INL/CON-24-78118-Revision-0

Engineering in Cyber Resilience with Cyber-Informed Engineering

May 2024

Virginia L Wright

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-78118-Revision-0

Engineering in Cyber Resilience with Cyber-Informed Engineering

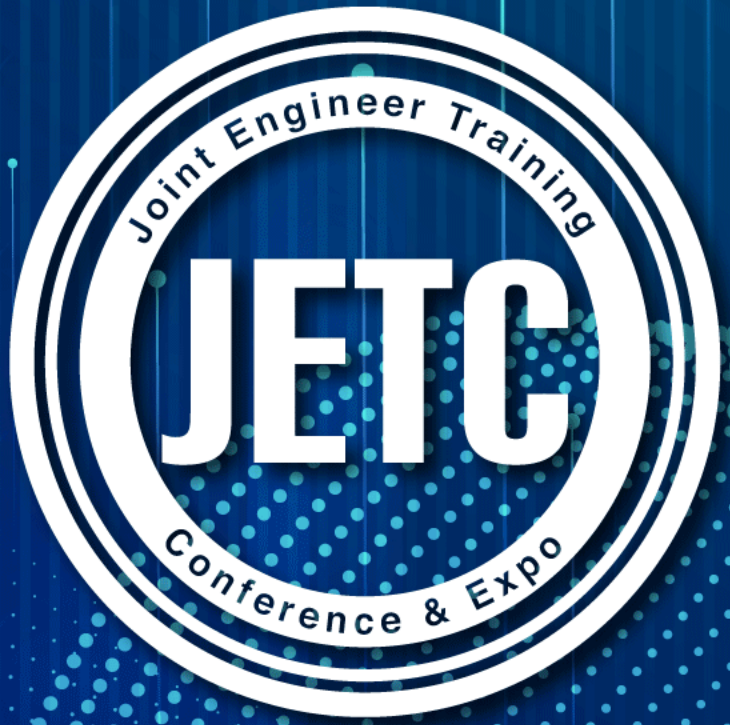
Virginia L Wright

May 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517



MAY 14-16, 2024
ORLANDO, FL

2024 JOINT ENGINEER TRAINING CONFERENCE & EXPO

OPERATION: COLLABORATION

SAME

SAMEJETC.ORG #SAMEJETC24

Engineering in Cyber Resilience with Cyber-Informed Engineering

Moderator: Lucian Niemeyer, Building Cyber Security

Speakers:

- Virginia Wright, Program Manager, INL
- Cheri Caddy, Senior Advisor, DOE

May 14, 2024, 1:30 p.m.

Joint Engineer Training JETC Conference & Expo

MAY 14-16, 2024
ORLANDO, FL

OPERATION: COLLABORATION

SAME SAMEJETC.ORG

SPEAKER

Virginia Wright

Idaho National Laboratory

CIE Program Manager

Fun Facts

- INL has a research range which is the size of Rhode Island.
- INL has hosted 52 reactors since 1949
- INL has demonstrated that nuclear power could fly an airplane

Joint Engineer Training JETC Conference & Expo

MAY 14-16, 2024
ORLANDO, FL

OPERATION: COLLABORATION

SAME SAMEJETC.ORG

SPEAKER

Cheri Caddy

U.S. Department of Energy

Senior Technical Advisor for Cyber

Fun Facts

- Cyber attacks on ICS keep increasing
  - Ransomware attacks on ICS are up 50% between 2022-2023 (according to Dragos)
- Connected Vehicles – a ubiquitous part of converged IT/OT – are an area of increasing focus

Joint Engineer Training
JETC
Conference & Expo

MAY 14-16, 2024
ORLANDO, FL

OPERATION: COLLABORATION

SAME SAMEJETC.ORG

conferences i/o

or browse to
jetc.cnf.io

This is an interactive session.
To participate, use your mobile device:
jetc.cnf.io
Or scan the QR Code

- Find the session.
- The presenter will unlock the poll(s) during the presentation.
- Please complete a brief Evaluation Survey at the end of the session.

HOUSEKEEPING ITEMS

- Take Note of Exits
- Silence Your Mobile Devices
- Presentations and Audio Recordings will be available in the Attendee Service Center until August 30, 2024
- Download your PDH record in the Attendee Service Center before August 30, 2024

Cyber-Informed Engineering

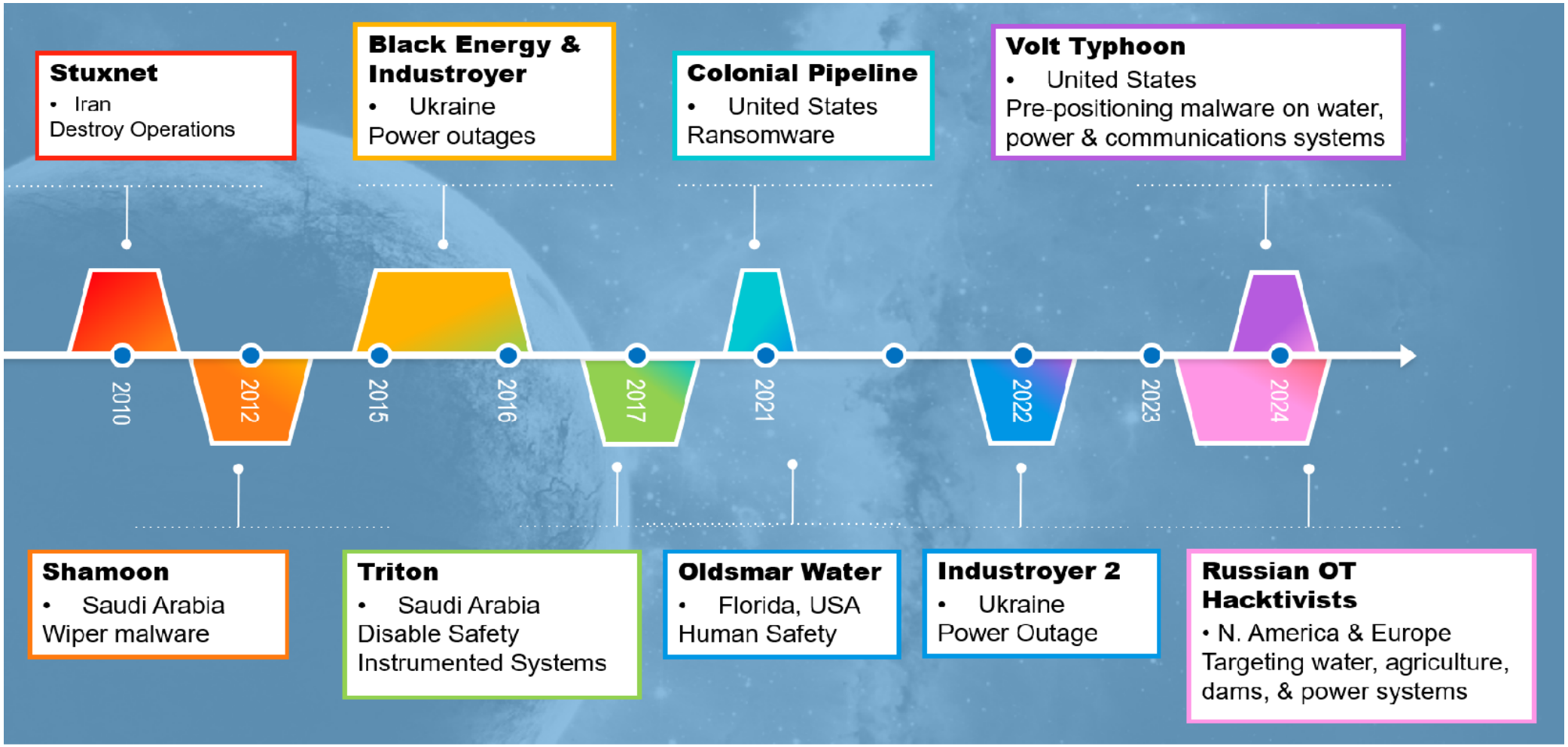
Engineering in Cyber Resilience with Cyber-Informed Engineering

