SMALL SYSTEMS AREN'T SMALL POTATOES

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

ACCOUNT PROTECTION

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

PASSWORDS & ACCOUNT MANAGEMENT

ANDREW HILDICK-SMITH, ADVISOR AT WATERISAC

PASSWORDS, UGH

Endless advice – length, complexity, passphrases, change frequency, etc.

Hashes – how computers use passwords

(one-way cryptographic formula that your computer applies to your password)

Your Password		Computer's Password Hash (Windows NT)
Spring2021	→	57912AFE60E9274C35672BF526BAED61
Spring2022	→	1E09A46BFFE68A4CB738B0381AF1DC96

PASSWORDS, SOME ADVERSARY TACTICS

Asking – adversary asks you for your password through phishing or other trickery

Cracking – takes a stolen password hash and cracks it with a software tool like hashcat

Credential Stuffing – takes your password exposed in a breach and tries it on another one of your accounts

Keystroke Logger – malware that captures your keystrokes, including your password

Spraying – attacking many accounts with the same few common passwords

PASSWORD STRENGTH AGAINST ATTACKS

✓ - secure password X - compromised

Passwords Techniques	**Spring2022!** *(common)*	**uT5cL7#y** *(short)*	**noodle*smog2-shriMp** *(18++ char. pass phrase)*	**2+YS8eT:0mVjg,71Cd** *(18+ char. random)*	*plus* **MFA**
Asking phishing, pop ups, reset	X	X	X	X	(✓)
Cracking harvested hash	X	X	(✓)	✓	✓
Credential Stuffing *(reused pw)* *	X	X	X	X	✓
Credential Stuffing *(unique pw)*	✓	✓	✓	✓	✓
Guessing	X	✓	✓	✓	✓
Keystroke Logger	X	X	X	X	(✓)
Look-up rainbow table	X	X	✓	✓	✓
Pass the Hash	X	X	X	X	✓
Spraying	X	✓	✓	✓	✓

Mission Critical Global Alliance

NRWA

WATER ISAC

PASSWORD CRACKING SPEED WITH GPU – BRUTE FORCE

Spring2022! - less than a *second using common password database*

uT5cL7#y - *16 hours (0.65 days)*

2+YS8eT:0mVjg,71Cd - *110,000,000,000,000,000 years*

GeForce GPU by NVIDIA

- 118 billion hashes per second
- $2,000 - $3,000

Example calculation:

- Character set size for numbers, letters and specials: 95
- Number of characters in the password: 8
- Hashes per second: 118×10^9
- **Calculation** $95^8 / (118 \times 10^9 \times 86{,}400\ ^{sec}/_{day}) = 0.65$ days to crack

SAMPLE PASSWORDS AND CHANGE FREQUENCY

Password Examples/Types:

Spring2022! - too common

uT5cL7#y - too short (8 chr.)

noodle*smog2-shrimp - perhaps a keeper (longer is better, 4+ words)

2+YS8eT:0mVjg,71Cd - tough to remember (longer is better)

Change Frequency: NIST and NSA do not recommend changing passwords unless they have been compromised.

GENERATING PASSWORDS

RandPassGenerator (NSA Java application on GitHub)

- Random passwords and passphrases
- High degree of randomness
- 18-character password meets minimum NSA data-at-rest requirement for SECRET classification (meets a minimum entropy requirement of 112 bits)

Password Managers

- Random passwords and passphrases

Password Managers

Options

- Pick a well-known password manager that has been around for a few years
- Consider whether you want it to sync to your other devices
- Password storage by browsers not recommended

Risks - Cloud hack attempts (credential stuffing against master passwords)

Alternatives - Paper version

ACCOUNT MANAGMENT

Remove Accounts when staff and consultants leave

Only use Admin passwords when required

Change default passwords on devices

Technical Stuff (for IT staff)

- Windows Defender Credential Guard
- Local Administrator Password Solution (LAPS)
- Etc.

