



COTS SECURITY GUIDANCE (CSG)

SUMMARY OF *OVERVIEW OF MULTI-FUNCTION DEVICES SECURITY FEATURES*

CSG-11\S

August 2009



This page intentionally left blank.



Foreword

The Summary of *Secure use of Multi-Function Devices (CSG-111S)* is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at itsclientservices@cse-cst.gc.ca or call (613) 991-7654.

Effective Date

This publication takes effect on 08/28/2009.

*Carey Frey
Director, IT Security Industry Program*

© Government of Canada, Communications Security Establishment Canada 2009

It is not permissible to make copies or extracts from this publication without the written consent of CSEC.



This page intentionally left blank.



Table of Contents

Foreword	i
Effective Date	i
Table of Contents	iii
List of Abbreviations and Acronyms	v
Annex A -- Summary of Recommendations	1
Annex B -- Security Features Checklists for Devices	3
Annex C -- Summary of Security Issues	7



This page intentionally left blank.



List of Abbreviations and Acronyms

3DES	Data Encryption Standard applied three times (triple DES)
AES	Advanced Encryption Standard
CSG	Context for Secure Use project at CSEC
Fax	Facsimile
FBI	Federal Bureau of Investigation
FLASH	Non-volatile memory that can be electrically erased/reprogrammed
FTP	File transfer protocol
GC	Government of Canada
HDD	Hard Disk Drive
HR	Human Resources
HTTP	Hyper Text Transport Protocol
HTTPS	HTTP over Secure Socket Layer
I&A	Identification and Authentication
ID	Identifier
IP	Internet Protocol
IPP over SSL	Internet Printing Protocol over Security Socket Layer
IPPS	Internet Printing Protocol over Security Socket Layer
IPSEC	Internet Protocol Security
IT	Information technology
LPR	Line Printer Remote protocol
MAC	Media Access Control
MFD	Multi-function device
NIC	Network Interface Card
OCR	Optical Character Reader
PIN	Personal Identification Number
PC	Personal Computer
RAM	Random Access Memory



Secure use of Multi-Function Devices (CSG-111S)

SANS	System Administrator and Network Security
SMB	Server Message Block protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
Telnet	Telecommunication Network protocol
TWAIN	Standard for linking applications and image acquisition devices
UNIX	Bell Labs computer operating system
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply



Annex A -- Summary of Recommendations

The lists on this page summarize the key threat mitigation strategies and policies for a typical GC environment. The ranking reflects the associated risk and priority.

Mitigation

- Protect printers and MFDs as network devices
- Apply the latest software updates and security patches
- Restrict network traffic
- Change default passwords
- Protect the devices physically
- Require that anyone accessing the device be identified and authorized
- Establish thorough change management and auditing programs
- Disable all unnecessary features
- Make use of private printing
- Overwrite spooled files, images, and other temporary data
- Encrypt document images prior to temporarily storing them
- Log all activities extensively
- Prevent tampering with audit logs
- Apply least privileges to users
- Use SNMPv3 for centralized management
- Encrypt data communications
- Employ strong user I&A (e.g., two-factor)



Policy

- Require that there be no unauthorized access
- Require security certification before allowing devices on the network
- Require that IT technology include appropriate security features
- Include printed output in security policy dealing with the protection of sensitive information
- Prohibit unauthorized external access
- Require periodic security audits
- Include the devices in IT security program and contingency planning
- Make the IT department responsible for protection and maintenance
- Require authentication for all activities
- Define acceptable use policy and make users aware through training
- Require extensive logging of all activities
- Require anti-virus and software updating for all networked devices
- Define departmental policies for acceptable codes, PINs and password and their protection
- Enforce least privileges



Annex B -- Security Features Checklists for Devices

This section is an IT security technology functionality requirements checklist. Each function listed has its own sub-heading and contains functionality, features or settings that will create the most secure configuration possible without sacrificing performance.

