SMALL SYSTEMS AREN'T SMALL POTATOES

WHY RURAL WATER UTILITIES NEED CYBERSECURITY AND WHAT TO DO ABOUT IT, PART 2

RISK MANAGEMENT

PRESENTERS

STEVE MUSTARD
Licensed Professional Engineer and industrial cybersecurity SME. MCGA Board Member and past president of the International Society of Automation (ISA).

JENNIFER LYN WALKER
Director of Infrastructure Cyber Defense, WaterISAC. Cybersecurity professional with over 20 years' experience supporting SLTT and other critical infrastructure sectors.

ANDREW HILDICK-SMITH
Advisor at WaterISAC. Licensed Professional Engineer with 30 years at a water and wastewater utility with responsibilities for SCADA security and emergency planning.

Mission Critical Global Alliance

NRWA

WATER ISAC

PATCHING

JENNIFER LYN WALKER, DIRECTOR OF INFRASTRUCTURE CYBER DEFENSE AT WATERISAC

PATCHING

NIST Special Publication (SP) 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology

The act of applying a change to installed software – such as firmware, operating systems, or applications – that corrects security or functionality problems or adds new capabilities. Enterprise patch management is the process of **identifying, prioritizing,** acquiring, installing, and verifying the installation of patches, updates, and upgrades throughout an organization.

BASICS OF PATCHING

Key facet of vulnerability management

Dependent on asset management (knowing your network)

IT vs. OT

PATCHING MISCONCEPTIONS

Everything needs to be patched - *true/false?*

- False. *But everything does need to be addressed.*

Bad guys don't exploit old vulnerabilities - *true/false?*

- False. *Threat actors DO exploit old vulnerabilities on systems left unpatched.*

PATCHING IN OT ENVIRONMENTS

Isn't always preferable, practical, or even possible

- Legacy systems
- Incompatibilities
- Void maintenance contracts
- Excessive downtime
- *ICS-Patch (defer, scheduled, ASAP)*

Importance of compensating controls

- Network segmentation
- Isolation
- Secure coding practices (e.g., *Top 20 Secure PLC Coding Practices)*

PATCH/VULNERABILITY PRIORITIZATION FOR SMALL SYSTEMS

- CISA's Known Exploited Vulnerabilities Catalog
- CISA's ICS-CERT Advisories
- ICS-Patch (Dale Peterson)

THE 4 W'S OF A VULNERABILITY DISCLOSURE
(TO HELP WITH PATCH PRIORITIZATION)

- Who: Vendor/Project/Product
- When: CVE/ICSA number
- What: Vulnerability Name
- Why: Short Description

Mission Critical Global Alliance

NRWA

WATER ISAC

KNOWN EXPLOITED VULNERABILITIES CATALOG (*SEARCH BY DATE ADDED*)

Cheat sheet

Date Added to Catalog

1. Who: Vendor/Project; Product
2. When: CVE (age of vulnerability)
3. What: Vulnerability Name
4. Why: Short Description

Show 10 entries

Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2022-23176	WatchGuard	Firebox and XTM	WatchGuard Firebox and XTM Privilege Escalation Vulnerability	2022-04-11	WatchGuard Firebox and XTM appliances allow a remote attacker with unprivileged credentials to access the system with a privileged management session via exposed management access.	Apply updates per vendor instructions.	2022-05-02	
CVE-2021-42287	Microsoft	Active Directory	Microsoft Active Directory Domain Services Privilege Escalation Vulnerability	2022-04-11	Microsoft Active Directory Domain Services contains an unspecified vulnerability which allows for privilege escalation.	Apply updates per vendor instructions.	2022-05-02	
CVE-2021-42278	Microsoft	A Directory	Microsoft Active Directory Domain Services Privilege Escalation Vulnerability	2022-04-11	Microsoft Active Directory Domain Services contains an unspecified vulnerability which allows for privilege escalation.	Apply updates per vendor instructions.	2022-05-02	
CVE-2021-39793	Google	Pixel	Google Pixel Out-of-Bounds Write Vulnerability	2022-04-11	Google Pixel contains a possible out-of-bounds write due to a logic error in the code that could lead to local escalation of privilege.	Apply updates per vendor instructions.	2022-05-02	
			Checkbox Survey		Deserialization of Untrusted Data	Versions 6 and earlier for this product are end-of-		

