

must be prepared to respond to disruptive

cyber activity." — CISA Shields Up warning

NEW CYBERSECURITY New connections require new protections

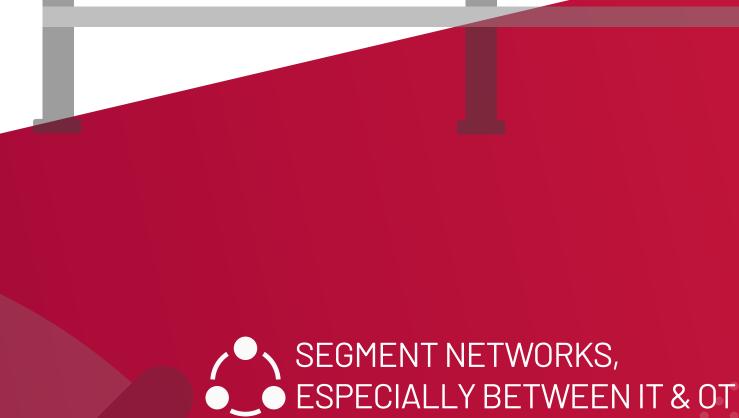
Prioritize action with the Power of 5.

for Industrial Control Systems (ICS).



THREATS TO CRITICAL

INFRASTRUCTURE



INSIDER THREATS





AUDIT NETWORK
INVENTORY FREQUENTLY





RESPOND

RECOVER

PROTECT

IDENTIFY

DETECT Gain real-time visibility into how, when, and where others are accessing or manipulating assets. 24/7 threat monitoring | Malware detection | Vulnerability scanning | Impact assessment |

IDENTIFY

PROTECT

RESPOND Implement an incident response plan to stop breaches from expanding infection and damage. Incident response | Containment | Mitigation | Communication planning | Tabletop exercises

Put a plan in place to quickly regain normal operations after an

incident, shortening the recovery cycle and minimizing impact.

Backup planning | Restoration | Investigation and analysis

security controls. Network segmentation | Multi-factor

Daily asset inventories | Alerts and advisories

authentication | IDMZ deployment | Secure ICS Protocols | Firewalls

| Patching | Zero Trust policies | Employee awareness training



| Resilience planning

RECOVER

REGIONAL / INTERNATIONAL CYBERSECURITY FRAMEWORKS

Australia

European Union



United Kingdom The National Cybersecurity Center (NCSC) issued its OT Security Design Principles in 2020.

The Critical Infrastructure Centre (CIC)

Compliance Strategy offers recommendations

for Critical Infrastructure owners/operators.

The Network and Information Security (NIS)

Directive (EU 2016/1148) is the EU's first

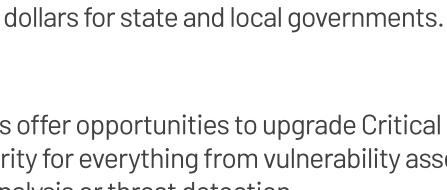
EU-wide cybersecurity legislation.

FACTS ABOUT \$1B+ IN U.S.

CYBERSECURITY GRANTS

To be eligible for a grant, state or local agencies must submit a cybersecurity plan

to the Department of Homeland Security (DHS), detailing technical capabilities



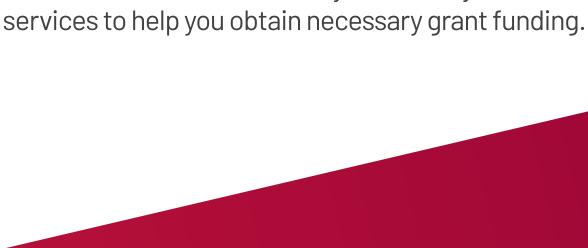
and protocols for detecting and responding to cyberattacks.

New grants offer opportunities to upgrade Critical Infrastructure cybersecurity for everything from vulnerability assessments, to malware analysis or threat detection.

It authorizes \$1.2 trillion in funding and set aside billions of

The bipartisan Infrastructure Investment and Jobs

Act (IIJA) was signed into law in November 2021.



Rockwell Automation offers cybersecurity assessment and planning

NEXT STEPS TO TAKE

Securing what the world relies on.



Rockwell Automation:





Publication GMSN-SP019A-EN-P-September 2022 | Copyright © 2022 Rockwell Automation, Inc. All Rights Reserved. Printed in USA.

Learn How a Canadian Water Utility Company
Improved Cybersecurity and Operational Resilience



