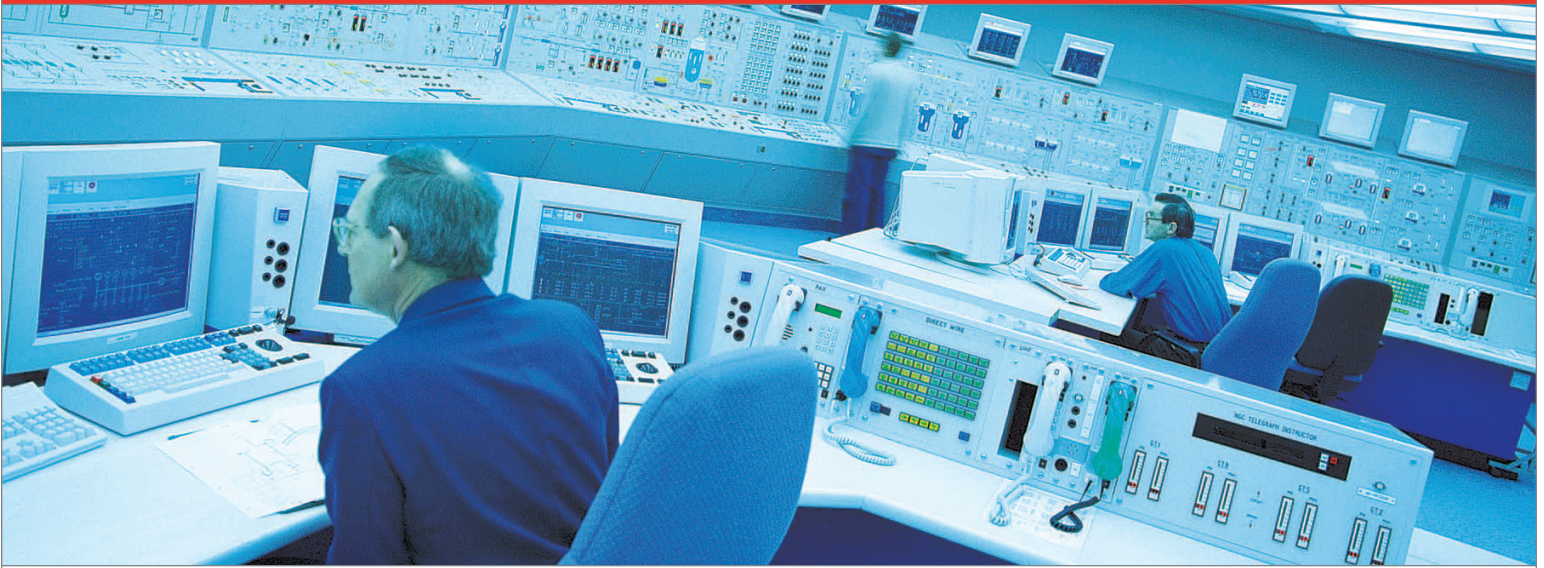


NERC CIP Requirements and Lexmark Device Security



Overview

The information in this document explains how Lexmark multifunction printers (MFPs) and network printers can assist with compliance to the NERC's Critical Infrastructure Protection (CIP) requirements.

The NERC CIP is the first set of comprehensive requirements to protect the electric utility assets from cyber security attacks. The CIP is divided into eight separate reliability standards. Each of the reliability standards identifies the minimum requirements to implement and maintain a cyber security program and protect cyber assets.

With proper setup and use, Lexmark devices and printing solutions can aid an electric utility to comply with six of the eight reliability standards outlined in the CIP. Lexmark will provide a high level overview on how the standard security features and functions in our printing solutions meet those six requirements.

The Lexmark devices that correspond to the information in this document include the Lexmark T640n, T642n, T644n, C532n, C534n, C780n, C782n, W840n, C920n, X642e MFP, X644e MFP, X646dte MFP, X646ef MFP, X850e MFP, X852e MFP, X854e MFP, X782e MFP, X940e MFP, and X945e MFP.