Mission Critical Global Alliance

NRWA

WATER ISAC

KNOWN EXPLOITED VULNERABILITIES CATALOG (*SEARCH BY VENDOR*)

Show 10 entries

Search: Fortinet

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2018-13382	Fortinet	FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Improper Authorization	2022-01-10	An Improper Authorization vulnerability in Fortinet FortiOS and FortiProxy under SSL VPN web portal allows an unauthenticated attacker to modify the password.	Apply updates per vendor instructions.	2022-07-10	
CVE-2018-13383	Fortinet	Fortinet and FortiProxy	Fortinet FortiOS and FortiProxy Out-of-bounds Write	2022-01-10	A heap buffer overflow in Fortinet FortiOS and FortiProxy may cause the SSL VPN web service termination for logged in users.	Apply updates per vendor instructions.	2022-07-10	
CVE-2021-44168	Fortinet	FortiOS	Fortinet FortiOS Arbitrary File Download	2021-12-10	Fortinet FortiOS "execute restore src-vis" downloads code without integrity checking, allowing an attacker to arbitrarily download files.	Apply updates per vendor instructions.	2021-12-24	
CVE-2019-5591	Fortinet	FortiOS	Fortinet FortiOS Default Configuration Vulnerability	2021-11-03	A Default Configuration vulnerability in FortiOS may allow an unauthenticated attacker on the same subnet to intercept sensitive information by impersonating the LDAP server.	Apply updates per vendor instructions.	2022-05-03	

Cheat sheet

Date Added to Catalog

1. When: CVE (age of vulnerability)
2. What: Vulnerability Name
3. Why: Short Description

Mission Critical Global Alliance

NRWA

WATER ISAC

ICS-CERT ADVISORIES FOR INDUSTRIAL CONTROL SYSTEMS

Industrial Control Systems > ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.
[change view]: ICS-CERT Advisories by Vendor | ICS-CERT Advisories by Vendor - sorted by Last Revised Date

Items per page 25 ▼ Apply

ICSA-22-097-01 : Pepperl+Fuchs WirelessHART-Gate
ICSA-22-097-02 : ABB SPIET800 and PNI800
ICSA-21-278-01 : Mitsubishi Electric GOT and Tensio
ICSMA-22-095-01 : LifePoint Informatics Patient Por
ICSA-22-095-01 : Rockwell Automation ISaGRAF
ICSA-22-095-02 : Johnson Controls Metasys
ICSMA-21-187-01 : Philips Vue PACS (Update B)
ICSA-22-090-01 : Schneider Electric SCADAPack Wor
ICSA-22-090-02 : Hitachi Energy e-mesh EMS
ICSA-22-090-03 : Fuji Electric Alpha5
ICSA-22-090-04 : Mitsubishi Electric FA Products
ICSA-22-090-05 : Rockwell Automation Logix Contro
ICSA-22-090-06 : General Electric Renewable Energy
ICSA-22-090-07 : Rockwell Automation Studio 5000
ICSA-22-067-01 : PTC Axeda agent and Axeda Deskto
ICSA-20-303-01 : Mitsubishi Electric MELSEC iQ-R, Q

ICS Advisory (ICSA-22-090-05)

Rockwell Automation Logix Controllers

Original release date: March 31, 2022

Print Tweet Send Share

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The I regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1. EXECUTIVE SUMMARY

- CVSS v3 10.0
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Rockwell Automation
- **Equipment:** Logix Controllers
- **Vulnerability:** Inclusion of Functionality from Untrusted Control Sphere

2. RISK EVALUATION

Successful exploitation of this vulnerability may allow an attacker to modify user programs. A user could then unknowingly download those modified elements containing malicious code.