Polling Question: (CHOOSE ALL THAT APPLY)

What role do you serve in ensuring cybersecurity for your infrastructure?

a) I set the requirements
b) I design systems, aligned to the requirements
c) I use systems, aligned to the requirements
d) I create or sell systems
e) I advise on cybersecurity
f) None

Cyber Attacks on Control Systems are Real – and Growing



Cybersecurity Threats are no longer Just Theoretical

Attackers May Be Coming for Your Plant. Time to Tighten Cyber Defenses.

The water and wastewater sectors are targets for a variety of cyber attacks. Some simple measures can go a

Every "Thing" Everywhere All at Once

Every asset in an organization's inventory that is not accounted for and protected is a potential attack vector that an attacker can use to gain access or move undetected.

BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to the Kremlin's Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn't dare to.

Cybersecurity

US warns hackers are carrying out attacks on water systems

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

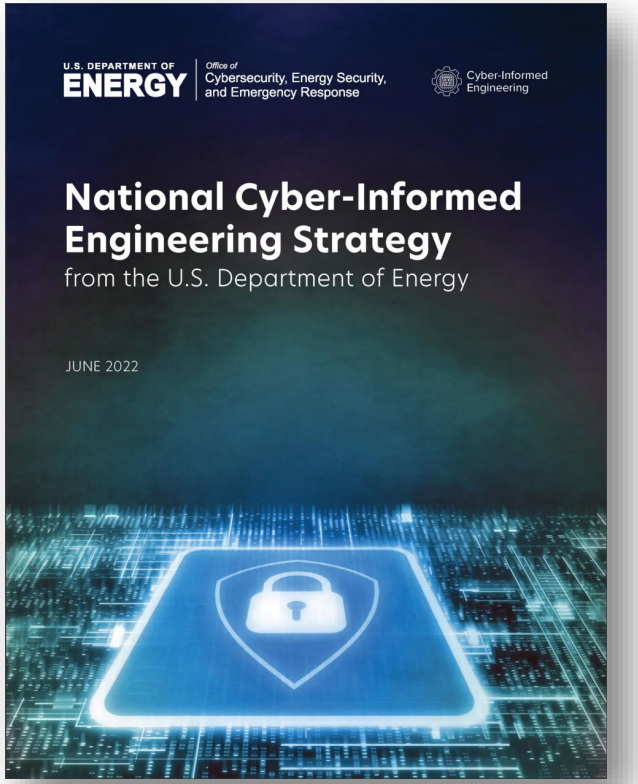
Date: May 24, 2023 **Alert Code:** AA23-144a

Russia-linked hackers claim cyberattacks on U.S., French and Polish water utilities

Russian hackers breached, sabotaged Texas water treatment plant, cyber firm says

National CIE Strategy

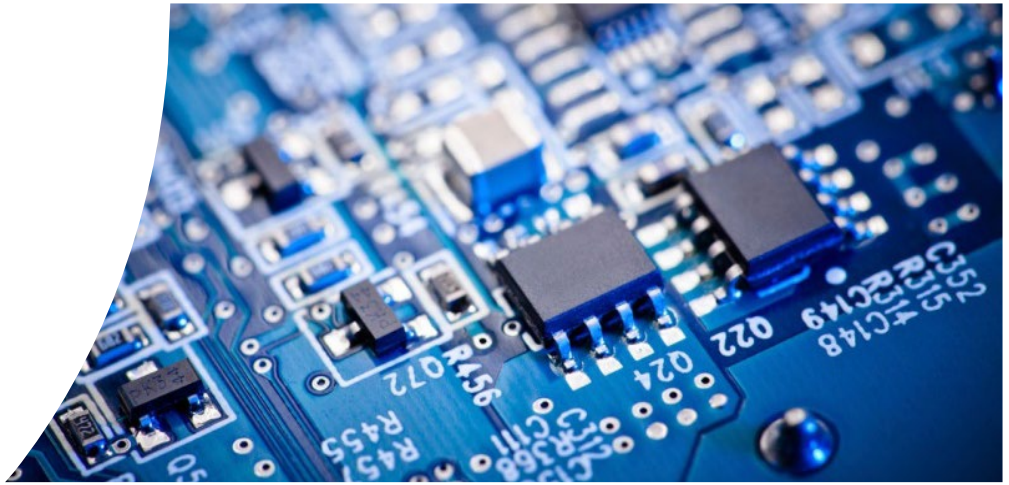
- Directed by the U.S. Congress in the Fiscal Year 2020 National Defense Authorization Act
- Outlines core CIE concepts
  - Defined by a set of design, operational, and organizational principles
  - Placed cybersecurity considerations at the foundation of control systems design and engineering
- Five integrated pillars offer recommendations to incorporate CIE as a common practice for control systems engineers
  - Intended to drive action across the industrial base stakeholders—government, owners and operators, manufacturers, researchers, academia, and training and standards organizations
- DOE issued the National CIE Strategy June 15, 2022
- CIE has been named in the National Cyber Strategy and the National Cyber Strategy Implementation Plan and in the report on cyber-physical systems by the President's Council of Advisors on Science and Technology



https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to create a **culture of security** aligned with the existing industry safety culture.



