**Eaton Guide Specification**

**Notes and instructions to Spec Writer**

The following guide specification is offered for your assistance in specifying this product as part of a CSI (Construction Specification Institute) compliant document. This guide specification has been created in MS Word and uses Word features including **Styles** and **Review** to assist in editing and formatting. You may also find it helpful to view the document in **Outline** mode when editing or selecting sections to copy/paste into your base document.

**Styles**

Styles are provided for all paragraph types described in the CSI Masterformat. Applying a Style to text will provide the correct indentation, paragraph letter/number, font, capitalization, etc. Styles are shown on the right-hand side of the Word “Home” ribbon.



**Review**

“Notes to Specwriter” (when available) are provided using the Reviews feature in Word. To view “Notes to Specwriter” select “All Markup” in the Tracking dropdown menu on the Review ribbon. To hide notes, select “No Markup”. You can advance from one note to the next using the Previous and Next buttons on the same ribbon. In earlier versions of MSWord hide notes by un-checking ‘Comments’ under Review>SH



**Outline view**

The Outline view within Word is often helpful when editing or copying sections from this Guide Specification. Also, when pasting sections from this document into a base document the Spec Writer may want to consider using right-click and “Merge Formatting’ or ‘Keep Text Only” features.

26-08-00

OT CYBERSECURITY SECURE COMMISSIONING AND HARDENING

# General

## SCOPE

### To enhance the resiliency and security of the installed equipment, a cybersecurity review for all devices capable of network connectivity shall be performed to address their ability to withstand unauthorized updates and malicious attacks while continuing to perform their intended function.  Equipment shall be configured in a manner that is consistent with manufacturer recommendations and appropriate with its specific application and installation environment. Special attention shall be given to how the equipment is interconnected and any software or systems that are networked to the equipment.  Manufacturer recommended hardening shall be completed by an original manufacturer trained representative.

*Definition of supplier and contractor responsibilities*

*Listing of customer equipment to be assessed.*

## RELATED SECTIONS

*If this specification is part of a larger Project spec, list references to other proposal specification sections/documents that pertain to this section*

## codes AND STANDARDS

### NFPA 70 – 110.3(A)

### NFPA 70 – 240.6 (D) 2.b

### NFPA 70 – 708.7

### IEC 62443

### NERC CIP

## References

### NIST RMF

### NIST.SP.800

### UL 5500

### UL 2900

## submittals

### The following information shall be submitted to the engineer:

#### Component Lists

#### Device Hardening Guides

#### *Master Drawing Index*

#### *Schematic Diagrams*

#### *Network Architecture Drawings*

## Qualifications

### The commissioning and hardening activities shall be performed by original equipment manufacturer trained personnel or by one of the following vendors:

### Eaton

### \_\_\_\_\_\_\_\_\_\_

### \_\_\_\_\_\_\_\_\_\_

### \_\_\_\_\_\_\_\_\_\_

## coordination

### Service Kick-Off Meeting

### The Contractor shall conduct a meeting with customer to discuss:

#### Project scope

#### Project Schedule

#### Site access and safety

#### Resources needed

#### Data handling, classification, and cybersecurity hygiene

#### Verifications & validation

#### Execution risk management

# EXECUTION

## cybersecurity commissioning and hardening

### The following activities will be performed on Eaton supplied equipment and/or systems capable of network connectivity.

#### **Secure Configuration Review**: Perform a thorough review of the configurations for each asset to ensure they follow industry best practices and OEM security guidelines. This includes examining settings, logical/physical ports, permissions, and other configurable parameters, within the context of the installed environment.

#### **Access Control Audit**: Conduct an audit of access controls to verify that only authorized personnel have appropriate access privileges. This includes reviewing user accounts, permissions, passwords, and other authentication methods. Assess the site’s current access control procedures (if available) and ensure devices are in compliance (as applicable). As appropriate, make any recommendations to site’s access control procedures.

#### **Patch and Update Management Review**: Ensure each Eaton supplied device is running the latest firmware and has the latest patches (as applicable). Assess the sites current patch and update management processes (if available) and ensure devices are in compliance (as applicable).. As appropriate, make any recommendations to site’s patch and update management process.

#### **Documentation and Asset Inventory Update**: Create a comprehensive catalog of all Eaton supplied devices. Unless otherwise agreed to with customer, this will include IP address, MAC address, device type and model, firmware/software version, hardware revision, serial number, location, and vendor information.

##### ***Network Segmentation Analysis****: Analyze the existing network segmentation in which the supplied devices and/or system exist. Assess the effectiveness in isolating critical assets and limiting unauthorized access. Identify any areas that require adjustment or improvement and make recommendations.*

##### ***Physical Security Analysis****: Review the physical security measures in place to protect the Eaton supplied assets. This can involve reviewing access controls, surveillance systems, and physical barriers to identify any potential vulnerabilities. Identify any areas that require adjustment or improvement and make recommendations.*

##### ***Vulnerability Analysis****: Conduct a thorough examination of the environment in which the Eaton supplied devices or system is installed, with the aim of identifying potential weaknesses, security flaws, and vulnerabilities that could be exploited by malicious actors. The analysis focuses on assessing the security posture of the Eaton supplied devices, resulting in recommendations for remediation and mitigation strategies to enhance the overall security of the system environment.*

##### ***Incident Response Plan Review****: Review the existing incident response plan to ensure it is up to date and aligned with the organization's objectives. Recommendations will be made as required. Verify that key stakeholders are aware of their roles and responsibilities in the event of a security incident.*

##### ***Security Policy and Procedure Review****: Review the existing security policies and procedures to ensure they reflect current best practices and industry standards. Identify any gaps or areas requiring updates or additional documentation. Recommendations will be made as required.*

# TRAINING AND CLOSEOUT ACTIVITIES

## Owners Training

1. The contractor shall provide a training session for up to five (5) owner’s representatives for 4 hours on the cybersecurity operation and maintenance of the secured devices.
2. Instruction shall include the following maintenance tasks:
3. Adding Users
4. Removing Users
5. Updating Passwords
6. Firmware Updates
7. Hardening Guidelines
8. Security Awareness Training

## verification and validation report

### Eaton will provide one electronic copy of hardening report detailing activities performed on each device.

--- END ---