Industrial Control Systems > ICS-CERT Advisories by Vendor

[change view]: ICS-CERT Advisories in Release Sequence | ICS-CERT Advisories by Vendor - sorted by Last Revised Date

Vendor starts with Rockwell Apply

Rockwell Automation

ICSA-22-095-01 : Rockwell Automation ISaGRAF
ICSA-22-090-05 : Rockwell Automation Logix Controllers
ICSA-22-090-07 : Rockwell Automation Studio 5000 Logix Designer
ICSA-22-088-01 : Rockwell Automation ISaGRAF
ICSA-21-189-01 : Rockwell Automation MicroLogix 1100
ICSA-20-280-01 : Rockwell Automation ISaGRAF5 Runtime (Update A)
ICSA-21-161-01 : Rockwell Automation FactoryTalk Services Platform
ICSA-21-145-02 : Rockwell Automation Micro800 and MicroLogix 1400
ICSA-21-133-01 : Rockwell Automation Connected Components Workbench
ICSA-21-110-02 : Rockwell Automation Stratix Switches

Mission Critical Global Alliance

NRWA

WATER ISAC

PATCHING – POLL QUESTION

Patching is the **only** way to protect/secure vulnerable computers, servers, software, and other digital devices and components from being compromised.

- ❑ True
- ❑ False

BACKUPS – YOUR INSURANCE

ANDREW HILDICK-SMITH, ADVISOR AT WATERISAC

BACKUPS – BASICS

Your Insurance – protection from random failures, physical disasters and ransomware

What to backup:

- **Data** – utility's files and user desktop files
- **Configuration information** – how software and hardware is deployed
- **Software** – executables and licenses for OS and software restoration
- **Gold Image** – baseline image of desktops, servers or virtual servers for quick restoration

BACKUPS – CHOICES

Frequency – What would be a reasonable backup frequency to avoid an unacceptable loss? Establish a policy and follow it.

Retention – How long to keep backups and how many versions back. If an adversary was in your system for a month, would you want to use the last backup?

Backup Approaches – Full, Differential, Incremental and variations …

BACKUPS – TECHNOLOGIES

Technologies

- Network Attached Storage (NAS)
- Hard Disk Drives (HDD)
- Solid State Drive (SSD)
- Optical Drives - Blue Ray Discs, etc.
- Tape
- Cloud based

NAS,
Wikipedia,
Bin im Garten

HDD, SDD, Thumb Drive, Optical Drive

Mission Critical Global Alliance

NRWA

WATER ISAC

BACKUPS – TECHNOLOGIES CONSIDERATIONS

Speed – backup and restoration speed

Capacity – storage capacity

Longevity – storage media failure rate

Obsolescence – technology lifespan

Services – off-site storage services

Internet – what if your internet service is down and you are dependent on the cloud?