Pillars of the National CIE Strategy

Awareness

Promulgate a universal and shared understanding of CIE

Education

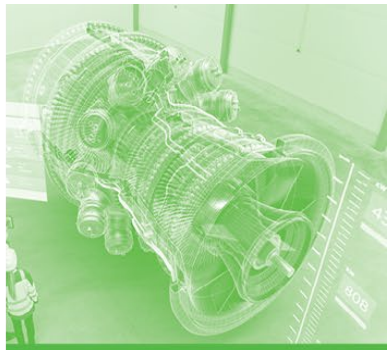
Embed CIE into formal education, training, and credentialing

Development

Build the body of knowledge by which CIE is applied to specific implementations

Current Infrastructure

Apply CIE principles to existing systemically important critical infrastructure



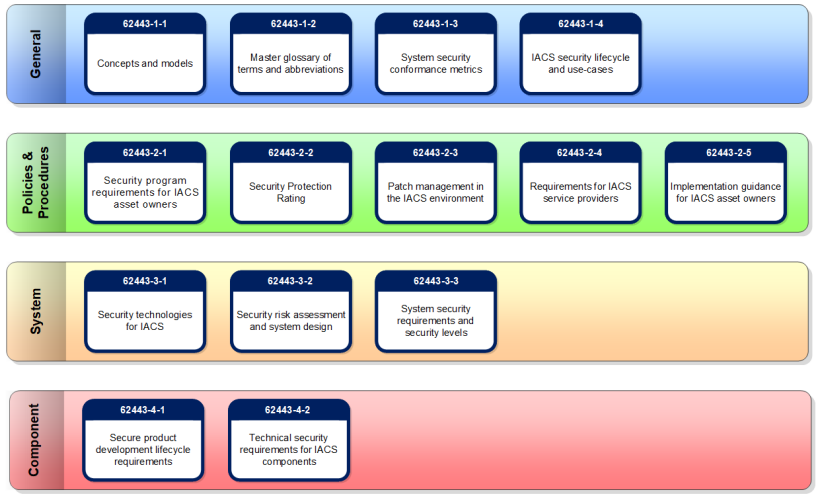
Future Infrastructure

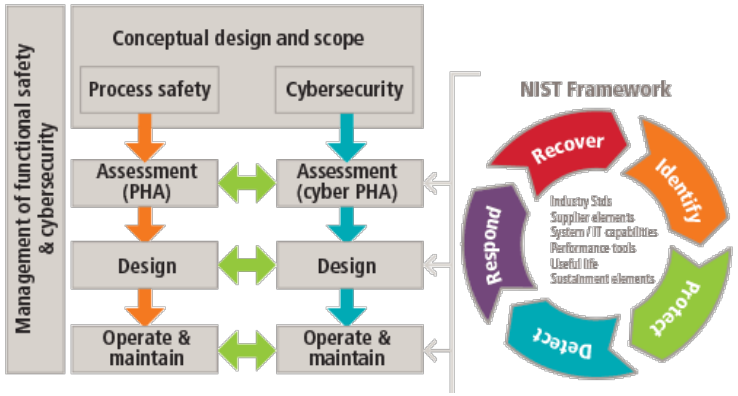
Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology

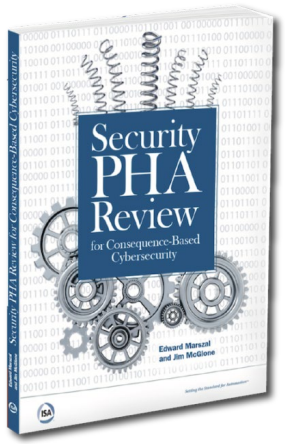
CIE Principles

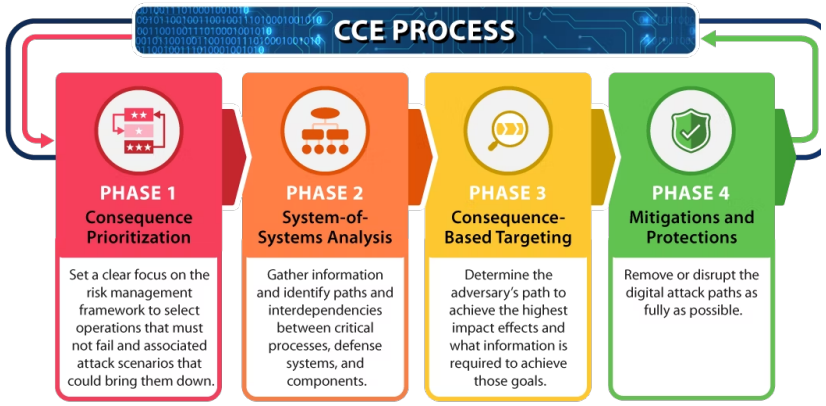
Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

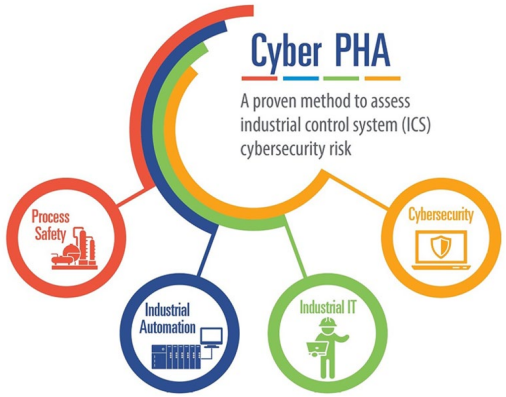
OK, But How Do You CIE?







