Rockwell Automation

ACTION PLAN:

How to Win a Critical Infrastructure Cybersecurity Grant

An essential guide to applying for federal funds to protect mission-critical data, applications, assets, and services in your state or local community

Table of Contents

Introduction

In this guide, we outline actionable steps in the application process, and provide a basic cybersecurity checklist to better protect critical infrastructure IT and OT.

At-a-glance: Simplifying steps to a successful federal cybersecurity grant application

If you lead efforts at the state or local government level to improve critical infrastructure cybersecurity as defined by CISA, this guide is for you.

Below, you will find guidance on how to identify resources and apply for federal funding in support of your mission under the IIJA cybersecurity grant program, which extends from 2022 to 2026. Specifically, this manual explains:

- What the cybersecurity grant program entails, why it is time-critical, and how leveraging it from the outset will help improve your critical infrastructure IT/OT
- Where to start and focus when identifying federal cybersecurity funding to improve the resilience of critical infrastructure in your local, tribal, or state agency
- How to avoid red tape or getting tripped up by the registration steps to successfully complete the grant application process long before the deadline.

> "Every organization – large and small – must be prepared to respond to disruptive cyber activity."
>
> *– CISA Shields Up warning*

Our checklist highlights essential steps and is designed to complement more detailed funding guidance for the State and Local Cybersecurity Grant Program as issued by DHS or FEMA, or provided by CISA's federal cybersecurity coordinator in your state (more on that role below).

Specifically, this manual does not replace any federal Notice of Funding Opportunity (NOFO) to be published in fiscal 2022 or beyond, for example on Grants.gov or by FEMA.

The sole purpose of this guide is to give organizations a preview of useful steps, links and informational resources available at the time of publication to support applying for a federal cybersecurity grant. Use the action plan below to accelerate the cybersecurity grant application process.

Critical Infrastructure Industries

16 Critical Infrastructure Industries as defined by CISA

Critical Infrastructure Under Attack

The federal funds awarded through the State and Local Cybersecurity Grant Program cannot arrive too soon. America's Critical Infrastructure providers have seen an unprecedented wave of damaging cyberattacks recently.

Criminal ransomware gangs, nation-state threat actors, and ideologically motivated "hacktivists" have increasingly targeted state and local government operations, as well as public safety, health services, and public utility providers. 2021 marked the first year in which at least two deaths were linked to ransomware attacks against healthcare facilities in the U.S. and in Europe.[1]

Many of the attacks could be attributed to threat actors operating out of Russia, China, North Korea, and Iran, say U.S. intelligence officials and leading private sector security researchers. With Russian president Vladimir Putin's threats of retaliatory attacks following sanctions imposed by the U.S. and allies in the aftermath of Russia's Ukraine invasion, this threat is heightened in 2022.

"Every organization – large and small – must be prepared to respond to disruptive cyber activity," warns CISA in a recent update. How can your state's or municipality's cybersecurity posture benefit from federal funding under IIJA – and when?

State and Local Cybersecurity Grant Program: Nuts and Bolts

The State and Local Cybersecurity Grant Program is budgeted at $200 million in fiscal year (FY) 2022, $400 million in FY 2023, $300 million in FY 2024, and $100 million in FY 2025. Granting agencies are expected to begin to accepting applications in the third quarter of 2022.

To be first in line, eligible entities must collaborate – the program awards coordination and planning across state and local government lines. Preparedness grants are awarded to entities that invest in strengthening Critical Infrastructure cybersecurity through rapid threat detection, response capabilities and proactive planning.

The preparedness grant application process and the allocation of funds under the State and Local Cybersecurity Grant Program are managed by FEMA, under guidance from CISA.

[1] GovInfoSecurity

Smart Grid and Cyber Resilience Grants

In addition to the State and Local Cybersecurity Grant Program, two Department of Energy (DoE) initiatives, the Smart Grid Investment Grant Program and Energy Sector Operational Support For Cyber Resilience Program, will provide $3 billion and $50 million, respectively, for electric utilities, including those run by municipalities and in public/private partnership.

These programs aim to modernize the electricity grid and increase resilience to cybersecurity threats. The Cyber Resilience Program is expected to begin accepting applications in the summer of 2022, the Smart Grid Program at the end of 2022.