Technology goes obsolete
Wikipedia

BACKUPS – PRECAUTIONS

Encrypt – protect your data

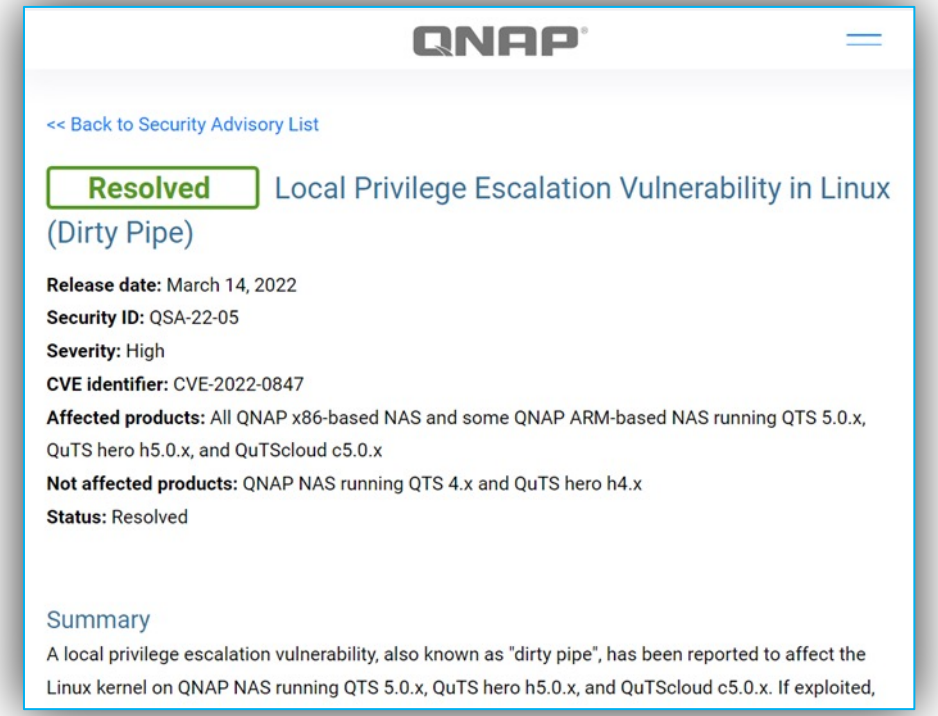
Keep Offline – protect from ransomware

Two Technologies – reliability through diversity

Store in Two Locations – disaster protection

Device Vulnerability – NAS vulnerabilities

Test Recovery – make sure you can recover and calculate the time it would take to recover



Vulnerable NAS product

Mission Critical Global Alliance

NRWA

WATER ISAC

BACKUPS – SCADA / OT / ICS ASPECTS

Regulatory Data – to ensure compliance

PLCs and HMI – software and program code

Configurations – software, PCs, PLCs / controllers, routers, switches, etc.

Hardware – backup (spare) hardware

PLC parts
Wikipedia, Elmschrat Coaching-Blog

Mission Critical Global Alliance

NRWA

WATER ISAC

BACKUPS – TAKE AWAYS

- Good backups are essential
- Store offline and off-site
- Test your backups to make sure you can restore from them
- Create and follow a backup policy and procedure
- Keep backup (spare) parts, especially for your SCADA system

POLL QUESTION

- When you make backups of your data, programs and system configuration it is important to?
  - Store copies at different physical locations
  - Store copies on different media
  - Keep at least one copy isolated from network connections (offline)
  - Test your ability to restore from your backups
  - All of the above

INCIDENT RESPONSE

STEVE MUSTARD, MCGA BOARD MEMBER AND FORMER ISA PRESIDENT

INCIDENTS

- Man-made disasters, such as earthquakes, floods or hurricanes
- Terrorist attacks
- Process incidents, such as loss of containment, fire or explosion
- Loss of critical power or other resources, such as water supply
- Cybersecurity incidents, such as deliberate attacks or accidental events

TYPES OF PLANS

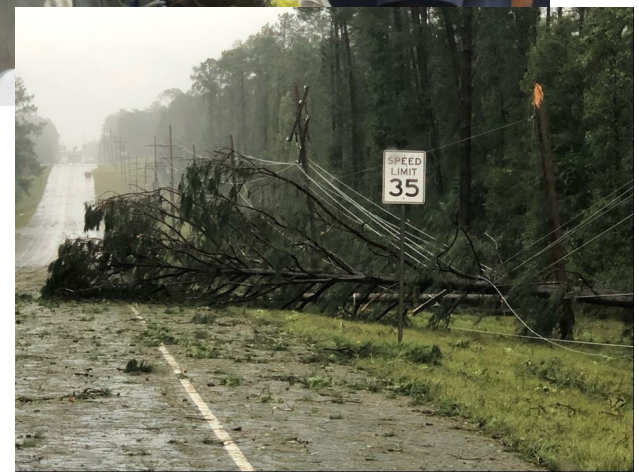
- **Business impact analysis**
  - Identify the essential functions and resources in the organization
  - Consider threats and vulnerabilities related to these functions
- **Business continuity planning**
- Continuity of operations plan, or COOP
  - Ensure that critical business functions can continue in the event of a serious incident where Disaster Recovery (DR) plans will require long term or major activities.
- **Incident response**
  - Identify the activities required during or immediately after an emergency.
- **Disaster recovery**
  - Takes over from an IR plan and is focused on restoration activities, such as re-establishing communications networks, IT equipment or process operations.