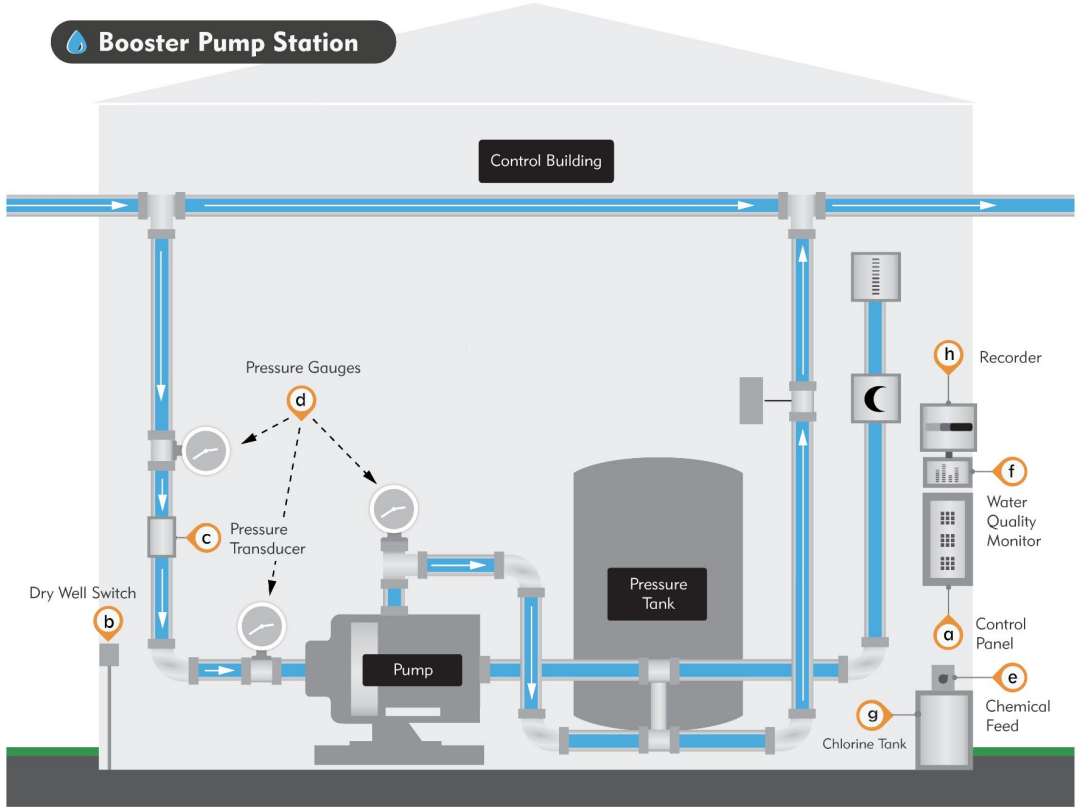




How does this work in practice?

Water Booster Pump Station

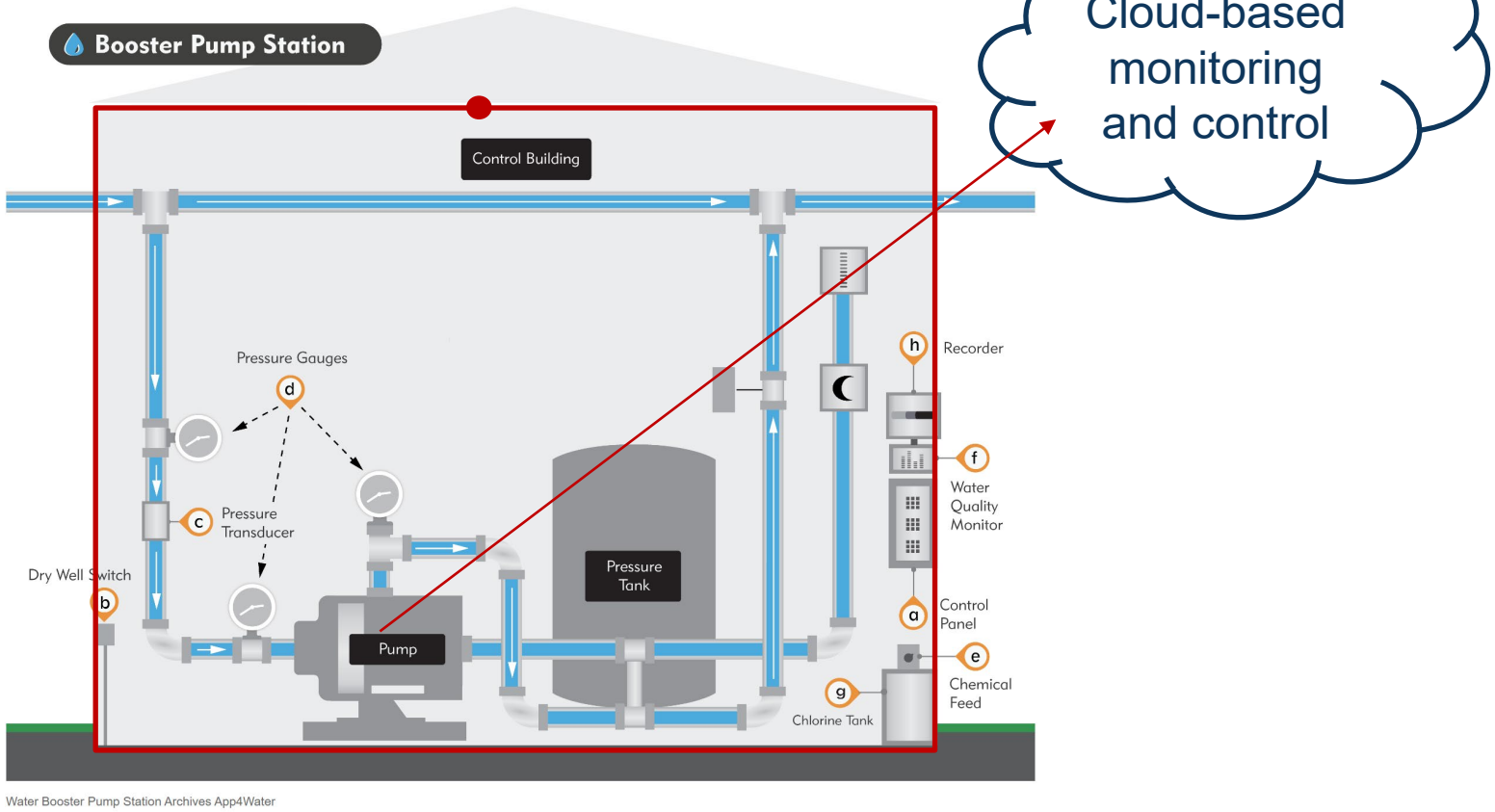
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://www.app4water.com/product-category/applications/booster-pump-station/

