This document is to provide suggested language to address cyber security elements as they may apply to physical and electronic security projects. Security consultants and specifiers should consider this language in light of the planned project and clients' specific security postures. As this is designed to be a guideline, consultants and specifiers should modify, add, or delete language to fit the specific circumstances which may exist within the client's organization and project. It is strongly recommended that final language be developed in cooperation with the client's Information Technology Department.

For additional information, contact:

SecuritySpecifiers
Phone: +1 203 405-3740
Web: www.securityspecifiers.com
Contact: Raymond Coulombe
E-mail: ray@securityspecifiers.com

CYBER SECURITY

DIVISION 28 – ELECTRONIC SAFETY AND SECURITY

28 05 11 Cyber Security Requirements for Electronic Safety and Security

Notes to Specifier:

1. Where several alternative parameters or specifications exist, or where, the specifier has the option of inserting text, such choices are presented in **<bold text>.**

2. Explanatory notes and comments are presented in ***italicized and colored*** text.

CYBER SECURITY

PART 1 GENERAL

1.01 SUMMARY

A. Section includes criteria to enhance project cyber security.

B. Related Requirements

1. 27 20 00 Data Communications
2. 28 05 13 Servers, Workstations and Storage for Electronic Safety and Security
3. 28 05 31 Communications Equipment for Electronic Safety and Security
4. 28 05 33 Safety and Security Network Communications Equipment
5. 28 08 00 Commissioning of Electronic Safety and Security

1.02 REFERENCES

A. Abbreviations

1. AD – Active Directory
2. DMZ – Demilitarized Zone
3. ICMP – Internet Control Message Protocol
4. IT – Information Technology
5. NTP – Network Time Protocol
6. SFTP – Secure File Transfer Protocol
7. SNMP – Simple Network Management Protocol
8. SSL – Secure Sockets Layer
9. TLS – Transport Layer Security
10. VLAN – Virtual Local Area Network
11. VPN – Virtual Private Network

B. Definitions

1. Strong password – A random sequence of 16 or more characters, employing upper and lower-case letters, numbers, and special characters.

C. Reference Standards and Guidance

1. National Institute of Standards and Technology (NIST) CyberSecurity Framework
2. ISO/IEC 27000 Family of Standards
3. IEEE 802.1x – 2010 Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control
4. **<ANSI/CAN/UL 2900-2-3:2017 - Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems>**

ANSI/CAN/UL 2900-2-3 is a new standard not yet broadly adopted by the security industry. The majority of security products have not yet been tested or approved in accordance with this standard.

5. Center for Internet Security – CIS Controls Version 7

1.03 SUBMITTALS

A. Informational
   1. Manufacturer cyber hardening manuals or guides.
   2. Certification report by an acceptable independent testing organization of successful cyber vulnerability test of proposed product,
      a. Certification testing shall have been completed no more than 12 months prior to submittal.
   3. Contractor's plan for secure assignment of unique strong passwords to all installed products requiring passwords.
   4. Contractor's plan for assignment of administrative and operator rights to installed products.
   5. List of cloud services and providers to be provisioned.

B. Closeout
   1. Asset Management
      a. Secured spreadsheet or equivalent summary of all security devices and software installed to include:
         1.) Manufacturer, model, and firmware or software version
         2.) Serial number and MAC address, if applicable
         3.) Network settings, including IP address, VLAN or subnet mask, default gateway
         4.) Equipment location
         5.) Device user names and passwords
   2. Licenses
      a. License files and license key numbers
      b. Additional codes required for operation
   3. Services and ports
      a. Summary of enabled and disabled product services
      b. Summary of all open ports
   4. Security recommendations
      a. Summary of additional recommended physical, network, or program actions to enhance the cyber security of the installation.
   5. Post-installation vulnerability test report

1.04 QUALIFICATIONS

A. Manufacturer shall have a documented process for secure development and testing of software code.

B. Manufacturer shall have a secure process for verifying and provisioning firmware and software updates.

C. Contractor personnel assigned to device programming and software installation shall have been certified in these tasks by the Manufacturer or possess industry certifications acceptable to the Manufacturer and the Owner attesting to the necessary competence.

1.05 SUPPORT

A. Manufacturer shall have a documented process for notifying and provisioning firmware or software updates to users of its products.

END OF SECTION

PART 2 PRODUCTS

2.01 DEVICES

A. Security devices shall have the following properties:
   1. Means to securely provision passwords
   2. Controlled use of administrative privileges
   3. Ability to synchronize with a common time base across all devices, such as an NTP server
   4. Ability to disable all unneeded or unused services, including ICMP and discovery protocols
   5. Option for encrypted communication and storage
   6. Limitation on remote access
   7. Support for secure versions of protocols to include HTTPS, SFTP, SNMP v3
   8. Support for IEEE 802.1x, port-based network access control
   9. Ability to prevent a valid digital certificate to third party and user processes
   10. IP and MAC address filtering
   11. Prompt for installer to change from default device password before security operation.