The IIJA also includes $250 million over five years for a Rural and Municipal Utility Advanced Cybersecurity Grant and Technological Assistance Program, to be overseen by DoE. Its goal is to "improve electric utilities' ability to detect, respond to, and recover from cybersecurity threats."

In addition to the grants currently available, an amendment to the Homeland Security Act of 2002 includes a bill working its way through Congress to establish a National Cyber Resilience Assistance Fund that will improve the federal government's ability to assist in enhancing Critical Infrastructure cybersecurity resilience.

Time-critical: Where to start

Many state and local governments have begun assembling teams to oversee and manage the grant application and implementation process. These priorities ensure a frictionless grant application and implementation process later on.

- **ACTION ITEM: Build your IIJA grant hunting team.**

State and local IT/OT security leaders in Critical Infrastructure sectors – in public/private utilities for example – recognize the opportunity to launch a continuous improvement and monitoring effort to strengthen their organizations' cybersecurity posture.

In this effort, they receive support from expert partners such as the Industrial Cybersecurity Services team at Rockwell Automation, the global leader in industrial automation cybersecurity.

Grant applicants can leverage the company's long-standing expertise in securing Critical Infrastructure systems when assessing their organizations' cybersecurity levels.

Most IT/OT security gaps and improvement opportunities that qualify for federal funding are found in the following areas:

- **Identification of critical assets and risks**
- **Cyber threat intelligence, detection, and real-time monitoring**
- **Planning for incident response and quick recovery after a cyber incident**

Learn about cybersecurity safeguards and where Critical Infrastructure industries typically stand in deploying them, along with best practice security recommendations in this report: Cybersecurity Preparedness in Critical Infrastructure: Avoiding 'The Big Shutdown.'

- **ACTION ITEM: Share preparatory resources in this Action Plan with your team of grant hunters.**

Applying for Federal Cybersecurity funding from DHS / FEMA

Learn about specific cybersecurity grant opportunities

Federal security, intelligence, and law enforcement agencies are urging Critical Infrastructure entities to "immediately strengthen their cyber posture." The Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST) can guide IT/OT practitioners in determining their entity's most pressing cybersecurity improvement needs.

The framework identifies five priorities NIST refers to as "Functions" that constitute core elements of a comprehensive and effective cybersecurity program. The five Functions are:

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

Grant applications submitted under the State and Local Cybersecurity Grant Program are expected to document how their efforts fit with the NIST framework to ensure continuous improvement in identifying exposures, deploying threat prevention, ensuring effective response, and planning recovery activities and outcomes ahead of time. See the NIST Cybersecurity Framework checklist at the end of this document for details.

In addition, observers have pointed out that cybersecurity requirements placed on federal entities per a 2021 executive order, such as the shift to a Zero Trust security strategy and multi-factor authentication, may also inform the stance of the agencies awarding federal cybersecurity preparedness grants.

- **ACTION ITEM: Assess which Function(s) would contribute most to strengthening your entity's overall cybersecurity posture if enabled by grant funding.**

Ask a CISA cybersecurity coordinator

A critical resource during the cybersecurity grant application process is CISA's newly established 50-state network of federal cybersecurity coordinators. States can request assistance from their respective coordinator with completing the steps required by the grant program.

The coordinators are expected to become an essential go-to resource for information on how to obtain federal funds. Entities eligible for a cybersecurity grant can leverage CISA's nationwide knowledge-sharing network through the federal coordinator in their state during the application phase.

When starting the process, make sure to connect with the federal cybersecurity coordinator assigned to your area:

- **ACTION ITEM: Contact your state's CISA cybersecurity coordinator.**

Research federal cybersecurity grants

Researching federal cybersecurity funding for a state, municipality, or public/private partnership is not for the faint of heart and can quickly feel overwhelming. Private vendors may try to capitalize on confusion and offer to sell you information on how to apply for federal preparedness grants. Save your money.

Teams in state, local, tribal, and territorial governments and their external partners can obtain information about federal cybersecurity grant programs under IIJA at no cost from the official and authoritative sources, Grants.gov and FEMA GO.