Cyber Solution Review

- Control System Software has a qualifying secure development lifecycle.
  - Very mature demonstrated processes
  - Provided SBOM
  - Component infrastructure is up to date
  - Mature vulnerability release process – with regular patches
  - 24/7 Support availability

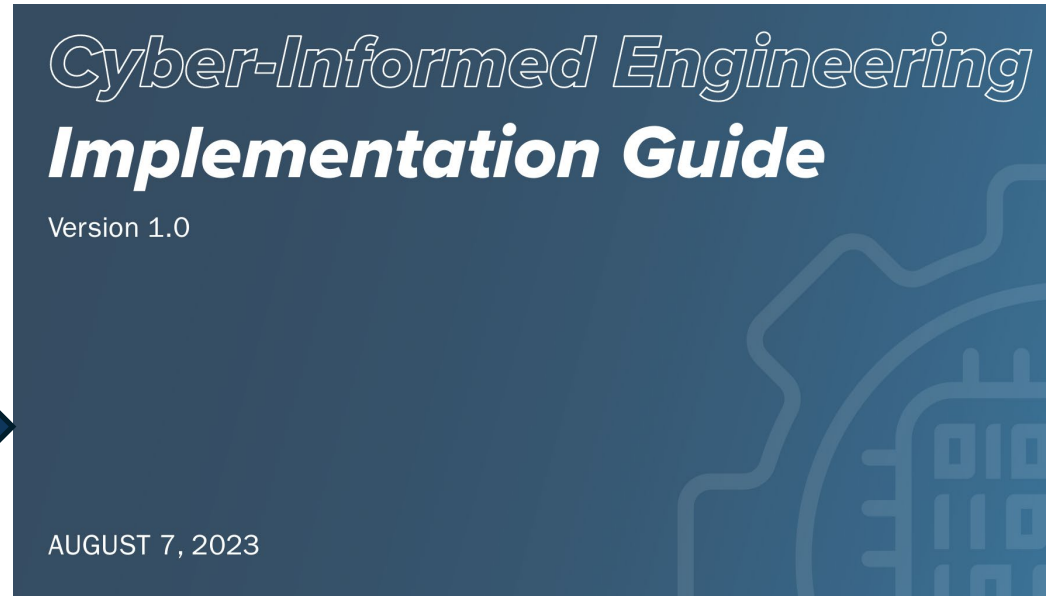
- Cloud provider is reputable and qualified
  - SOC Type 2 and FedRamp (if needed), great physical security
  - Very mature, experienced in hosting critical infrastructure services
  - Demonstrated response and restoration capabilities

IT Installation Review

- Network entry point has standard security package
- Monitoring and logging traffic on this interface according to standard practice
  - Logging interfaces with organizational logging system
- Traffic in and out is encrypted between the cloud provider and the site network boundary

Organizational Review Board Votes

- Finance / Accounting –
- Information Technology –
- Cybersecurity –
- Engineering Operations –



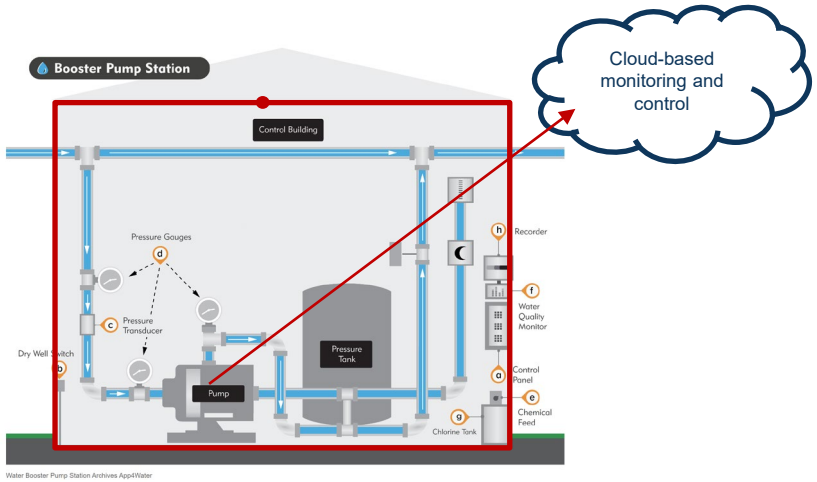
CIE Application for

Water Booster Pump Station

Consequence-Focused Design

KEY QUESTION

How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?



Assuming attacker defeats security controls:

- What is the worst that can happen?
  1. Attacker turns pumps on / off
  2. Attacker turns multiple pumps on / off
  3. Attacker turns pumps on / off quickly to damage equipment
- How would we respond?
  - For 1 and 2, return to manual mode operations until resolved
- Would any of these issues be catastrophic?
  - 3 would cause loss of pressure, water hammer effect, significant outage, replacement of equipment and significant expense

Engineered Controls

KEY QUESTION

How do I implement controls to reduce avenues for attack or the damage which could result?

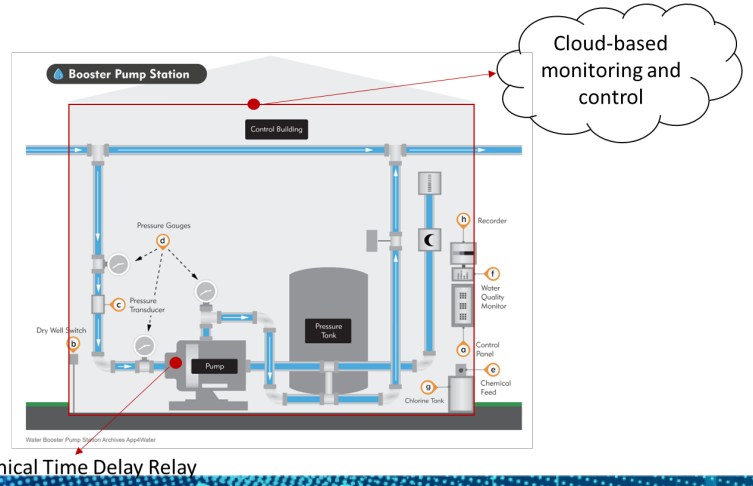
Attacker defeats security and turns pumps on / off quickly to damage equipment – 18-month outage, large repair / replacement project

- Ideal control:
  - Deterministic (governed by physics)
  - Not networked / digital
  - It is visible and can be seen in infrastructure
  - Complimentary with existing protections
- Engineer suggests analog time-delay relay – slows command speed and eliminates potential for water hammer conditions resulting in equipment damage

Secure Information Architecture

KEY QUESTION

How do I prevent undesired manipulation of important data?