PASSWORD ADVICE, DOUBLE UGH

Never reuse the same password

- Do not use simple variations either *(rX5gJoe2, rX5gJoe3, rX5gJoe4, etc.)*
- If you have reused passwords, go back and change them over time

Password length of at least 18 characters for important accounts

Consider using a password manager *(1password, dashlane, lastpass, etc.)*

Remove accounts when staff and consultants leave

Only use Admin passwords when required

QUESTION

- What is the most important characteristic in making a strong password?
  - Length
  - Using special characters
  - Complexity
  - Using Unicode characters
  - Regularly changing it

MULTI-FACTOR AUTHENTICATION

JENNIFER LYN WALKER, DIRECTOR OF INFRASTRUCTURE CYBER DEFENSE AT WATERISAC

MULTIFACTOR AUTHENTICATION (MFA)

National Institute for Standards and Technology (NIST)

An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

BASICS OF MFA

Something you know (password/PIN)

Something you have (ID badge, cryptographic identification device/token)

Something you are (biometric)

COMMON METHODS OF MFA

- SMS text-based or email
- Authentication app
- FIDO key
- Biometrics

IMPORTANCE OF MFA

Helps utilities protect against users' bad passwords

Adds an additional layer of protection against cracked, phished, or stolen passwords

MFA ISN'T PERFECT

MFA bypass techniques

- Sim-swap
- Session reuse
- Leveraging weak default configuration protocols
- Overlay login forms
- Social engineering

IMPLEMENTING MFA FOR SMALL SYSTEMS

Critical Infrastructure Defense Project

Set expectations through planning and training

Start with administrators and privileged users

Prioritize most critical applications/access

QUESTION

What is the LEAST secure method of multifactor authentication?

a. FIDO key

b. Authenticator app

c. SMS/text-based or email

d. Biometrics

MFA TAKEAWAYS

Reduces the risk from successful phishing attacks due to credential harvesting or stolen credentials

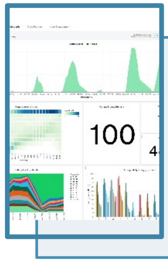
Reduces the risk posed from poor password practices

Two or more factors are better than one

REMOTE ACCESS

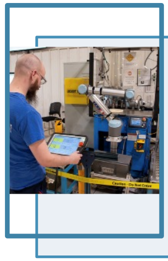
STEVE MUSTARD, MCGA BOARD MEMBER AND FORMER ISA PRESIDENT

WHAT DO WE MEAN BY REMOTE ACCESS?



