SECURITY RESOLUTION CERTIFICATE FOR FIRE ALARM COMMUNICATORS

1. Security Resolution Certificate Number (SRCN-Facility Location Number-MMDDYYYY):	2. Facility Name
	3. Facility Location Number (8 digits)

4. Facility Address

5. City	6. State/Territory

7. Device Name and Model Evaluated (e.g., Bosch B465)

8. Communication Pathway

☐ Cellular Only ☐ Radio Only ☐ Ethernet Only ☐ Radio and Ethernet ☐ Cellular and Ethernet

9. Vulnerability Findings	Vulnerability Finding Resolved?		
	N/A	Yes	No
a. Have factory default passwords for all "out-of-the-box" accounts been changed? (i.e., passwords shall be alphanumeric and a minimum of ten (10) characters which include a combination of letters, numbers, and special characters)	☐	☐	☐
b. Has the Hypertext Transfer Protocol Secure (HTTPS) web service been enabled?	☐	☐	☐
c. Has the Hypertext Transfer Protocol (HTTP) web service been disabled?	☐	☐	☐
d. Has the Telnet protocol been disabled?	☐	☐	☐
e. Has the Simple Network Management Protocol (SNMP) protocol been disabled?	☐	☐	☐
f. Has the Secure Shell (SSH) protocol been disabled?	☐	☐	☐
g. Has the Trivial File Transfer Protocol (TFTP) been disabled?	☐	☐	☐
h. Has the File Transfer Protocol (FTP) been disabled?	☐	☐	☐
i. Has the Cloud (Remote Connect) via Ethernet been disabled?	☐	☐	☐
j. Has the Cloud (Remote Connect) via Cellular been disabled?	☐	☐	☐
k. Have wireless communications (e.g., 802.11 Wi-Fi, Bluetooth, ZigBee, Z-Wave, Ultra High Frequency (UHF)/Radio High Frequency (RHF), etc.) been disabled, unless previously specified as required?	☐	☐	☐
l. Has Transport Layer Security (TLS) version 1.2 or higher encryption been enabled?	☐	☐	☐

Vulnerability Findings *(Continued)*	Vulnerability Finding Resolved?		
	N/A	Yes	No
m. Has Secured Sockets Layer (SSL) version 1.0 through SSL version 3.0 encryption been disabled?	☐	☐	☐
n. Has TLS version 1.0 and TLS version 1.1 encryption been disabled?	☐	☐	☐
o. Has the device been configured to be compliant to Federal Information Processing Standards (FIPS) 140, if possible?	☐	☐	☐
p. Has the device been configured to have user management roles? (e.g. administration level user, regular user, etc.)	☐	☐	☐
q. Have the Domain Name System (DNS) servers been configured as follows? • Primary 159.142.69.100 • Secondary 159.142.45.40	☐	☐	☐
r. Have the Network Time Protocol (NTP) servers been configured? • ntp.gsa.gov	☐	☐	☐
s. Have the following Internet Protocol (IP) addresses been configured for NTP if DNS is not supported? (Not all devices will support multiple entries) • 172.30.139.240 • 172.30.99.240 • 172.30.69.240	☐	☐	☐
t. Has the GSA warning banner been configured? (e.g., Full Banner "This is a U.S. General Services Administration Federal Government computer system that is FOR OFFICIAL USE ONLY. This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution." or Abbreviated Banner "This is a U.S. General Services Administration Federal Government computer system that is FOR OFFICIAL USE ONLY.")	☐	☐	☐

This certificate ensures a reasonable level of assurance that the security vulnerabilities noted in the Security Assessment Report (SAR) have been resolved and implemented correctly at the subject facility during installation of the subject device.

10. Name of Installation Technician	11. Name of Firm	
12. Signature	13. Telephone Number	14. Date
15. Name of GSA Approving Official		
16. Signature	17. Telephone Number	18. Date

THIS CERTIFICATE IS VALID ONLY FOR THE SUBJECT FACILITY AND THE SPECIFIC DEVICE

INSTRUCTIONS

Item 1 - Security Resolution Certificate Number: Begin with the letters "SRCN" followed by 8-digit GSA Facility Location Number designation and certificate date (e.g., SRCN-DC0031ZZ-01232022).

Item 2 - Facility Name: List official facility name in the Real Estate Across the United States (REXUS) system.

Item 3 - Facility Location Number: List the 8-digit GSA Facility Location Number (e.g., DC0031ZZ).

Item 4 - Facility Address: List official facility street address.

Item 5 - City: List official City the facility is located.

Item 6 - State/Territory: List the abbreviation of the State/Territory that the facility is located (e.g., DC).

Item 7 - Device Name and Model Evaluated: (e.g., Bosch B465 Universal Dual Path Communicator).

Item 8 - Communication Pathway: Check one based on the SAR report.

Item 9 - Brief Description of Vulnerability Findings and Vulnerability Findings Resolved: Must address each Vulnerability Finding (a - t). Must check either Not Applicable (N/A), Yes, or No for each Vulnerability Finding.

Item 10 - Name of Installation Technician: Enter the name of the Installation Technician.

Item 11 - Name of Firm: Enter the name of the Firm employing the Installation Technician.

Item 12 - Installation Technician Signature: The Installation Technician signs here.

Item 13 - Installation Technician Telephone Number: Enter the Installation Technician's work phone number.

Item 14 - Installation Technician Signature Date: Enter the date the Installation Technician signed the certificate.

Item 15 - Name of GSA Approving Official: Enter the name of the GSA Approving Official (the GSA Regional Fire Protection Engineer) who witnessed installation of the device.

Item 16 - GSA Approving Official Signature: The GSA Approving Official (GSA Regional Fire Protection Engineer) signs here.

Item 17 - GSA Approving Official Telephone Number: Enter the GSA Approving Official's (GSA Regional Fire Protection Engineer's) work phone number.

Item 18 - GSA Approving Official Signature Date: Enter the date the GSA Approving Official (GSA Regional Fire Protection Engineer) signed this certificate.