What are the data elements in this system where manipulation could have the most impact?

- *IT says: Denial / Loss of View or Denial / Loss of Control*

Where could manipulation of data lead to Engineering or Operational Impacts?

- Loss of Protection
- Loss of Safety
- Loss of Productivity and Revenue
- Damage to Property

How should the potential for these specific operational impacts inform the cybersecurity strategy?

Design Simplification

KEY QUESTION

How do I determine what features of my system are not absolutely necessary?

VFD-driven Pump

Relay-driven Pump

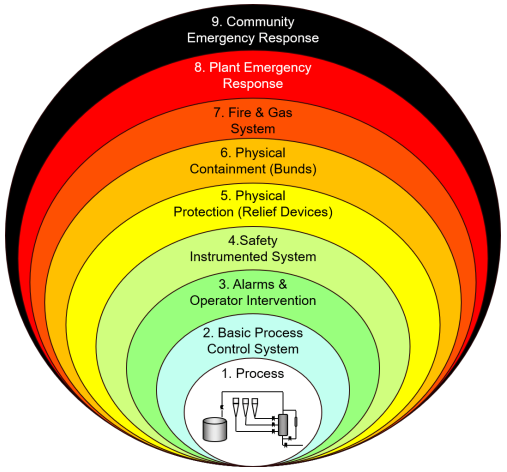
Where could we eliminate a system feature that would reduce potential for attack impacts? If we can't eliminate the features, how can we ensure they are not misused?

- When this pump station was built, the team considered a network-connected, Variable Frequency Drive-controlled pump.
- The team chose instead to have a relay control the pump.

Layered Defenses

KEY QUESTION

How do I create the best compilation of system defenses?



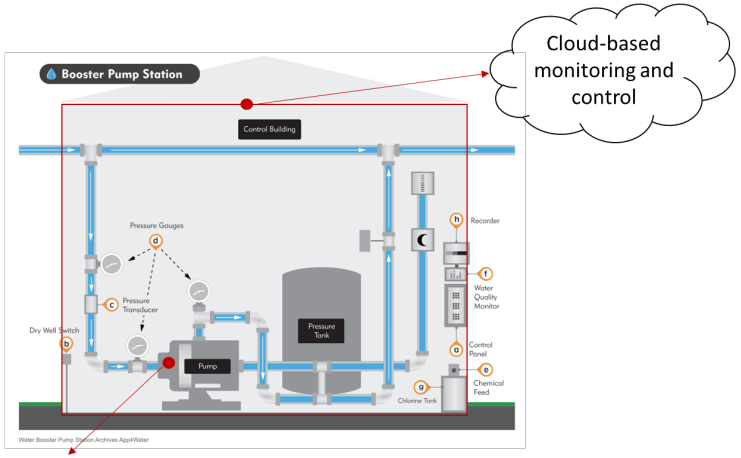
If we identify that an adversary turning on and off pumps leads to our worst engineering consequences -

- How can cybersecurity prioritize the defenses from our side and from the vendors to detect or prevent that from happening?
- How many layers of protection can we assemble?
- How can we inform cybersecurity requirements?

Active Defense

KEY QUESTION

How do I proactively prepare to defend my system from any threat?



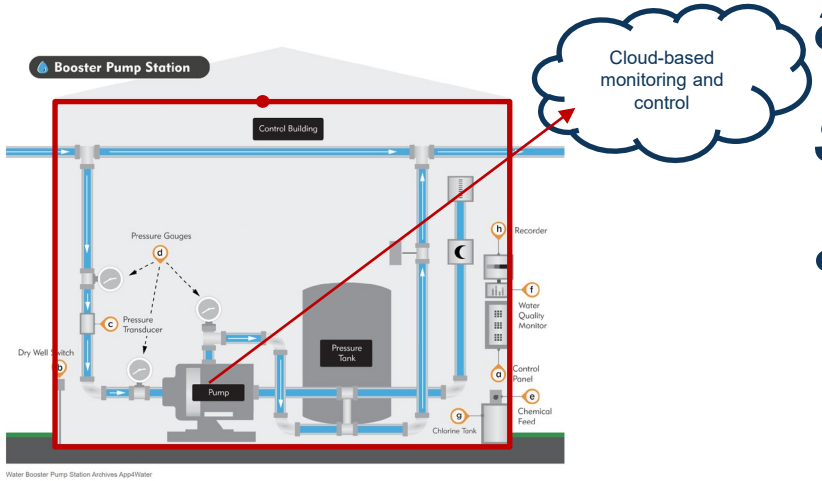
If we identify that an adversary turning on and off pumps leads to our worst engineering consequences -

- How would we defend against that action?
- What do we expect of our vendor? Do we need additional contracts?
- How will engineering and cyber work together during the defense?
- Have we documented and practiced our defense?

Interdependency Evaluation

KEY QUESTION

How do I understand where my system can impact others or be impacted by others?



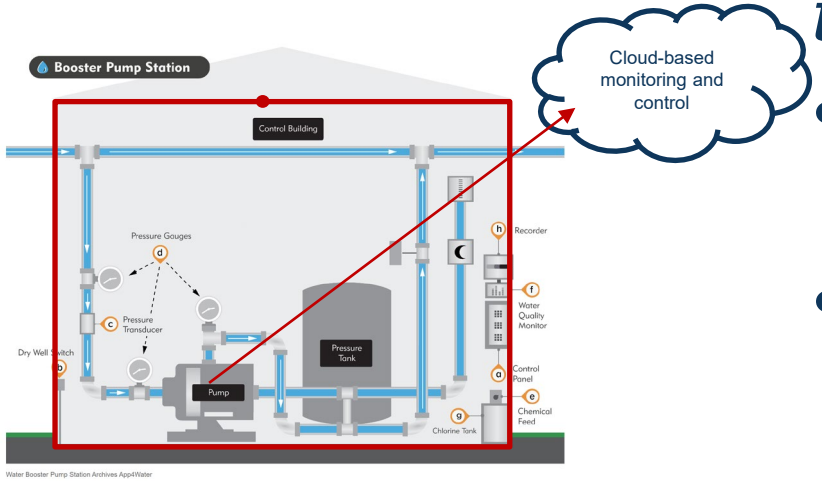
We have added a new interdependency – the cloud service and software. Beyond specific cyber attack, how might instability in this service affect our operations?