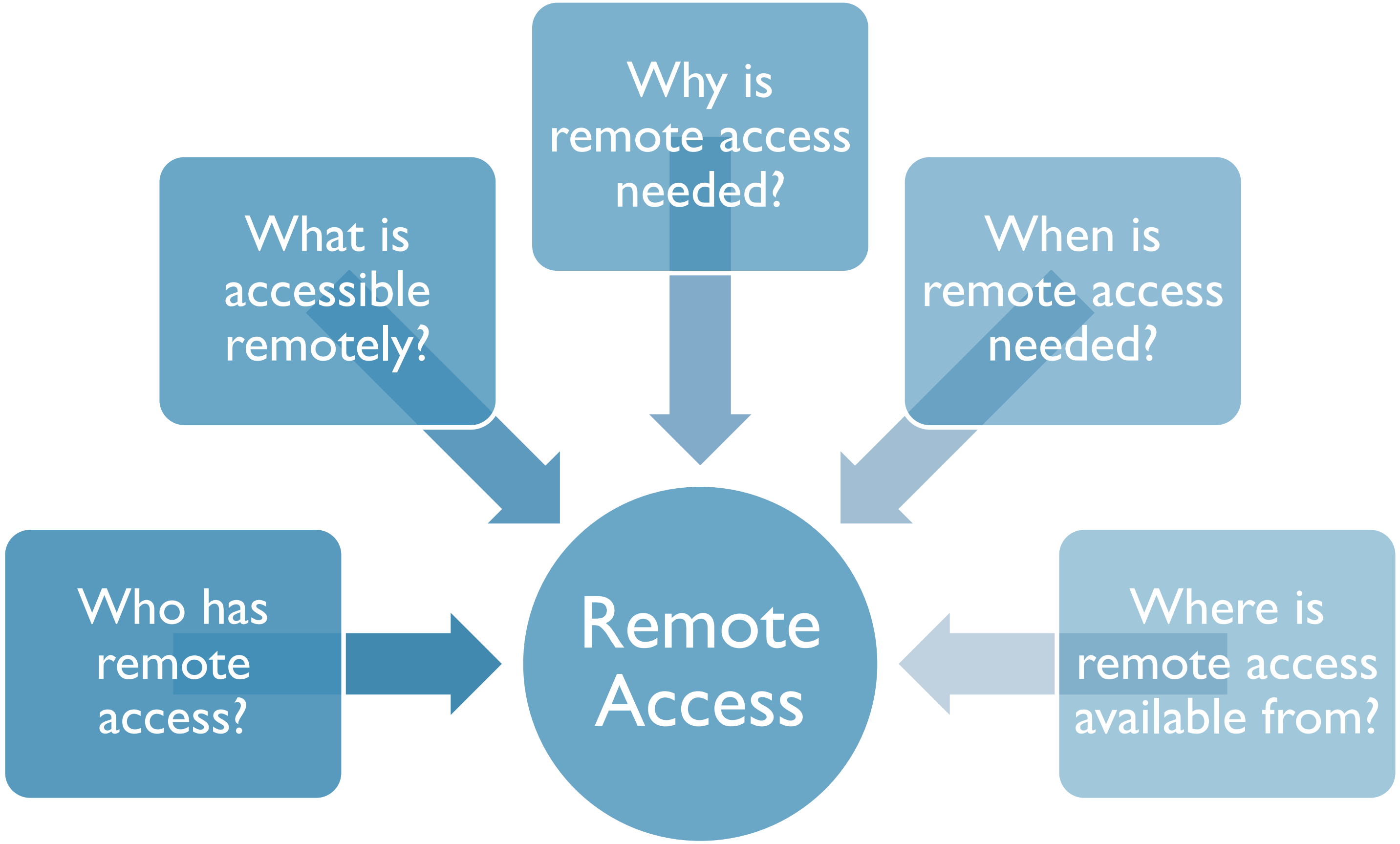
Read only access to view data

Ability to download/stream data from system



Replicating in-person access to system

REMOTE ACCESS QUESTIONS



Why is remote access needed?

What is accessible remotely?