Let Grants.gov keep you in the loop

Grant.gov, should you not be familiar with it yet, is an essential information resource for federal funding applicants. The service is operated under the governance of the Office of Management and Budget.

Grants.gov serves as the federal government's official website for federal agencies to post grants and for grantees to find funding opportunities and apply to them. The service aggregates information on more than 1,000 grant programs. Find out how it works at its Grants Learning Center.

- **ACTION ITEM: Get up to speed on the Grants Learning Center.**

PLEASE NOTE: Because FEMA manages the State and Local Cybersecurity Grant Program, a registration with FEMA GO, the agency's grants management platform, will later be required to submit your entity's grant application. More information is below, in the section titled "Registration."

Is my organization ready for a federal cybersecurity grant under the IIJA act?

How can you ensure that your entity is eligible for funding under the new program?

For starters, the bill requires state, local, territorial, and tribal governments to coordinate with their counterparts in local communities to develop comprehensive cybersecurity plans based on their needs on the ground.

Multiple eligible entities (think: state and tribal governments, multiple state governments, multiple municipalities) may apply for funding as a group. To do so, they must meet the same requirements as any single entity.

Providing matching funds is a condition for state and local governments to receive a federal cybersecurity grant under the program. For FY 2022, the federal government picks up not more than 90% of any funded effort under the grant program. This cap is lowered each following year by 10%.

To become eligible for a grant, applicants are expected to establish a cybersecurity planning committee that includes industry experts and representatives of local jurisdictions. This committee will oversee the development, approval, and funding priorities of the applying entity's cybersecurity plan.

- **ACTION ITEM: Create a cybersecurity planning committee.**

Grant applicants are also expected to develop a comprehensive Cybersecurity Plan. For this process, seek input and feedback from organizational leadership and the members of your planning committee. Include external experts on Critical Infrastructure cybersecurity. For example, reach out to the consultant team at Rockwell Automation

Rockwell Automation models its cybersecurity approach on the NIST Cybersecurity Framework. We have over 100 years of experience in industrial operations, from controllers to cybersecurity.

We've served Critical Infrastructure organizations globally and can help you navigate what's needed, how to prioritize and support or handle implementation entirely.

- **ACTION ITEM: Start or update your Cybersecurity Plan.**

According to the law, this plan should include "any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems." It will have to be submitted for approval and periodic review by the federal government.

Other essential requirements for grant applicants are to demonstrate, in their Cybersecurity Plan, the adoption of fundamental methodologies, such as the NIST Framework, and assessment and mitigation of, "to the greatest degree possible, cybersecurity risks and [...] threats relating to Critical Infrastructure."

Such a plan will require asset inventories of data, personnel, devices, systems, and facilities, as well as network security assessments, to identify Critical Infrastructure weaknesses, vulnerabilities, and improvement opportunities. If you follow NIST's Framework, you can implement a System Security Plan (SSP) to help identify security requirements. An

SSP can help you develop, document, and periodically update the system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with, or connections to other systems. Experts also recommend involving external cybersecurity service providers specializing in Critical Infrastructure protection, such as Rockwell Automation's cybersecurity team.

- **ACTION ITEM: Identify cybersecurity gaps.**

Grant applicants are also required to lay out in their Cybersecurity Plan how they will "manage, monitor, and track information systems, applications, and user accounts" owned or operated by them, or on their behalf.

Most state and local entities providing critical infrastructure facilities and services don't have the resources to keep track of external and internal cyberthreats and network vulnerabilities 24/7/365. One way out of this dilemma is partnering up with others in the public and private sectors to gain such capabilities.

To that end, Rockwell Automation commands a global network of threat detection and response services. We help empower IT/OT security personnel watching over critical infrastructure at the state level or in local communities to correlate alarms and events and mount adequate responses

- **ACTION ITEM: Partner up and plan how to "manage, monitor, and track."**

In a nutshell, the law requires agencies to show that the "resiliency of information systems, applications, and user accounts" will be improved by the Cybersecurity Plan. This proactive approach includes the capability to recover quickly AFTER a security-related downtime event has impacted critical infrastructure.