User and Device Authentication

- ❑ Administrator (device) authentication
- ❑ Change default passwords/PIN codes
- ❑ User I&A
 - Local at device
 - Networked
- ❑ Strong authentication
 - Complex passwords
 - GRID cards
 - Smartcards
 - Security access cards (e.g., HID)
 - Biometrics

Data Encryption

- ❑ Encrypt communications (e.g., IPP over SSL, IPSec)
- ❑ Encrypt latent data, documents and images
- ❑ Handle encrypted/password protected PDF file
- ❑ Encryption algorithms
 - Advanced Encryption Standard (AES)



- Triple-Data Encryption Standard (3DES)

Memory Clearing and Sanitization

- Overwrite (RAM, FLASH, HDD)
 - Temporary data between jobs
 - Image data after completion of jobs
- Multiple overwrite with random 0s and 1s
 - 3 times
 - 7 times

Access Control, User Authorization and Restrictions

- Control user activities
 - Page count limits per job
 - Colour
 - Allowable times (e.g., normal working hours)
- Disable or control scan-to functionality
 - Uniquely identify user as sender in scan-to-e-mail
- Discretionary access controls
- Password protection
- Private or confidential printing
- Controlled physical access



Resistance to Attacks

- ❑ Common Criteria certified¹
- ❑ Isolation of fax from network
- ❑ Control panel lock
 - Require authenticated access
- ❑ Lockable internal hard drive
- ❑ SNMPv3
- ❑ Operating system
 - Proprietary
 - Widely supported
- ❑ Anti-virus protected
- ❑ Software updates and security patches
- ❑ Minimum applications and services

Compliance Auditing

- ❑ Logging
- ❑ Secure storage of logs
- ❑ Separate log backup
- ❑ Security checklists
- ❑ Accountability
- ❑ Security incident detection and response
- ❑ Automated configuration change detection tools

¹ See Glossary and URL <http://www.cse-cst.gc.ca/its-sti/services/cc/index-eng.html>.



Default “Deny” access

- ❑ Prevent public access
- ❑ Disable Windows sharing
- ❑ Limit trusted addresses
- ❑ Least privilege
- ❑ Firewall
- ❑ Block all but necessary protocols and ports
- ❑ IP and/or MAC address filtering

Installation & Operation

- ❑ UPS
- ❑ Maintenance/service schedule
- ❑ Asset tracking

Management

- ❑ Device management
 - Stand-alone
 - Centralized
- ❑ Configuration control
 - Production state
- ❑ Limited administrators
- ❑ No default fax output



Annex C -- Summary of Security Issues

Security Issue	Risk	Mitigation	Policy
Out of sight, out of mind	Printers and MFDs are networked computers vulnerable to compromise and use for malicious purposes.	Protect them as servers or workstations.	Include them in the organization's Configuration management, change management, IT security standards, and IT contingency planning.
Failure to identify organization's approach to security	Every hole and missed patch on IP-addressable network devices represents an exposure.	Understand the vendor's security strategy and ensure that the vendor will provide timely maintenance and security patches.	Select products that reflect the organization's strategy and risk tolerance.
Printer sharing	Shared printers reduce some control and can lead to abuse of resources.	Implement user I&A. Strive for single sign-on across the organization. Use strong authentication and support of private printing.	Require I&A for access to networked devices of any kind.
Device sharing	Replacing individual devices with a few shared MFDs may result in loss of productivity	Protect the devices with uninterruptible power supply (UPS) and establish appropriate maintenance	The IT department is responsible for the availability and maintenance of IT



Secure use of Multi-Function Devices (CSG-111S)

Security Issue	Risk	Mitigation	Policy
	due to device failures.	service regimes.	devices.
Unacceptable use of devices	Replacing individual devices with a few shared MFDs may result in excessive use for non-business related activities.	Establish and maintain the appropriate user activity authorizations or privileges.	Have an acceptable use policy that covers the use of all business assets.
Lack of standards	There are no widely accepted security standards for network printers and MFDs.	Establish audit standards and device security checklists.	Include printers and MFDs in periodic organizational security audits.
Lack of preparation for installation	There is excessive risk if the IT department neglects to configure carefully devices before making them accessible on the network.	Use an asset management system to identify and track devices. Protect new installations until the operating system is installed and hardened. Disable or remove unnecessary features, options, protocols or applications. Apply change management and configuration management. Test all continuity controls.	Require that intelligent devices meet departmental security configuration criteria before their connection to a network.
Poor physical	Shared printers and MFDs are located in easy-to-access,	Enforce network I&A and challenge visitors or strangers	Locate intelligent devices inside an appropriate security