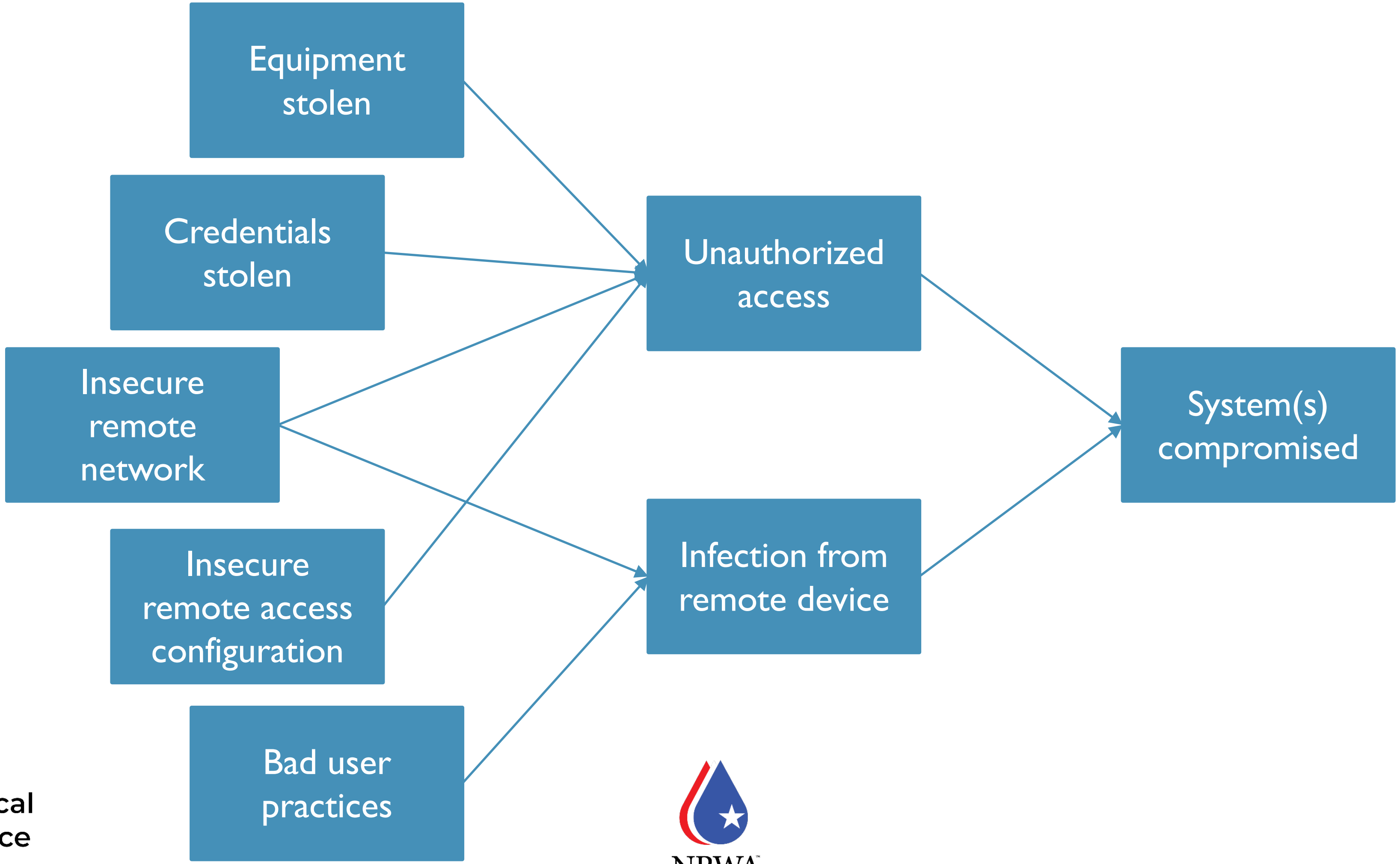
When is remote access needed?

Who has remote access?

Remote Access

Where is remote access available from?