KEY ELEMENTS OF EMERGENCY RESPONSE

- **Mitigation** - this includes activities that reduce the likelihood of an emergency occurring or reduce the impact of the effects of the emergency if it does occur. Mitigations could include purchasing insurance or implementing certain cybersecurity controls
- **Preparedness** – this includes the plans and preparations that must be performed before an emergency occurs. Maintaining offsite system backups is an example of a preparedness activity
- **Response** – this includes the actions that are performed in the event of an emergency. A typical response action is restoring a system from offsite backups
- **Recovery** – This includes the activities that are performed after the immediate danger of the emergency is over. This may include replacement of non-essential items that were damaged in the incident

COMMUNICATIONS

- Stakeholders:
  - Employees
  - Directors
  - Shareholders
  - Customers
  - Suppliers
- Governmental and regulatory bodies
  - Local elected and appointed officials
  - Local departments and agencies
  - State agencies
  - Regional organizations or groups
  - Federal agencies



Mission Critical Global Alliance

NRWA

WATER ISAC

RTO AND RPO

- The recovery time objective (RTO) - The duration of time and a service level within which a process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in service.
- The recovery point objective (RPO) - The acceptable amount of data loss measured in time (e.g., data must be restored from within two hours of a disaster for the loss of that data to be acceptable).

Process	Sub-system	RTO	RPO
Process A	Sub-system 1	8h	72h
	Sub-system 2	36h	72h
	Sub-system 3	36h	72h
Process B	Sub-system 1	2h	8h
	Sub-system 2	4h	8h
	Sub-system 3	8h	8h
	Sub-system 4	8h	8h

BACKUP STRATEGY

- Use RTO and RPO to determine backup frequency
- Maintaining multiple rotating sets of backups can help in the event of a problem with one backup
- Keep backups offsite – the cloud is better than an external drive in your office
- Establish SOPs for backups, and restoration
  - Backup steps: Scan machine for malware, run backup, scan backup and machine for malware
  - Testing restoration: Scan machine and backup for malware, run restoration, scan machine for malware
- Test restoration
- Have an incident response plan that includes the possibility that restoration may introduce malware
  - Worst case you may need original operating system and application software installation files

INCIDENT REPORTING

- It is essential that all security incidents are reported
- WaterISAC urges utilities and others sector stakeholders to report incidents and suspicious activity to our analysts. Reporting incidents and suspicious activity helps strengthen sector resilience, because it allows WaterISAC to identify threats and vulnerabilities and to warn other members and partners.
- The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) requires owners and operators of critical infrastructure to report cyber incidents to CISA within 72 hours and ransom payments within 24 hours
- Reporting an incident may help protect another facility/asset and provide information to improve security
- Like safety, it is just as important to review "near misses"
- **If in doubt, report it**