Secure use of Multi-Function Devices (CSG-111S)

Security Issue	Risk	Mitigation	Policy
security	high traffic locations with weak access controls.	before they enter the vicinity of the device. Provide knowledgeable escorts for service technicians and use only certified service technicians. Purge or reset internal storage and configuration settings prior to any uncontrolled servicing.	zone to reduce unauthorized physical or network access. Protect any sensitive content or configuration before servicing.
Vendor supported diagnostics and management	Access by any external organization means extending trust to anyone in one of these organizations, or anyone they trust in their own extended network connections.	Deny external access except those necessary to business. Strictly control any authorized external access.	Prohibit unauthorized external access. Establish legal agreements explicitly identifying security obligations with any external organizations. Enforce a least privilege policy on external relationships.
Failure to enable device activity logging	Unsecured devices are prime targets to attackers.	Require certification of all IT devices before connection to any network. Log extensively and protect the logs.	Require extensive logging and security for these logs. Establish log retention policies and audit periodically.
Lack of protection from malicious	There is a danger of widespread compromise when all devices share the same	Ensure that all network devices have anti-virus scanning of their storage.	Require anti-virus protection for all networked devices. Require up-to-date software



Secure use of Multi-Function Devices (CSG-111S)

Security Issue	Risk	Mitigation	Policy
software	configuration.	Apply the latest tested and approved software updates and security patches. Use automated configuration change control tools to detect unauthorized manipulation of settings.	and patches be employed provided they prove reliable.
No device auditing	Inappropriate activities that go unnoticed can represent a serious, ongoing, security exposure.	Define the level of audit to perform, who is to perform audits and their frequency. Include review of logs as part of the audit. Invoke the incident response plan in cases where there is suspicion that a device has been compromised.	Establish accountability for IT security audits, their depth, scope and frequency. Establish policy for dealing with security incidents including investigations and sanctions.
Production configuration	Devices may lose their settings after a reboot or power failure.	Ensure that a process is in place to reconfigure the MFD/Printer back to its secure production state.	See Preparation for Installation.
Stale user accounts	Directories of user access accounts get stale over time. Malicious individuals can hijack inactive accounts and	Remove user access and disable their codes when a user no longer needs access;	User access and privilege policy should include removing access and disabling codes when a user



Secure use of Multi-Function Devices (CSG-111S)

Security Issue	Risk	Mitigation	Policy
	use these to carry out inappropriate activities anonymously.	periodically audit user access.	no longer requires such access. The organization can conduct periodic audits of user accounts to detect omissions.
Support for FTP	FTP can be used to upload files, including malicious software, directly to the printer without any need for password authentication.	Unless there is a business need for direct printing, disable support for FTP.	Operate all network devices with least privilege.
Network sniffing	Someone can intercept some, or all, of the document contents or capture management codes/passwords by eavesdropping on the network.	Encryption will make the contents of packets unintelligible. Investigate the use of SNMPv3, IPP over SSL (also called IPPS) or IPSEC.	Prohibit unauthorized network sniffing. Allow only controlled sniffing by a few authorized IT support personnel and monitor their use of sniffing. Require the use of encryption where practical.
Windows printer sharing	Early Windows operating systems established unrestricted printer sharing over all network interfaces by default, potentially exposing it the Internet.	Establish a standard Windows installation that has printer sharing turned off by default.	The organizational least privilege policy should cover printer sharing.