REMOTE ACCESS CONCERNS



Equipment stolen

Credentials stolen

Insecure remote network

Insecure remote access configuration

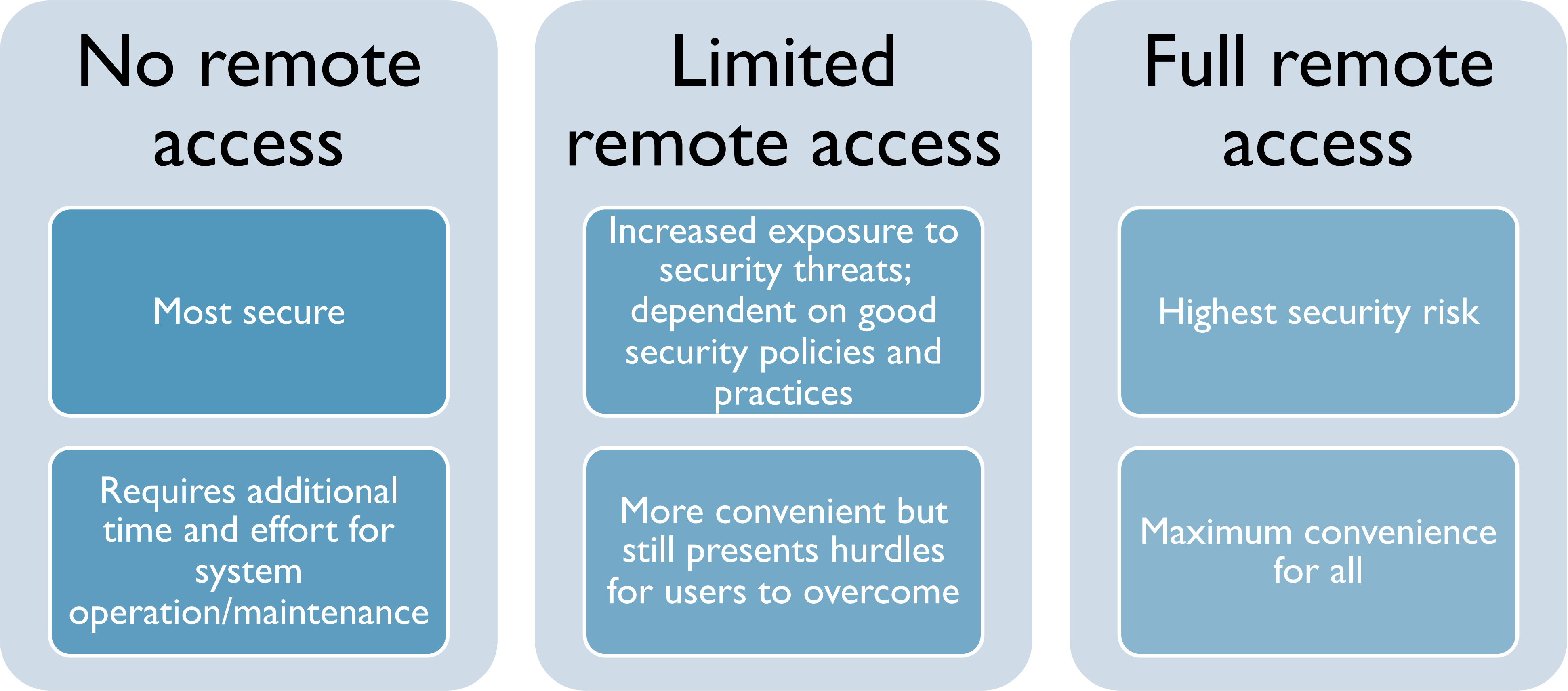
Bad user practices

Unauthorized access

Infection from remote device

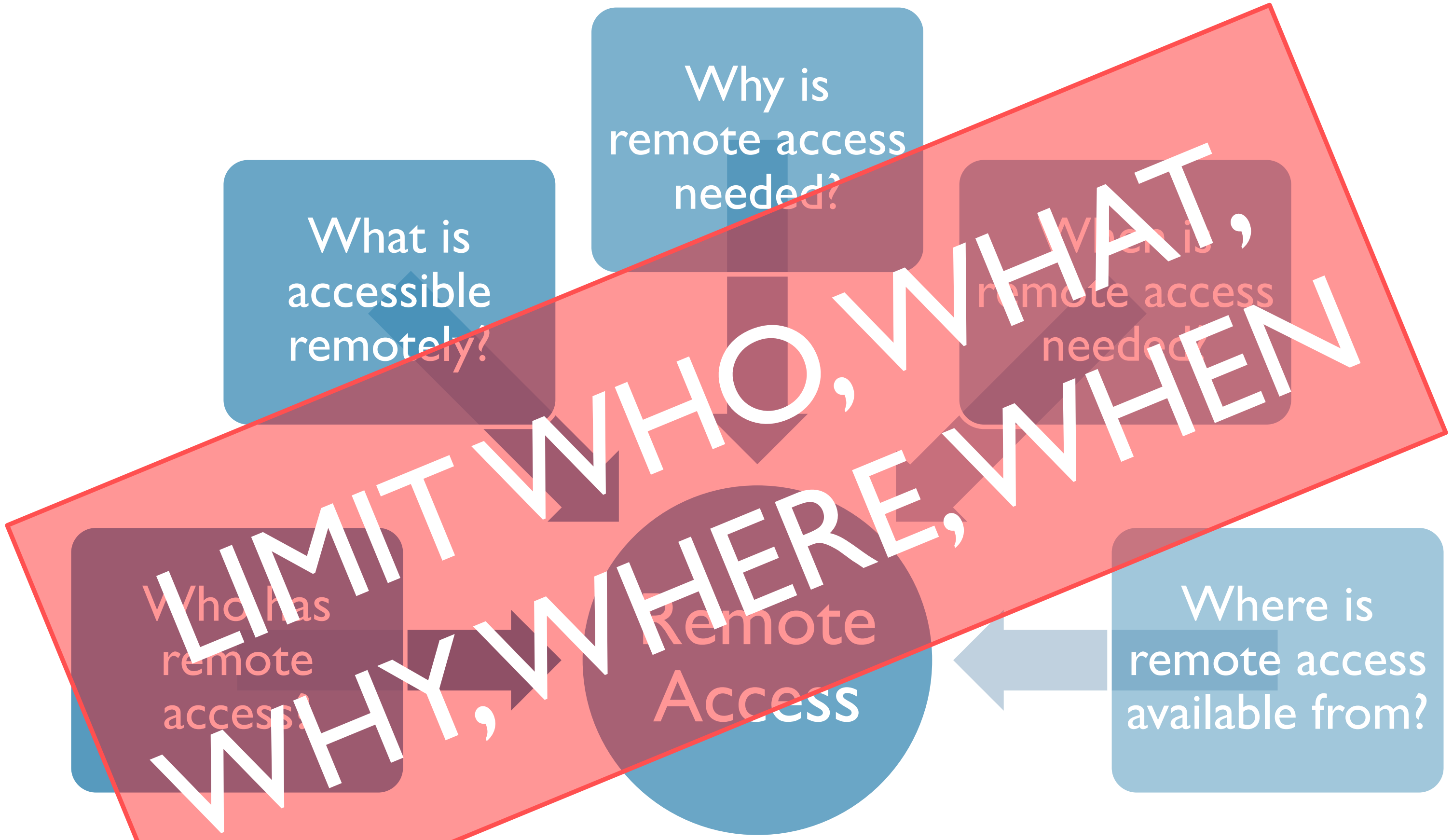
System(s) compromised

REMOTE ACCESS OPTIONS



No remote access	Limited remote access	Full remote access
Most secure	Increased exposure to security threats; dependent on good security policies and practices	Highest security risk
Requires additional time and effort for system operation/maintenance	More convenient but still presents hurdles for users to overcome	Maximum convenience for all

REMOTE ACCESS QUESTIONS



Why is remote access needed?

What is accessible remotely?

When is remote access needed?

Who has remote access?

Remote Access

Where is remote access available from?

LIMIT WHO, WHAT, WHY, WHERE, WHEN

HOW TO PROVIDE SECURE REMOTE ACCESS IF REQUIRED

Secure private network

- End to end encryption
- Mutual device authentication

Network monitoring and log analysis

- Looking for unusual activity (location, time, user, etc)

Good segregation of network devices

- Jump servers, port filtering and network address translation

End-user managed

- Disabled when not required
- Manually enabled when needed
- Hold MFA token generator on site

