SHARP® Sharp Imaging and Information Company of America

May 25, 2010

Dear Sharp MFP Customer,

The recent CBS evening news story focusing on Copier Security has shined a much-needed spotlight on the subject. At Sharp, we are gratified to have this attention turn to a subject we've championed for the better part of a decade. Although other manufacturers have followed Sharp's lead and now offer some copier security features, this leadership was on display as Sharp was the only copier vendor contacted by CBS to go on camera to discuss this issue. In fact, a portion of the story was filmed at our US Headquarters office in Mahwah, New Jersey and featured an appearance and comments by our company President, Ed McLaughlin.

For a decade now, Sharp has offered a broad array of standard and optional security features that are designed to help you protect your confidential and private information. To address the specific issue of image data on the hard drive, Sharp offers the Data Security Kit, which when equipped on the MFP provides additional security, including two key steps:

- The first step is that all data on the Hard Drive is stored at 256 bit encryption.
- Once the job is complete, the data is overwritten up to seven (7) times. This can be done after every job, when the machine is turned on or on demand. If used correctly, this process renders the data on the drive virtually unrecoverable.

If customers choose not to purchase a Sharp Data Security Kit, Sharp strongly recommends that at the end of the product life, you purchase a new Hard Drive for your MFP and retain and destroy the original Hard Drive that contains your confidential information. While many people have considered reformatting the Hard Drive as a measure to protect the information on the drive, we do not recommend this method as a secure alternative to protect the confidentiality of your information. In order to complete any of these actions, please contact your Sharp Authorized Service Provider.

While the CBS story highlights the issue of confidential and protected information remaining on the hard drive, the security concerns on a networked, digital copier run much deeper. The recently published IEEE Standard for Information Technology: Hardcopy Device and System Security Requirements (IEEE 2600™-2008) addresses multiple aspects of security including, but not limited to, authentication, authorization, privacy, integrity, device management, physical security, and information security. This new standard validates the Sharp position that true security requires much more than simple overwrite at the end of a lease.

We have included the attached Security At a Glance and a Security Q & A which addresses many of the questions you may have and provides a comprehensive overview of the security issue and what can be done to protect your organization.

Sincerely,

Mike Marusic
Vice President, Marketing & Service
Sharp Imaging and Information Company of America

Attachments:	Sharp Security At-A-Glance, Security Q&A

Sharp is a registered trademark of Sharp Corporation. All other trademarks are the property of their respective holders.

Sharp Security At a Glance

As a leader in office equipment security, Sharp makes it easy for virtually any business or government entity to safely deploy digital copying, printing, scanning and faxing. We have been awarded BERTL's "Most Secure MFP Range" Award – for six consecutive years, were the first in the industry to achieve Common Criteria (ISO 15408) certification, to date have achieved the industry's highest level of certification and we continue to maintain a full line of validated products.

Sharp offers products that meet the requirements of the recently published IEEE Standard for Information Technology: Hardcopy Device and System Security Requirements (IEEE 2600™-2008) which defines security requirements for manufacturers, users, and others on the selection, installation, configuration, and usage of hardcopy devices, including printers, copiers, and multifunction devices (MFDs).

This commitment to security is designed to help protect your data, and makes Sharp the optimum choice to protect confidential and protected information through our layered approach to security:

Access Control

Account management enables administrators to control access functions (Copy, Scan, Fax, and Print) and to monitor usage. Also provides support for Common Access Card (CAC) login.

Documents Remain Confidential

To help protect your printed documents from unauthorized viewing, Sharp MFPs offer confidential printing that requires users to enter a PIN code in order to print a queued document. Additionally, Secure Fax Release holds fax documents in memory until an authorized user enters a PIN code—making it easier to comply with health care regulations like HIPAA.

Network Scanning Access

To help protect your network from unauthorized e-mail communications, Sharp MFPs support user authentication. Requires users to login before performing any network scanning operations.

Control Device Access Over the Network

To help restrict access to the device over the network, Sharp MFPs support:

- Secure Socket Layer (SSL Encryption)
- IPv6 and IPsec
- IP/MAC address filtering
- Port/Protocol management for maximum security

Data Erase and Encryption

To help protect your data, an optional Data Security Kit is available that encrypts document data in compliance with Advanced Encryption Standards (AES -256 bit). Additionally, the Data Security Kit erases temporary hard drive memory by over-writing the data up to seven times, providing an unprecedented level of assurance.

Tracking and Auditing Information

Sharp offers both standard and optional features that allow our customers to control, access and track usage of each device on the network. These scalable security offerings aim to protect your intellectual property, preserve confidential information and help your business to meet regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm Leach Bliley Act (GLB).

For additional information visit: www.sharpusa.com/security