Executive Summary

Lexmark International, Inc. (NYSE: LXX) makes it easier for businesses and consumers to move information between the digital and paper worlds. In doing so, we are guided by a simple vision: Customers For Life. To earn our customers' loyalty, we listen to them, anticipate their needs and the needs of their industries, acting to create value in their eyes. Our customer-driven approach targets mission-critical processes and areas that matter most to your business.

We are aware that utilities are actively working to understand and integrate NERC's Critical Infrastructure Protection (CIP) requirements into their overall security plans. And as the CIP documents include IT assets, Lexmark is committed to providing our utilities customers with additional resources to aid inclusion of output equipment (printers, multifunction printers) as part of that plan.

As printers and multifunction printers (MFPs) continue to evolve into digital on-ramps/off-ramps, understanding the implications of distributed scanning/printing will become more important. Lexmark has identified areas of the CIPs documentation that may be affected, and we have offered guiding information to the IT administrators. CIPs standards discussed in this document are as follows:

- CIP 002 – Critical Cyber Asset Identification
- CIP 003 – Security Management Controls
- CIP 005 – Electronic Security Perimeter
- CIP 006 – Physical Security
- CIP 007 – Security Management Systems
- CIP 009 – Disaster Recovery

This document offers a cursory understanding of how output devices may be included in a CIPs strategy; individual circumstances may require additional discussions.

NERC CIP Requirements

CIP 002 Critical Cyber Asset Identification

As the title suggests, Standard CIP 002 is focused on identifying cyber assets within a utility. However, the requirement to identify the cyber assets does not stop there. The standard also outlines requirements for analyzing the risk associated with the asset, monitoring the asset and annually reviewing an asset. The areas where Lexmark can assist most are the critical asset inventory requirement and the monitoring of an asset. Lexmark tools can discover, catalogue, list the details, and monitor every print asset within the utility's environment.

Lexmark devices and software solutions provide easy to use, but an effective approach to identify and monitor assets within the utility with tools like:

Device Asset Tags

Lexmark MFPs and printers have the ability to personalize each device with an asset tag. Generally used with device management applications, asset tags provide a way to discover, identify, organize, and manage devices on the network.

Asset Tracking and Monitoring

MarkVision Professional (MVP) is a client-server application designed to provide IT professionals a secure, web-enabled way to manage and monitor network print devices in real-time. MVP provides a single platform to discover, communicate, display, and manage information on not only Lexmark devices, but other manufacturer's devices as well. With its built-in security provisions, MVP is designed to prevent unauthorized access to print devices on the network and allow authorized users to display print device information customized to the user's role or job function from a supported Web browser.

FleetView is a remote monitoring system that tracks devices/device status at specified intervals (average is every 15 minutes). FleetView has the ability to store device status and device status changes for the life of the asset, allowing for auditing/reporting of device history. As with MVP, FleetView can monitor Lexmark as well as other manufacturer's devices that are on the network.

CIP 003 Security Management Controls

When looking at the Security Management Control requirements outlined in CIP 003, Lexmark can provide the most assistance in the requirement concerning access control. Lexmark and its partners can provide a utility with solutions that can restrict access to documentation that is considered sensitive within the utility.

Confidential Print

Lexmark MFPs and printers support confidential print. Confidential Print is a normal print job that is held in RAM or on hard disk until the intended recipient enters the appropriate PIN, which causes the job to be printed. Held jobs can be set to expire after an elapsed time (configurable from one hour to one week), and a limit on the number of times a PIN can be entered incorrectly can be set before the corresponding jobs are purged.

Document Level Security

Lexmark MFPs, when combined with Lexmark Document Distributor and Adobe Policy Server, can offer document level security for all scanned documents. Using this solution allows an end user to apply document-specific policies that ensure that scanned images are viewed by authorized individuals or groups. Out-of-date documents can be terminated via policies from a centralized location.

