. Standard firmware (MX color) also supports encrypted PDF files. Installation of the Sharp DSK encrypts all stored files.
  - Sharp MFPs provide support for strong authentication mechanisms for user or administrator password access (up to 32 alphanumeric characters).
  - Sharp MFPs provide configurable access control mechanisms for user access and administrator access to data stored on the HCD.
  - Sharp MFPs (MX color with DSK option) will embed a nearly invisible watermark within a first-generation copy made on the MFP. If someone attempts to duplicate that hardcopy on a Sharp MFP equipped with the DSK, the MFP will terminate the copy operation and display a warning message.

1.5.2 From Modification (IEEE-2600-2008 section 8.1.1.5.2[(5)])

- *HCD Requirement:*
  - The HCD shall protect User Document Data, User Function Data, HCD Confidential Data, Protected Data, and Software from unauthorized modification when such data is in the HCD.
- *Sharp Mitigations*
  - Sharp MFPs provide configurable access control mechanisms for user access and administrator access to data stored on the HCD
  - Sharp takes a comprehensive approach to securing valuable MFP assets by providing monitoring tools to help avoid the risk of resources being misused or abused.
  - Access Control types:
    - **User authentication**: Authentication to the LDAP server or to Active Directory (or other authentication servers) identifies the sender and ensures that only authorized users (with a valid username/password or access cards such as Proximity card or Common Access Card (CAC)) can access MFP functions.
    - **Account codes**
    - **User/group profiles**
    - **Password protection**

1.6 Protecting User Document Data, User Function Data, HCD Confidential Data, Protected Data, and Software in Transit

1.6.1 From Disclosure (IEEE-2600-2008 section 8.1.1.6.1[(5)])

- *HCD Requirement:*
  - The HCD shall protect User Document Data and HCD Confidential Data from unauthorized disclosure when such data is in transit to or from the HCD over a shared communications medium.
- *Sharp Mitigations*
  - Sharp MFPs encrypt network traffic using SSL, SMB and/or SNMPv3 protocols, thus blocking any attackers trying to sniff the network traffic of companies that have implemented network encryption.

1.6.2 From Modification (IEEE-2600-2008 section 8.1.1.6.2[(5)])

- *HCD Requirement:*
  - The HCD shall protect User Document Data, User Function Data, Confidential Data, Protected Data, and Software from unauthorized modification when such data is in transit to or from the HCD over a shared communications medium.
- *Sharp Mitigations:*
  - Sharp MFPs encrypt network traffic using SSL, IPSEC, SMB and/or SNMPv3 protocols, thus blocking any attackers from sniffing the network traffic of companies that have implemented network encryption.
  - Sharp MFPs offer secure device authentication protocols (for details see section 1.9 below) that assist in preventing an attacker ("man in the middle") from tapping into data/document files, changing the content, and then redirecting the file – all while appearing to come from an "authorized" device.
  - Sharp MFP (MX color series) users can send encrypted PDF files (scan and print) over the network. Only those recipients with the correct pass code can open the file. PDF encryption is important for healthcare companies, financial firms, education institutions and many other that must comply with stringent federal, state or local privacy mandates.

1.7 Administrator Identification, Authentication, and Authorization (IEEE-2600-2008 section 8.1.1.7[(5)])

- *HCD Requirement:*
  - The HCD shall identify and authenticate each HCD administrator, and shall ensure that administrators are authorized prior to permitting access to HCD data assets and performance of administration functions on the HCD.
- *Sharp Mitigations:*
  - Sharp MFPs provide support for strong authentication mechanisms (up to 32 alphanumeric characters) for administrator access.
  - Sharp MFPs with the optional DSK can be configured to block admin access after three attempts.

1.8 Monitoring of HCD Events (IEEE-2600-2008 section 8.1.1.8[(5)])

- *HCD Requirement:*
  - The HCD shall create and maintain a log of HCD use and security-relevant events.
- *Sharp Mitigations:*
  - Sharp MFPs provide the capability to create and securely maintain a log of user and e-mail activities
  - Sharp MFPs (MX color series) activity can be logged (Who, When, To, From, What [file name]) to create an audit trail/log file, ensuring compliance with privacy regulations set forth by the federal government.
  - The log file can be viewed by administrator to detect any unauthorized activities that might pose a security risk.