2.02 SERVERS

A. Servers shall be delivered with the server manufacturer, operating system(s) and provisioned applications full patched and testing to the latest supplier version.

B. Servers shall be provisioned with antivirus/anti-malware software acceptable to the Owner.

C. SQL (database) applications shall be provisioned on separate server(s) **<in a redundant fashion>**.

2.03 CLIENTS

A. Client machines provided by the Contractor shall be delivered with the server manufacturer, operating system(s) and provisioned applications full patched and testing to the latest supplier version.

B. Supplied client machines shall be provisioned with antivirus/anti-malware software acceptable to the Owner.

C. Client shall be provisioned credentials in accordance with the principle of least privilege.

D. Client machines shall be provisioned with the minimum functionality required to perform their required tasks.

2.04 SOFTWARE

A. Application software shall have been developed in a secure coding environment, as certified by its manufacturer.

B. Software shall have been subjected to and successfully passed third party vulnerability testing within 12 months prior to Contractor proposal of the product.

C. Software shall have the ability to accept encrypted communication from remote client and field devices.

D. Required ports shall be clearly identified in the Manufacturer’s documentation.

E. Software shall have configuration settings permitting back-up and failover in the event of the failure of its primary server.

F. Software shall have log capability to document user activity, performance, and usage patterns.

2.05 NETWORK

A. The security system shall be isolated from other User systems via **<firewall> <VLAN> <subnetting>** in a manner acceptable to the User IT department.

B. Any network product deployed within this project shall be furnished with the latest manufacturer firmware.

C. User names and passwords, if applicable, shall be changed from their default value to be consistent with the strength of passwords provisioned in network connected devices.

D. Wireless Networks

1. Wireless transmission devices shall employ WPA2 security.
2. Wireless functionality shall be disabled on all devices not requiring it.

2.06 CLOUD SERVICES

A. To the extent that cloud services are deployed, any party with access to those services in relation to this project shall be subject to approval by the User, and credential levels shall be provisioned in accordance with the principal of least privilege.

B. Provisioned cloud services shall be redundant in nature such that the loss of a cloud server or connection thereto shall not cause a loss of data or services to the User.

2.07 MOBILITY

A. Services for mobile services shall use only those ports recommended by the Manufacturer associated with the given service.

B. Mobile servers shall be placed in a DMZ with separate interfaces for internal and external access.

C. All non-essential protocols and services shall be disabled on the mobile services server.

D. Mobile services shall be provisioned with multi-factor authentication enabled.

E. Mobile communications shall be provisioned to operate only through HTTPS or secure VPN connections.

END OF SECTION

PART 3 EXECUTION

3.01 INSTALLERS

A. Contractor personnel shall comply with all applicable state and local licensing requirements.

B. Contractor personnel assigned to device programming and software installation shall have been certified in these tasks by the Manufacturer or possess industry certifications acceptable to the Manufacturer and the Owner attesting to the necessary competence.

3.02 PREPARATION

A. Before installation of the system, the Contractor shall coordinate system network settings with the Owner's IT Department.

B. The Contractor shall prepare an asset management worksheet for approval by the Owner.

C. The Contractor shall insure that all devices to be installed possess the current version of manufacturer firmware or software.

It is recommended that the User perform a pre-installation network vulnerability assessment in order to establish a secure baseline condition for the system.

3.03 SECURE STORAGE

A. All security system components, including servers and client machines, shall be stored in a secure environment prior to installation.

3.04 INSTALLATION

A. Installers shall follow all recommended procedures and guidelines from the Manufacturer to securely provision network connected products.

B. The Contractor and its authorized installers shall:

1. Follow an Owner-approved password provisioning plan
2. Complete the owner-approved asset management worksheet to include:
   a. Manufacturer, model, and firmware or software version
   b. Serial number and MAC address, if applicable
   c. Network settings, including IP address, VLAN or subnet mask, default gateway
   d. Equipment location
   e. Device user names and passwords

   Note: Alternatively, if the worksheet is not protected, user names and passwords should be provided via a secured means to the Owner.
3. Synchronize security devices with a common time base acceptable to the Owner
4. Disable all services and ports not required for ongoing system operation
5. Provision device and system privileges in a manner approved by the Owner.

3.05 PHYSICAL ACCESS

A. The Contractor and its authorized installers shall make the Owner aware of any physical condition or circumstance at the project site which it deems to constitute a potential cyber risk.

Cyber security should involve physical access control to potentially vulnerable security devices and systems and recording of activity around them.

3.06 TESTING

A. In conjunction with the Owner's IT Department, the Contractor shall arrange for a post-installation vulnerability test to verify that additional cyber vulnerabilities have not been introduced into the Owner's network as a result of this project.

END OF SECTION