Printing Permissions

Plus Technologies' OM Plus Server, when combined with Lexmark print devices, can offer an enterprise the ability to decide which documents can be printed or not printed (based on print criteria such as user, application, document size, etc.).

CIP 005 Electronic Security Perimeter

This CIP requirement is a major strength for Lexmark MFPs and printers. Lexmark looks at this requirement as overall device hardening. Device hardening is the process of securing the device's network interfaces. This includes eliminating unneeded or unused features and functions to prevent their abuse, locking down any interfaces that remain, and securing the data hosted by the device.

Lexmark MFPs and printers include a variety of mechanisms to facilitate the device hardening process such as:

TCP Connection Filtering

MFPs and printers can be configured to allow TCP/IP connections only from a specified list of TCP/IP addresses. This disallows all TCP connections from other addresses, which protects the device against unauthorized printing and configuration.

Network Port Filtering

The network ports on which MFPs and printers listen for or transmit network traffic can be configured, allowing a huge degree of control over the device's network activity.

By filtering out traffic on specific network ports, protocols such as telnet, FTP, SNMP, HTTP, and many others can be explicitly disallowed.

Hard Disk Encryption

Hard disks in MFPs and printers can be configured to use encryption, allowing a utility to secure the data stored on the Lexmark device (regardless of length of storage time). A 128-bit AES key is internally generated by the printer or MFP and used to encrypt all data on the drive.

The key is stored non-contiguously on the device, making the contents of the drive accessible only on the drive's original printer or MFP. The data on a stolen drive would not be accessible, even if it were installed in an identical model of printer or MFP.

802.1x

802.1x port authentication allows MFPs and printers to join networks that require devices to authenticate prior to accessing the network. 802.1x port authentication can be used with the WPA (Wi-Fi Protected Access) feature of an optional wireless print server to provide WPA Enterprise security support.

Digitally Signed Firmware Updates

Lexmark MFPs and printers automatically inspect downloaded firmware upgrades for the appropriate Lexmark digital signatures. Firmware that's not correctly packaged and signed by Lexmark is rejected. This ensures that non-approved firmware is never run on the devices, which avoids exposing the MFPs and printers to malicious software such as viruses and worms.

Secure LDAP over SSL

All LDAP traffic to and from MFPs can be secured with SSL. Exchanging LDAP over an SSL connection. This means the information exchanged via LDAP, including the user's credentials, names, email addresses, and fax numbers, is encrypted to preserve the confidentiality and privacy of the data.

Certificate Management

Lexmark MFPs and printers use certificates for HTTPS, SSL, IPSec, and 802.1x authentication. The certificate management feature of printers and MFPs allows the devices to integrate with a PKI environment by allowing the devices' certificates to be signed, and by allowing the printers and MFPs to trust certificate authorities in the customer's PKI environment.

CIP 006 Physical Security

Like device hardening, physically securing a device is a must. This CIP focuses on restricting access to and monitoring the use of a device. Lexmark MFPs and printers include standard features to secure the use of the device, ensuring only appropriate users use the device functions and that the information associated with those users is protected.

Some of the mechanisms used to facilitate the protection of Lexmark MFPs and printers are as follows:

Secure User Authentication

Lexmark MFP functions can be restricted so that users must authenticate prior to performing copy, scan to email, scan to fax, scan to network, workflow scripts, or embedded applications. MFPs can be configured to authenticate users against the customer's corporate directory via LDAP, LDAP over SSL, Kerberos, or NTLM. These authentication methods are secure, and compatible with Active Directory and other directory server platforms.

IPSec

IPSec allows all network traffic to and from Lexmark MFPs and printers to be secured with encryption and authentication. This allows data to be sent to MFPs and printers securely and allows scanned jobs to be transferred securely from MFPs.

Printer Lockout

Printers can be locked so that the printer's front panel is disabled and all incoming print jobs are stored securely on the printer's hard drive. The printer can then be unlocked by entering the appropriate PIN. This feature is available on printers that are equipped with a hard drive.

