

April 26, 2010  
PRM-57-10

To: Canon Office Imaging and Office Products Dealers

Subject: Inquiries Concerning Multi-Function Device Security

---

As you may be aware, the CBS Evening News recently aired a news segment regarding potential information and security vulnerabilities of multi-function devices which utilize a hard disk drive. Since you may be receiving inquiries regarding information security on imageRUNNER and imagePRESS devices, we have included in this letter a description of three technologies which can support the securing of information on the hard disk drives used in these systems.

The Hard Disk Drive Format is a standard security feature on all imageRUNNER and imagePRESS systems. This function allows a user or system administrator to conduct a onetime overwrite of a device hard drive prior to returning that device at the end of the lease, redeploying the device to another location, or otherwise disposing of the device. This feature is designed to address customer concerns about data remaining readily accessible on the device hard drive at the end of the product lifecycle. In addition to the information available in the product manuals and other product materials, a Hard Drive Format Bulletin has also been developed to describe the details of this feature and how to initiate the capability.

Canon also offers optional Hard Drive Overwrite and Encryption Security Kits for imageRUNNER and imagePRESS devices, designed for those users and companies requiring enhanced security of document data stored on the Hard Disk Drives. The overwrite technology can overwrite the internal hard disk up to three times, while the encryption technology allows the data on the hard drive to be encrypted with either 256 bit AES encryption or 168 bit 3DES encryption, depending on the device model, rendering the data unreadable.

As a final consideration, if a customer has additional security concerns not satisfied by one of the technologies described above, a dealer may offer for purchase a Canon replacement hard drive in which case the customer can properly destroy the replaced hard drive.

To further assist you with communicating to customers Canon's comprehensive security suite of solutions, the following documents are available for download, including:  
*imageRUNNER ADVANCE "RUN" Security Solutions Brochure and  
imageRUNNER & imagePRESS Bulletin "Hard Drive Format Technology"*

This content is the latest material created by Canon, and along with our previous Security solutions content, can be accessed through [www.isgcentral.cusa.canon.com](http://www.isgcentral.cusa.canon.com). Please go to ISG Product Marketing >Browse Content > Security Solutions. They also can be located on the Canon USA "Let your Business RUN" micro site in the security section of [www.usa.canon.com/RUN/corporate](http://www.usa.canon.com/RUN/corporate).

The Canon USA Systems and Technical Support Division also recently posted a Technical Publication which addresses information and data security on Canon imageRUNNER ADVANCE devices. The technical publication number of this document is TP10 095.

As noted in the Technical Publication, Canon U.S.A., Inc. assumes no responsibility for customer decisions relating to erasing or overwriting data prior to returning the equipment to the dealer or any leasing company or otherwise disposing of the same. However, it is recommended that the dealer explain to the customer the availability of the various security functions and options described in this letter and other Canon materials in the course of the dealer's sales and maintenance activities.

We hope you will find this information helpful in addressing customer inquiries about Canon multi-function device security, and in assisting customers in responding to their various data security needs.

Sincerely,

Sam Yoshida  
Vice President and General Manager  
Marketing & Field Sales Division  
Imaging Systems Group  
Canon U.S.A. Inc.