Secure use of Multi-Function Devices (CSG-11IS)

Security Issue	Risk	Mitigation	Policy
Risk averse configuration	Printers and MFDs are installed as fully accessible devices within the network, leaving them exposed to denial of service attacks.	Limit the allowable means of sending print jobs. Configure print spoolers to restrict access only to authorized users and restrict users to managing only their jobs. If risk averse and willing to expend the resources, lock down the network devices extensively.	This complies with earlier assessment of level of risk the organization is willing to accept and imposition of least privilege.
Latent documents and image data threats	Storing of spooled print jobs, scanned images, temporary files and other data on internal disk storage makes this data available to someone with physical or network access.	Centrally manage the settings and sharing of printers and MFDs. Configure the device to overwrite temporary data between jobs and the print file after jobs. Encrypt document images prior to temporarily storing them.	Require that IT devices and software have sufficient security features to protect the organization's information.
Threats to hardcopy output	Anyone passing by an open printer can read the contents of the output tray.	Secure the physical device locations. Require that the user authenticate at the console before picking up the output as it is produced.	Include printed output in policy dealing with the protection of sensitive information.
Default	The vendor's default	Replace default administrator	Define policies for acceptable



Secure use of Multi-Function Devices (CSG-111S)

Security Issue	Risk	Mitigation	Policy
passwords	passwords are readily available on the Internet.	passwords with complex passwords. Make a record of the passwords and store them in a secure location. If possible, require two factor authentication mechanisms.	key operator codes, administrator passwords and user codes; identify who can change these and how often; define the acceptable format for these items; and stipulate how they are to be recorded and secured.
Sequence to reset to factory settings	Some devices provide a well-documented sequence of key entries that restore the device configuration to default factory.	Control physical access. If possible, disable this reset sequence or lock the control panel so that authentication is required before making a keypad entry.	Require strong authentication to put the device in user service mode or to override console security controls.
Threats to sensitive documents	If several people have access using one shared identity, any of them can gain access to stored documents, address books, e-mail messages, alter privileges, etc.	Enforce stronger identification and authentication than that afforded by simple PIN codes.	Include appropriate use of access controls in user awareness training.
Threats from scan-to functions	Scan-to functionality can be used to store image files on the device's internal file server, on an FTP server or	Prohibit or carefully control who can use scan-to functionality and carefully log the use of this function.	Re-enforce the organization's acceptable use and protection of information policies through an awareness program. If



Secure use of Multi-Function Devices (CSG-111S)

Security Issue	Risk	Mitigation	Policy
	an SMB server or directly to portable storage such as a USB token, MP3 player, or cellular telephone.	Restrict and control the use of the various scan-to functions as much as possible.	appropriate, prohibit the use of personal storage devices.
Vendor claims	The vendor claims that its products pass stringent internal security controls and are resistant to attack.	It is safest to select devices that are Common Criteria-certified. Ensure the device isolates fax and network support and includes secure file erasure and secure storage erasure.	Whenever possible require that IT products be security certified either using Common Criteria or other expert testing service. Exceptions to this policy should require senior management review and waiver.
Automatic forwarding	MFD settings could be manipulated to automatically forward all faxes to another number.	Logging and periodic reviews of the logs should detect such activity and reconfigured settings.	No new policy is required.
Fax output	By default, some devices print out the first page of every fax sent. This could expose sensitive documentation at the printer.	If possible, disable this feature. At minimum, control physical access and prevent unauthorized individuals from gaining access to the output.	No new policy is required.
Failure to limit allocation of	Allowing individuals within the organization to carry out	The organization should apply standard settings and controls	The IT department is accountable for all aspects of



Secure use of Multi-Function Devices (CSG-111S)

Security Issue	Risk	Mitigation	Policy
administrative rights	support in an <i>ad hoc</i> manner can lead to serious security exposures.	across networked devices. A strictly limited number of authorized individuals should have administrative rights and they should have proper training in support of the devices.	support of its devices.
Remote management web interface	Printers and MFDs often provide a web application interface for remote administration and management tasks. Security researchers have shown that web interfaces are vulnerable to attacks.	Apply the latest security patches. Restrict access by external parties to internal printers and MFDs	No new policy is required.
Support for telnet	Some printers and MFDs will accept Telnet commands for simple management of the device.	Unless there is a vital business need for direct printing, disable support for Telnet. Use more robust system management such as SNMPv3.	Operate all network devices with least privilege.