MFP Lockout

MFPs can be locked so that the MFP's touch screen is disabled; all incoming print and fax jobs are stored securely on the hard drive until the MFP is unlocked by entering the appropriate PIN. This feature is available on MFPs that are equipped with a hard drive.

Incoming Fax Holding

Lexmark MFPs can be configured to hold, rather than print, incoming faxes during scheduled times. Incoming faxes are held securely on the MFP's hard drive until a predefined password is entered.

Separation of Fax and Network Cards

The fax modem on a Lexmark MFP is restricted to Facsimile Class 1 mode, and the data transferred over the modem is limited to facsimile image data, only. The connection is not like a laptop modem or other device where an arbitrary network connection can be established via the fax modem. The information exchanged over the MFP's modem is restricted to image data, only.

Network protocols are not supported through the fax modem. There's no support for exchanging TCP/IP traffic of any sort, including telnet, FTP, HTTP, SNMP, or any other form of network packet.

There's no support for modifying the MFP's configuration via the fax modem connection. Settings can't be viewed or changed, and there's no access to the MFP's file system through the fax connection.

Compatible with Physical Locks

MFPs and printers support Kensington-style locks, which allow the devices to be physically secured. Locking a printer or MFP also locks down the metal cage that houses hard drives and

optional components, preventing those components from being tampered with or stolen.

Hard Disk Encryption

Hard disks in MFPs and printers can be configured to use encryption, ensuring that any data stored on the Lexmark device cannot be easily removed by unauthorized individuals. A 128-bit AES key is internally generated by the printer or MFP and used to encrypt all data on the drive.

The key is stored non-contiguously on the device, making the contents of the drive accessible only on the drive's original printer or MFP. The data on a stolen drive would not be accessible, even if it were installed in an identical model of printer or MFP.

Hard Disk Wiping

Lexmark MFPs that contain hard drives support two levels of disk wiping (fast and secure). A fast disk wipe is a single low-level hard disk wipe. A secure disk wipe, otherwise known as a DoD 5220.22-M compliant wipe, is a multiple pass disk wipe. Both of the wiping processes apply to the entire hard drive, so all residual data left over from buffered data is completely removed from the device. The hard drive wiping process can be activated manually, through the MFP's operator panel. Disk wiping is a level of protection designed to be used when the system is taken out of service or removed from a secure location. This functionality ensures that any data present on the hard drive could not be recovered even if the encryption key was compromised.

CIP 007 Security Management Systems

Lexmark summed up this CIP requirement as secure device/fleet management. Management of a fleet of networked MFPs and printers remotely is a must; however, the remote management must be secure. The device must allow authorized people to configure it, while rejecting those that are unauthorized. Also, the process of managing the device must be secured so that the network traffic associated with the remote management cannot be sniffed, stolen or abused.

Lexmark MFPs and printers include a variety of features to make remote device management easier and more secure. Detailed below are some features that can assist a utility in complying with the requirements outlined in this standard:

Administrative Password Protection

Lexmark MFPs support two administrative passwords. The “Advanced Password” provides control over all of the MFP’s settings, but does not give access to the MFP’s operating system or hard drive. The “User Password” allows configurable access to functions that are set by the administrator of the device. These two passwords protect the configuration of the device via the touch screen operator panel and through network access via HTTP, HTTPS, and telnet.

MFP passwords must be at least 8 characters in length, and can be up to 128 characters in length. Passwords can include alphabetic, numeric, and other characters to allow for substantial complexity. There is no support for creating additional passwords, and there are no means to grant administrative access to users or administrative accounts that exist in the corporate domain, outside of the MFP.

Lexmark Printers support a network password to keep unauthorized people from using a browser or other network tool to configure the printer. Users can point their browser to the printer on the network and see the basic status of the device, but any attempt to configure the printer results in a challenge for the password. If the user can’t provide the password, then configuration of the printer is not allowed.