Recent incidents have shown that local entities in particular were unable to manage a quick recovery on their own following a ransomware attack, for example. To prevent this situation, more state and local

governments turn to the private sector for data backup and recovery services. Rockwell Automation's Industrial Security Services team has specialized in Critical Infrastructure incident investigations to identify root causes and strengthen resilience.

- **ACTION ITEM: Plan for resiliency.**

Find the Right Federal Cybersecurity Grant(s) Under IIJA

Start by prioritizing your entity's cybersecurity investment needs and developing a project pipeline. Federal funding experts recommend revisiting projects previously considered impossible due to lack of funding or regional coordination. Monitor Grants.gov, FEMA GO, and CISA bulletins for state and local cybersecurity grant announcements, packages, and amendments.

Involve you CIO and CISO early on

- For a successful grant application, it's essential to follow modern cybersecurity best practices, such as the NIST Cybersecurity Framework,– from the start.

Early in the process, make sure you have close collaboration with your CIO and CISO. Consider fundamentals, costs, and the bigger picture before applying for funding. Issues to consider:

- Fundamentals. Focus on understanding who is and what is on your networks, protecting your data, training staff, and planning for resiliency, including cybersecurity incident response plans. Identify and prioritize business-critical systems to protect key operational and data resources more effectively.
- Investments. Plan for investments in transparent, enterprise-wide capabilities that minimize attack surfaces, disrupt malicious connections, and ensure fast recoverability of normal operations.
- Holistic Approach. Explore how to leverage regional or state-wide efforts for maximum effectiveness and efficiency in protecting Critical Infrastructure IT and OT. There will likely be larger efforts you can join.
- **ACTION ITEM: Confirm eligibility for a cybersecurity grant.**

Master the Registration Process

To apply for a grant under the new program, you will need an Employer Identification Number (EIN), which can be obtained on the IRS.gov website – and starting April 4, 2022, a Unique Entity Identifier (UEI), a.k.a. Identity ID.

The UEI replaces the Data Universal Numbering System (DUNS) number from Dun & Bradstreet (D&B) that was required for federal funding applicants in the past. This "SAM UEI" phases out the nine-character Data Universal Numbering System (DUNS) Number from Dun & Bradstreet (D&B) on April 4, 2022. Also required is a current registration with the System for Award Management (SAM).

- **ACTION ITEM: Obtain an EIN and UEI.**
- **ACTION ITEM: Register or update your entity's SAM registration.**

Taking immediate action on these basics is essential. Obtain an EIN and UEI first, if applicable, and then register in SAM or renew your existing SAM registration, because it may take four weeks or more after you submit your SAM registration before your registration is active in SAM.

Register early

PLEASE NOTE: Completing the registration steps ASAP is important because FEMA may not make a federal award until the applicant has complied with all applicable UEI and SAM requirements.

Suppose an applicant's prior SAM registration has expired, expires during application review, or expires any other time before the grant is awarded? In that case, FEMA may determine that the applicant is not qualified and may instead award the grant to another applicant.

Registering and applying for funding under the Cybersecurity Grant program is a multi-step process that requires time to complete. Allow 4-6 weeks to complete the necessary registration steps before submitting the actual grant application.

Applicants are expected to closely read the respective FEMA guidance and instructions. It is advised to prepare the information requested before beginning the registration process. Reviewing and preparing such information beforehand will prevent last-minute scrambling to fill critical gaps.

Create a Login.gov account

To register with SAM or update an existing SAM registration, applicants need a login.gov account.

You can create a login.gov account here:

https://secure.login.gov/sign_up/enter_email

- **ACTION ITEM: Create a Login.gov account.**

Applicants for federal funding only have to create a login.gov account once. Do you have a SAM account already? Then use the same email address for the login.gov account as with SAM.gov so that the two accounts can be linked. More on the login.gov requirements for SAM registration, see https://www.sam.gov/SAM/pages/public/loginFAQ.jsf.

Register on FEMA GO

FEMA Grants Outcomes (GO) is the agency's new platform for submitting, approving, and managing grants, including those under the State and Local Cybersecurity Grant Program.

Add your organization to the system, and follow the instructions to establish the Authorized Organization Representative (AOR). The AOR is the only individual who can sign and submit a grant application to FEMA on behalf of your organization.