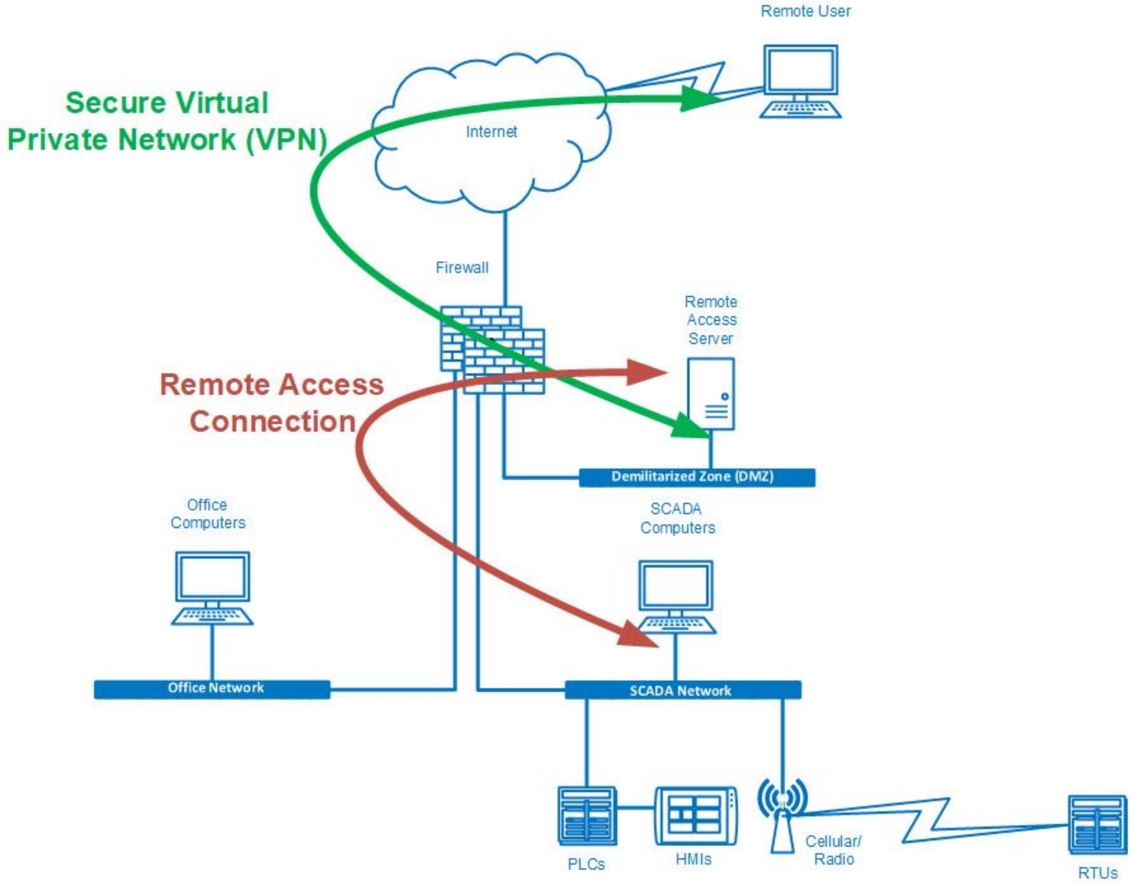
Strict management of external users

- Minimum number of named users
- End-user managed devices or strict monitoring of AV/patch status
- Access only from specific remote locations or devices

Manage centrally through standardized solution

- Avoid vendor-specific or point solutions
- Follow the configuration hardening guidance provided by the solution vendor

RECOMMENDED ARCHITECTURE



QUESTION

- Which of the following controls would be MOST EFFECTIVE in a secure remote access solution:

1. Ensuring remote access is always available
2. Enforcing multi-factor authentication on all user accounts
3. Limiting firewall traffic to only allow the remote access application through
4. Creating a shared user account for remote access only
5. Maintaining active anti-malware controls on the remote access server

RESOURCES

CYBERSECURITY RESOURCES – PASSWORDS

- NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management, 2017
- NSA, Commercial Solutions for Classified, Data-at-Rest Capability Package V5.0, Nov. 18, 2020.
- NSA, Network Infrastructure Security Guidance, Mar. 2022
- NSA, RandPassGenerator, https://github.com/nsacyber/RandPassGenerator

CYBERSECURITY RESOURCES - MFA

- CISA MFA Fact Sheet
- CISA CAPACITY ENHANCEMENT GUIDE – Implementing Strong Authentication
- Executive Order 14028: Improving the Nation's Cybersecurity
- Secure access to resources with multifactor authentication (Microsoft)
- Critical Infrastructure Defense Project
- FIDO Alliance
- CISA Bad Practices

CYBERSECURITY RESOURCES - GENERAL

- NRWA Cybersecurity web page, https://nrwa.org/issues/cybersecurity/
- MS-ISAC membership (state, local, tribal, territorial), https://www.cisecurity.org/ms-isac/
- WaterISAC membership (60-day free trial available), https://www.waterisac.org/membership
- 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

SAVE THE DATE
FUTURE NWRA-WATERISAC WEBINARS

- PART 3: April 14 – Risk Management
  - Patching
  - Backups
  - Incident Management

QUESTIONS

STEVE MUSTARD

smustard@mcgalliance.org

JENNIFER WALKER

walker@waterisac.org

ANDREW HILDICK-SMITH

hildick-smith@waterisac.org

THANK YOU