The printer password can be up to 128 characters in length, and supports alphabetic, numeric and other characters to allow for substantial complexity. The password is not associated with a user name, and there’s no support for creating additional administrative accounts—there’s just one administrative account, and this password controls access to it. (The ability to create additional accounts can lead to more vulnerabilities by allowing undetected and potentially long-lasting accounts to be created.)

Lexmark printers also support a PIN to protect the printer from unauthorized configuration via the printer’s operator panel. When an attempt is made to configure the printer via the operator panel, the printer prompts the user for the PIN. Unless the proper PIN is entered, the printer’s settings cannot be changed.

The PIN is 4 digits of a value 0-9 with a range of 10,000 values and is set up through the printer’s web page. It can be applied

to all of the settings accessible through the operator panel, or it can be selectively applied to the sections of the printer’s menus that deal with paper settings, general device settings, reports, and network/port settings.

HTTPS

HTTPS provides a means to securely manage networked MFPs and printers. It allows web traffic to be encrypted, so that remote management via the printer and MFPs web pages can be performed securely.

SNMPv3

SNMP is a standard network management protocol, and version 3 (SNMPv3) includes extensive security capabilities. Lexmark’s MFPs and printers support SNMPv3, including the authentication and data encryption components, allowing for secure remote management of the devices.

Note that SNMPv1/v2 are also supported and can be independently configured and/or disabled.

Remote Asset Monitoring

MarkVision Professional (MVP) is a client-server application designed to provide IT professionals a secure, web-enabled way to manage and monitor network print devices in real-time. MVP provides a single platform to discover, communicate, display, and manage information on not only Lexmark devices, but other manufacturer’s print devices as well. With its built-in security provisions, MVP can prevent unauthorized access to print devices on the network and allow authorized users to display print device information customized to the user’s role or job function from a supported Web browser.

CIP 009 Disaster Recovery

Although many precautions are in place to prevent a disaster, a utility cannot overlook the possibility that one could happen. The key is to have a speedy recovery to limit downtime and loss of data. CIP 009 outlines requirements to aid in the recovery effort. Lexmark devices and device management solutions can also assist with the recovery effort by providing methods of exporting or backing up device settings and quickly redeploy those settings.

Listed below are a few Lexmark solutions that can aid with the recovery effort:

Import/Export Device Settings

Lexmark MFPs and printers have the ability to export and import device configuration settings. This provides a mechanism to take the settings from a configured device and transfer them to a single device or deploy those settings to multiple devices. The exported file, known as a Universal Configuration file or UCF, can also be used as a backup in case of device failure.

Remote Device Configuration

MarkVision Professional (MVP) is a client-server application designed to provide IT professionals a secure web-enabled way to manage and monitor network print devices in real-time. In the event that output devices must be reconfigured due to catastrophic event or other extenuating circumstances, Markvision's device policy feature will provide a utility a quick method for remote reconfiguration of their output devices. Thus ensuring that users can begin communicating immediately and that predetermined security policies can be restored.

Co-authored by:

Lyle McMillin - Lexmark Industry Consultant, Energy & Utilities

Sean Gibbons - Lexmark Technical Security Consultant

Lexmark reserves the right to change specifications or other product information without notice. References in this publication to Lexmark products or services do not imply that Lexmark intends to make them available in all countries in which Lexmark operates. LEXMARK PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. This publication may contain third party information or links to third party sites that are not under the control of or maintained by Lexmark. Access to any such third party information or site is at the user's own risk and Lexmark is not responsible for the accuracy or reliability of any information, data, opinions, advice or statements made by these third parties. Lexmark provides this information and links merely as a convenience and the inclusion of such information and/or links does not imply an endorsement. All performance information was determined in a controlled environment. Actual results may vary. Performance information is provided "AS IS" and no warranties or guarantees are expressed or implied by Lexmark. Buyers should consult other sources of information, including benchmark data, to evaluate the performance of a solution they are considering buying.