1.9 HCD cannot be used as a proxy for malicious attacks (IEEE-2600-2008 section 8.1.1.9[5])

- *HCD Requirement:*
  - The HCD shall ensure that its shared communication media interfaces cannot be used as a proxy for or a source of malicious attacks on the external IT environment.
- *Sharp Mitigations:*
  - Sharp's Network Interface supports four key security features:
    - **IP address filtering**: Limits access to select IP addresses.
    - **MAC address filtering**: Limits access to specific computers, regardless of IP address.
    - **Protocol management**: Specific communication protocols can be disabled (e.g., TCP/IP, NetBEUI, NetWare, Ether Talk).
    - **Port management**: Specific communication ports address can be changed individually as well as disabled (e.g., SMTP, LDAP, HTTP, FTP, LPD, IPP, Telnet, JCP, RARP, IPV6, IPSEC, POP3 and others).
  - Sharp MFPs provide the ability to disable individual protocols and ports on the device.
  - Sharp MFPs provide address or destination filters to block or permit connections from known or unknown hosts (e.g., white list, black list of IP, MAC, phone, etc.)
  - Sharp MFPs use unique embedded firmware that is not based on the Windows®/Linux® operating system. Therefore, the Sharp MFP's internal systems are not subject to the same virus vulnerability as Microsoft and Linux operating systems. Sharp's unique architecture provides no user interface and cannot execute downloaded files or commands sent by an attacker to compromise the system.
    - This has the added benefits that while other MFP manufactures struggle to provide security patches to protect their customers, Sharp customers are virtually immune to these threats, thus are freed from the onerous task of installing security patches.
  - Sharp offers secure device authentication that utilizes Kerberos, 802.1x, Digest-MD5 (for LDAP-v3) and/or SSL (Secure Socket Layer with Digital Certificate) protocols. Kerberos, Digest-MD5 and SSL are network authentication protocols that use private-/public-key cryptography to provide strong authentication for client (MFP)/server applications.

1.10 HCD cannot be used to bridge between fax interface and a shared communications media (IEEE- 2600-2008 section 8.1.1.10[5])

- *HCD Requirement:*
  - If a shared communication interface (e.g., network connection) is present on the HCD, the HCD shall not permit users to establish a malicious connection to the external IT environment via the fax interface and should not permit an unauthorized non-fax data connection to the HCD via the fax interface.
- *Sharp Mitigations:*
  - Sharp MFPs provide the capability to disable the fax function on the HCD.
  - Sharp's MFP architecture prevents network infiltration via a fax modem. This means common executable viruses, and other similar infectious software cannot be used to compromise MFP security or disrupt network operations.
  - Sharp's MFP architecture provides a logical separation between the fax telephone line and Local Area Network (LAN). It is, therefore, virtually impossible for attackers to gain access to the MFP's internal systems and the network. Important points to remember include the following:
    - The fax modem controller is separate from the MFP's LAN network controller.
    - The fax function is logically independent of the other MFP functions.
    - The fax modem is fax-only (Class I, not data/fax, thus responds only to fax transmission protocols, prohibiting all others - including data communications).
    - The fax modem controller has no mechanism to support any external code or executable file.
  - Sharp's DSK encrypts image data coming from the fax modem. After the received message is printed, the data is automatically erased. Without encryption, businesses run the risk those attackers can access sensitive documents residing in the internal memory.

1.11 Mitigation of Denial of Service (IEEE-2600-2008 section 8.1.1.11[(5)])

- *HCD Requirement:*
  - The HCD should protect assets during DoS attacks against the external HCD interfaces, and should restore normal operation without requiring human intervention upon termination of such attacks.
- *Sharp Mitigations:*
  - Sharp MFPs ensure that even when an attack of this type causes the MFP's network interface to fail, it does not interfere with the operation of those MFP subsystems that do not require network access.
  - Sharp MFPs ensure that the MFP's network interface can recover automatically and in a timely fashion after the end of the attack.
  - Sharp MFPs provide the capability to enable only protocols that require user authentication before jobs can be sent to the HCD, limiting the number of protocol exposed to potential DoS attack:
    - **IP address filtering**: Limits access to select IP addresses.
    - **MAC address filtering**: Limits access to specific computers, regardless of IP address.
    - **Protocol management**: Specific communication protocols can be disabled (e.g., TCP/IP, NetBEUI, NetWare, Ether Talk).
    - **Port management**: Specific communication ports address can be changed individually as well as disabled (e.g., IPV6, SSL, IPSEC, SMTP, LDAP, HTTP, FTP, LPD, IPP, Telnet, JCP, RARP, POP3 and others).

(5) From IEEE Std.2600-2008 Copyright 2008, by IEEE. All rights reserved.