Mission Critical Global Alliance

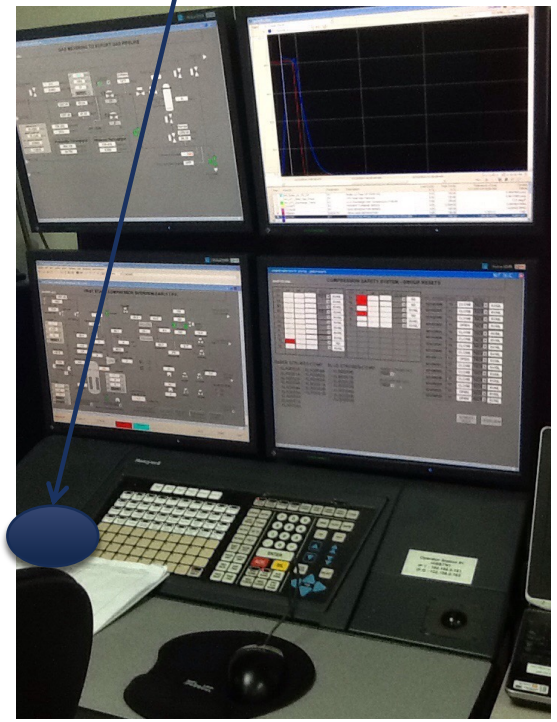
NRWA

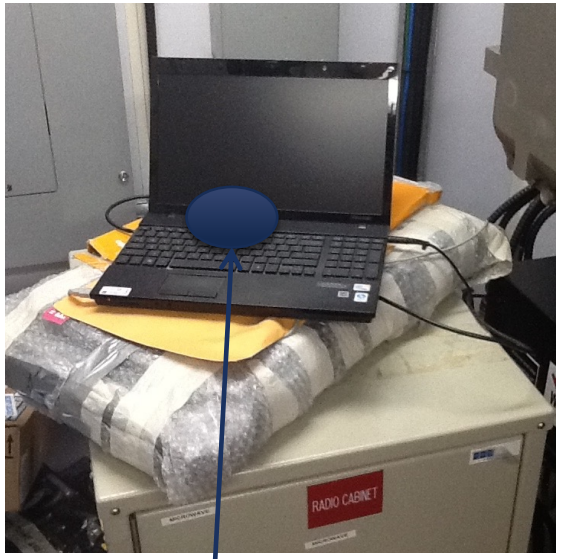
WATER ISAC

NEAR-MISSES

PLC programming laptop for gas turbine controller has no password protection or anti-virus software installed

Username and password for operator workstation labeled on workstation





Key interface between control systems inadequately secured

Mission Critical Global Alliance

NRWA

WATER ISAC

POLL QUESTION

- What is the name of the recovery objective that defines an acceptable amount of data loss in the event of a disaster?

1. Recovery time objective (RTO)
2. Recovery point objective (RPO)
3. Response time objective (RTO)
4. Response point objective (RPO)

RESOURCES

CYBERSECURITY RESOURCES - PATCHING

- NIST Special Publication (SP) 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
- NIST SP 1800-31, Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways
- ICS-Patch (Dale Peterson)
- Secure PLC Coding Practices: Top 20 List (securePLC)
- CISA's Known Exploited Vulnerabilities Catalog
- CISA's ICS-CERT Advisories
- Best Practices in OT Vulnerability Management: OT Vulnerability Prioritization is Different (Dragos)
- 6 Steps for Effective Patch Management (Verve Industrial)
- Weathering the Deluge of OT Vulnerabilities: A Pragmatic Approach (Verve Industrial)

CYBERSECURITY RESOURCES – BACKUPS

- Backup and recovery approaches on AWS. https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/welcome.html *(example of cloud backup services)*
- Data Backup Options. US-CERT. https://www.cisa.gov/uscert/sites/default/files/publications/data_backup_options.pdf
- Great Smoky Mountains National Park Standard Operating Procedure: Backup, Storage & Recovery. https://irma.nps.gov/DataStore/DownloadFile/552537 *(example of a backup policy)*
- Protecting Data From Ransomware and Other Data Loss Events. NIST & NCCoE. https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf

CYBERSECURITY RESOURCES - GENERAL

- CISA Incident Reporting System, https://us-cert.cisa.gov/forms/report
- WaterISAC reporting, https://www.waterisac.org/report-incidents-and-suspicious-activity-waterisac-and-authorities
- CISA Resources, https://www.cisa.gov/uscert/resources
- NRWA Cybersecurity web page, https://nrwa.org/issues/cybersecurity/
- MS-ISAC membership (state, local, tribal, territorial), https://www.cisecurity.org/ms-isac/
- WaterISAC membership (free trial membership available), https://www.waterisac.org/membership

CYBERSECURITY RESOURCES - GENERAL, cont.

- DHS CISA Stop Ransomware Site, https://www.cisa.gov/stopransomware
- Joint Cybersecurity Advisory "Ongoing Cyber Threats to U.S. Water and Wastewater Systems" (CISA, FBI, EPA, NSA), https://www.cisa.gov/uscert/ncas/alerts/aa21-287a
- SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final
- Quick start guide to ISA/IEC62443 https://gca.isa.org/isagca-quick-start-guide-62443-standards
- Mission Critical Operations Primer, https://www.isa.org/products/mission-critical-operations-primer

QUESTIONS

STEVE MUSTARD

smustard@mcgalliance.org

JENNIFER WALKER

walker@waterisac.org

ANDREW HILDICK-SMITH

hildick-smith@waterisac.org

THANK YOU