- What happens if the service goes down?

Digital Asset Awareness

KEY QUESTION

How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?



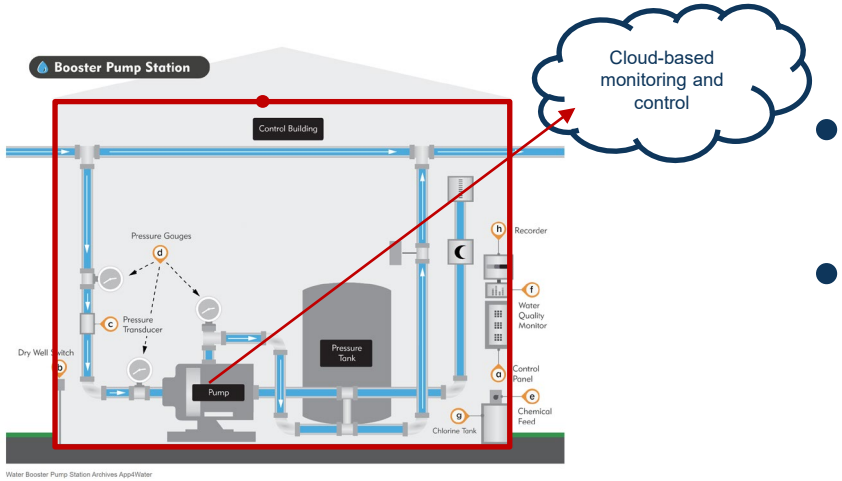
We have talked to the vendor about extending the product to allow remote control of the chlorinator. We are used to operating it manually. How will the use of digital technology change engineering risk?

- Is the dispensed amount hardwired or adjustable?
- How do we know that the product was actually dispensed?

Cyber-Secure Supply Chain Controls

KEY QUESTION

How do I ensure my providers deliver the security we need?



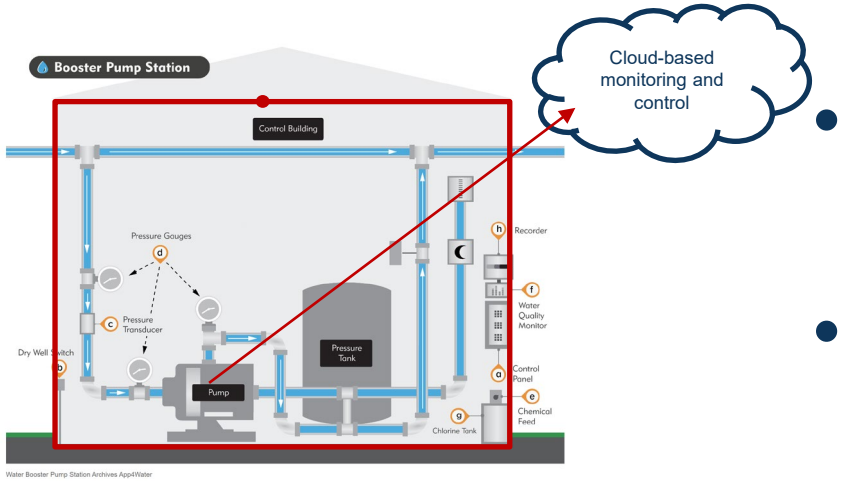
We examined the components used by the vendor and the security culture of the cloud company and both were very mature. However, there are still some questions we need to ask.

- How is the system patched? How are patches delivered? Can the asset owner accept or reject a patch?
- Does the software vendor or cloud provider ever allow access to our system to their vendors or maintainers?
- How are 3rd-party support providers, including the call-in support qualified and vetted?

Planned Resilience

KEY QUESTION

How do I turn “what ifs” into “even ifs”?

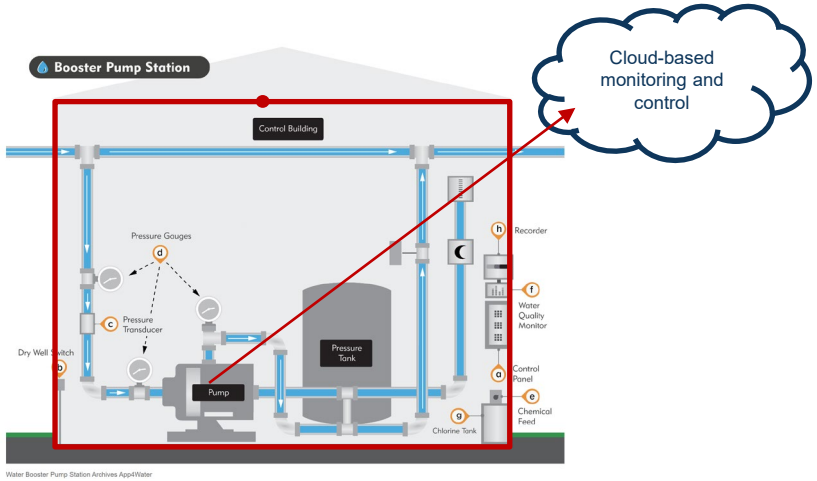


- *What if an attacker turned all of the pumps on or off?*
  - We use manual operations and contact the vendor. We predict very little loss from this scenario.
- *What if the application vendor reported an adversary attack?*
  - We return to manual operations and have a contract vehicle to ensure we can staff that for up to 2 weeks.
- *What if the application stopped working?*
  - See above. After two weeks, we would need to arrange for emergency staffing.
- *What if the cloud vendor had ransomware?*
  - See above.

Engineering Information Control

KEY QUESTION

How do I manage knowledge about my system? How do I keep it out of the wrong hands?



- *How much information about this upgrade must be shared*?
  - Municipal water activities are public record.
  - High level information about this upgrade must be shared.
  - Engineering team recommends to leadership that the specific vendor, product name, and cloud vendor name be kept out of the record.

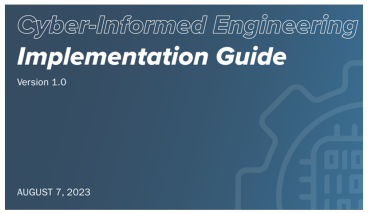
Cybersecurity Culture

KEY QUESTION

How do I ensure that everyone performs their role aligned with our security goals?