This step may require the involvement of your organization's electronic business point of contact (EBiz POC) from the SAM registration. It is recommended to read the step-by-step guide for the FEMA GO registration.

- **ACTION ITEM: Register on FEMA GO.**

...and get your team ready on FEMA GO to save time.

Applying for a federal cybersecurity grant is a team sport. For example, many involve the Finance Department, an outside grant writer or other consulting entities.

For AORs, the menu item "Manage my team" (under "Organizations") is one of the first destinations on FEMA GO. It enables you to add new members from within and outside the organization and assign various permission levels, based on their role in the grant application process. The "Grant Writer" role, for example, allows the user to view and edit all information for an application or sub-application.

- **ACTION ITEM: Set up your grant application team on FEMA GO.**

Apply for a federal cybersecurity grant under IIJA

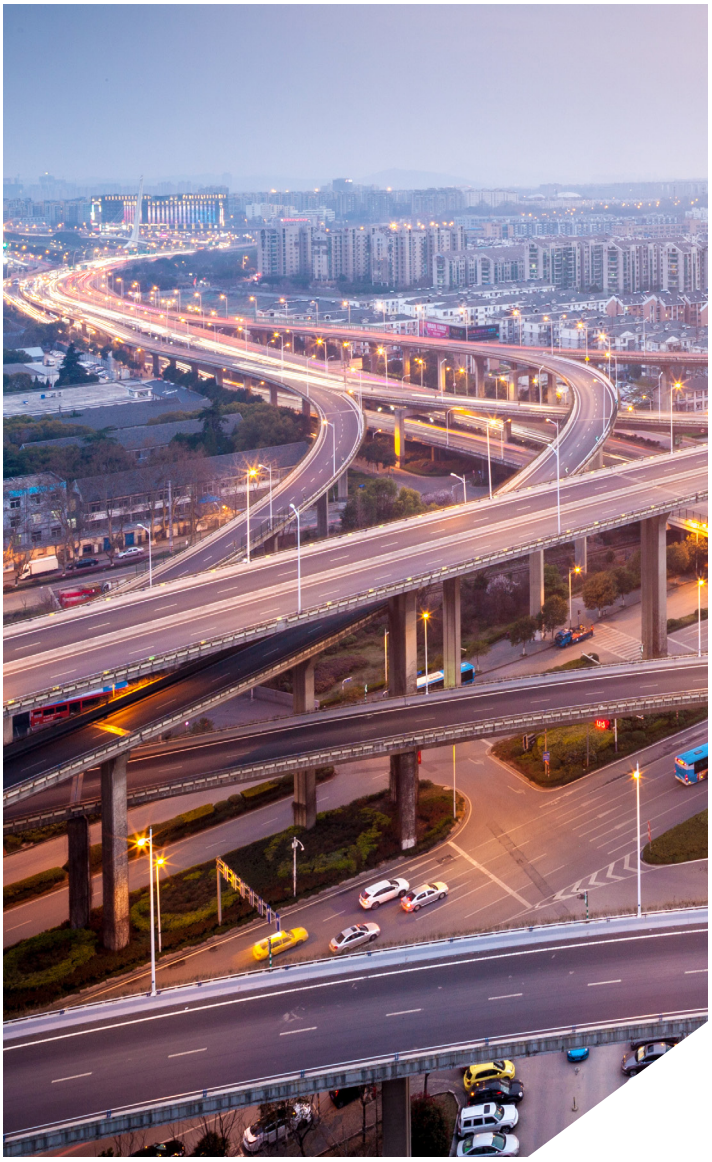
After lining everything up, complete and submit your completed application on FEMA GO.

- **ACTION ITEM: Submit your application on FEMA GO.**
- **ACTION ITEM: Track the application status.**

If you have checked off all of the items on this Action Plan, then congratulations. As Alexander Graham Bell said, "Preparation is the key to success."

Once you meet the requirements and have submitted all required forms early on FEMA GO, then get ready to hear back from the federal government - hopefully with the news that your organization will receive grant funding. Taking these steps will strengthen your cybersecurity protections and help defend customers from downtime and damage caused by cyber incidents.

