




**State of North Carolina
Office of Information Technology Services**

Pat McCrory
Governor

Chris Estes
State Chief Information Officer

Memorandum

To: State Security Liaisons

From: Maria S. Thompson 
State Chief Information Risk Officer

Subject: Securing Multifunctional Devices (MFDs) and Network Printers

Date: February 11, 2015

The purpose of this memo is to provide guidance to the implementation, configuration and use of multifunctional devices (MFDs) and network printers on the State and agency networks. MFD's are defined as those devices which offer multiple functionalities such as the following: printer, copier, scanner, fax, and email. MFDs and network printers provide a needed function throughout the State, however, they can have significant vulnerabilities if not properly configured. Many devices used today have embedded operating systems. While these may provide additional capabilities, there are also added risks that could lead to the loss of confidentiality, integrity and availability to State data and resources. The following is a list of recommended techniques that can reduce the risk of using these devices on the State and agency networks and strengthen the overall information security posture. These techniques are intended to be vendor neutral, however, many of these steps may not be applicable for specific brands and model devices.

Configuration Security

- Replace older less secure devices with devices that support secure configuration features.
- Uninstall all unnecessary applications that are not required for business use
- Update the device firmware to the highest level available using vendor signed firmware updates.
- Disable the remote firmware update ability until it is needed. Once the firmware is updated with this process, promptly disable the remote firmware update ability.
- Password protect the firmware update process/utility.
- Use the most currently available client and admin device management software.

- Change all default passwords or community strings, to strong passwords that comply with statewide standards.
- Disable SNMP v1 & v2 and use only SNMP version 3 for printer management if supportable.
- Change the default SNMP parameters and use strong passphrases.
- Disable unneeded network protocols, printer services, and features on the device, example FTP, Telnet, SMTP etc.
- FTP and Telnet should **ONLY** be enabled for firmware updates, if needed, and promptly disabled when finished. Note: Unless there is a specific business need, most MFDs and network printers should **NOT** communicate with the internet.
- Use an Access Control List (ACL) in the device configuration that restricts which subnet, IP address range or specific hosts can use the device.
- Encrypt network traffic to/from the device and use HTTPS, using SSL/TLS for web based device maintenance.
- Configure device authentication (account name and password) for end user functions, where possible.
- Enable the device firewall and configure it to restrict traffic to only those hosts and services that need access to the device.
- Enable auditing and logging on the device and ensure logs are reviewed on a regular basis.
- Generate reports from the device that show users' printing behavior.
- Where possible, configure the device to erase data remanence after each print, scan, copy or fax job.
- Power down the device when it is not needed.

Network Security

- Install devices on an isolated network segment with no internet access.
- Assign a static Internet Protocol (IP) address and disable DHCP on the print device.

Physical Security

- Prevent unauthorized physical access to the device. This requirement is especially critical to those devices used to process sensitive information
- If the device has removal hard drives, restrict access to the keys and/or ability to remove the hard drives

In addition to configuring these devices using the guidelines above, it is recommended that agency information security officers/liaisons ensure a scan of the network be done to identify any MFDs on the network that are vulnerable and/or configured insecurely, and take remediation actions. Note: Depending on the type of data in use, there may be additional restrictions levied due to regulatory requirements, e.g. IRS 1075. More information about securing MFDs and network printers may be found at the following resources.

Resources

HP Jetdirect Security Guidelines

http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c00746792-3.pdf

NCCIC Bulletin "Multifunction Printer Vulnerabilities

<https://msisac.cisecurity.org/resources/reports/documents/A-0012-NCCIC-130020120223MFPVulnerability.pdf>

Internal Revenue Services - *Publication 1075, Tax Information Security Guidelines For Federal, State and Local Agencies* - <http://www.irs.gov/pub/irs-pdf/p1075.pdf>

NIST National Checklist Program - <http://checklists.nist.gov/nep.cfm?scap.cfm>

NIST *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers* (SP 800-70) - http://nvd.nist.gov/docs/SP_800-70_20050526.pdf

Please contact me if you have any questions about the guidelines mentioned in this memo. Thank you.