Organizational Review Board Votes

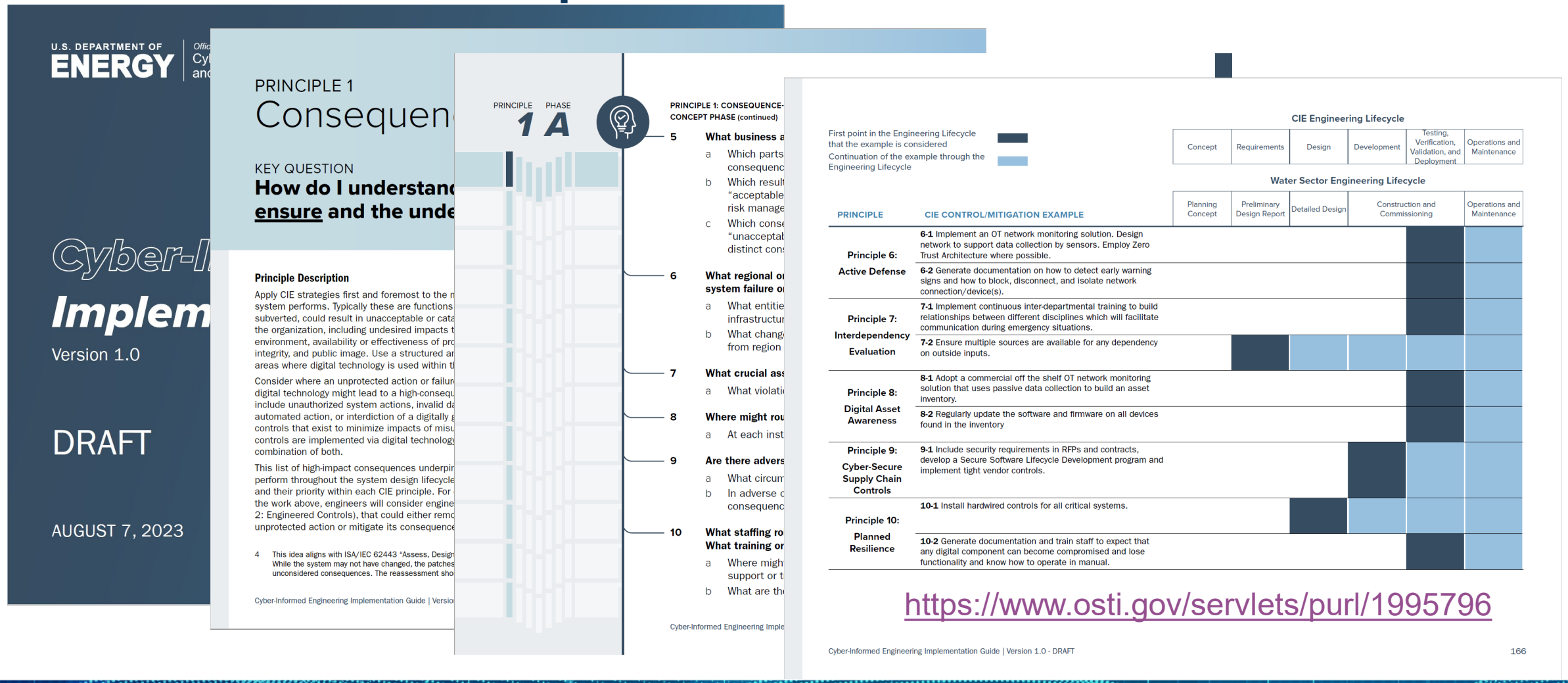
- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ? ➡



- *How do we build an inclusive cybersecurity culture?*
  - The fact that engineering could drive the implementation based on potential impacts of a cyber attack was a major change.
  - Engineering will need to talk to procurement to ensure resiliency resources are obtained.

So Where from here with CIE?

CIE Implementation Guide



https://www.osti.gov/servlets/purl/1995796

Takeaways and Actions

- **Key Takeaway**: Cybersecurity *is* for Engineers
- **Action**: Review the CIE Implementation Guide to see how cybersecurity can apply to your engineering tasks
- **Action**: Join a CIE COP Working Group!

CIE COP and Working Group Purpose

Cyber-Informed Engineering COP

Quarterly

11 AM ET on the 2nd Wednesday of January, April, July, and October

Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

CIE Standards WG

Monthly

1st Wednesday, 9 AM MT / 11 AM ET

Support integration of CIE into engineering and cybersecurity standards

CIE Education WG

Monthly

3rd Wednesday, 9 AM MT / 11 AM ET

Develop curricula and materials that integrate CIE principles into engineering degree programs

CIE Implementation WG

Monthly

4th Wednesday, 9 AM MT / 11 AM ET

Develop CIE implementation guidance and an open-source library of resources

Current Activities

Working with Standards Bodies

- IEEE PES, and others
- ISA99 – 62443

Working with Universities

- Developing curriculum guidance
- Incorporating CIE into engineering education

Working with Asset Owners

- Incorporate CIE into ongoing efforts
- Refine products
- Templates for cyber-informed designs

Recent CIE Publications

Websites

- **DOE CESER CIE Website –** https://www.energy.gov/ceser/cyber-informed-engineering
- **INL CIE Website -** https://inl.gov/cie/
- **NREL CIE Website -** https://www.nrel.gov/security-resilience/cyber-informed-engineering.html

Publications

- **CIE Implementation Guide:** Cyber-Informed Engineering Implementation Guide (Program Document) | OSTI.GOV
- **CIE Workbook (Distribution, ADMS):** https://www.osti.gov/biblio/1986517
- **CIE Workbook (Microgrids):** https://www.osti.gov/biblio/2315001

Articles and Briefings

- **SANS ICS Concepts Video:** https://youtu.be/o_vIxW6UTeg
- **Industrial Cyber**: CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
- **Harvard Business Review**: Engineering Cybersecurity into U.S. Critical Infrastructure (April 17, 2023) by Ginger Wright, Andrew Ohrt, and Andy Bochman
- **Shift Left video podcast on GrammaTech blog**: Shifting Left for Energy Security (April 4, 2023) with Ginger Wright, Idaho National Lab and Marc Sachs, Auburn University
- For more CIE articles and publications, visit: inl.gov/cie

Engineering in Cyber Resilience with Cyber-Informed Engineering

Please provide feedback!

Thank You!

CIE@inl.gov

https://www.energy.gov/ceser/cyber-informed-engineering

conferences i/o

or browse to
jetc.cnf.io