- **ACTION ITEM: Set up a Rockwell Automation consultation today.**



Rockwell Automation: Securing What the World Relies On

Rockwell Automation provides a range of industrial security solutions and services to help you manage threats and boost the resiliency of your OT and IT ecosystem. We can help you build a robust and secure network infrastructure while helping to defend against threats and rapidly respond to incidents.

In addition to deep expertise and knowledge of the latest best practices, we bring production operations wisdom from more than 100 years in industrial automation. Our worldwide locations enable customers to apply cybersecurity protections on a global scale across multiple sites with logistics as finely tuned as you'd expect from the industry leader in industrial automation.

Resources to help you get started

- Take the Rockwell Automation Cybersecurity Preparedness Assessment and receive a custom report, benchmarked against original survey respondents. See how your organization compares by industry, company size and region.
- Talk to a Rockwell Automation expert and learn how we can help you with the right OT cybersecurity program to best protect your industrial operations.

Please Contact Us to learn more about how we can help.

ACTION ITEMS

- ☐ Build your IIJA grant hunting team.
- ☐ Share preparatory resources in this Action Plan with your team of grant hunters.
- ☐ Assess which Function(s) would contribute most to strengthening your entity's overall cybersecurity posture if enabled by grant funding.
- ☐ Contact your state's CISA cybersecurity coordinator.
- ☐ Get up to speed on the Grants Learning Center.
- ☐ Create a cybersecurity planning committee.
- ☐ Start or update your Cybersecurity Plan.
- ☐ Identify cybersecurity gaps.
- ☐ Partner up and plan how to "manage, monitor, and track."
- ☐ Plan for resiliency.
- ☐ Confirm eligibility for a cybersecurity grant.
- ☐ Obtain an EIN and UEI.
- ☐ Register or update your entity's SAM registration.
- ☐ Create a Login.gov account.
- ☐ Register on FEMA GO.
- ☐ Set up your grant application team on FEMA GO.
- ☐ Submit your application on FEMA GO.
- ☐ Track the application status.
- ☐ Set up a Rockwell Automation consultation today.

Appendix

Cybersecurity Planning Checklist

Use this checklist to evaluate gaps and goals around strengthening cybersecurity.
For a professional assessment and planning support, contact Rockwell Automation.

Rockwell Automation's Cybersecurity Framework
A NIST-based Approach for 360⁰ Protection

☐	**Identify**	Asset Management: Software Inventory
☐	**Identify**	Asset Management: Data Flow
☐	**Identify**	Asset Management: System Criticality
☐	**Identify**	Supply Chain Risk Management
☐	**Identify**	Identity Management: Credentials
☐	**Protect**	Identity Management: Logical Access
☐	**Protect**	Identity Management: Authentication
☐	**Protect**	Identity Management: Network Perimeter
☐	**Protect**	Identity Management: Remote Access
☐	**Protect**	Identity Management: Physical Access
☐	**Protect**	Security Awareness: Roles & Responsibilities
☐	**Protect**	Security Awareness: Training
☐	**Protect**	Protective Technology: Removable Media

☐	**Protect**	Protective Technology: SIEM
☐	**Protect**	Protective Technology: Endpoint Security
☐	**Protect**	Information and Data Protection: System Hardening
☐	**Protect**	Information and Data Protection: Backups
☐	**Protect**	Information and Data Protection: Vulnerability Management
☐	**Detect**	Anomalies & Events: Event Baseline
☐	**Detect**	Anomalies & Events: Event Analysis
☐	**Detect**	Anomalies & Events: Impact Assessment
☐	**Detect**	Security Continuous Monitoring: Logical Security
☐	**Detect**	Security Continuous Monitoring: Physical Security
☐	**Detect**	Security Continuous Monitoring: Malware Protection
☐	**Detect**	Security Continuous Monitoring: Vulnerability Scanning
☐	**Detect**	Detection Process: SOC Organization
☐	**Detect**	Detection Process: Communication Flow
☐	**Respond**	Communications: Process Flow
☐	**Respond**	Communications: Communication Flow
☐	**Respond**	Analysis: Investigation
☐	**Respond**	Mitigation: Containment
☐	**Recover**	Recovery Planning
☐	**Recover**	Improvements
☐	**Recover**	Communications

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-SP017A-EN-P-June 2022