WELCOME

- Consequence-driven Cyber-informed Engineering (CCE)
- Cyber Informed Engineering (CIE)
- Building CCE into a Large SCADA System Upgrade Program

City of SACRAMENTO
Department of Utilities

WHAT IS CCE

- 1. Consequence Prioritization – Generation of a sharply prioritized risk management framework focused on a handful of operations that simply must not fail.
- 2. System of Systems Breakdown – Identification of the multifaceted interdependencies between critical process, defense systems, and enabling or dependent components.
- 3. Consequence-based Targeting – Determination of what the adversary must accomplish to achieve the highest impact effects, where they need to be to conduct the attack, and what information is required to achieve their goals.
- 4. Mitigations and Protections – Production of a plan to remove or disrupt the digital attack vectors as fully as possible

City of SACRAMENTO
Department of Utilities

AGENDA

- PROJECT BACKGROUND
- WHY WE CHOSE TO USE CCE/CIE
- SACRAMENTO'S CCE/CIE PROCESS
- LESSONS LEARNED
- NEXT STEPS

City of SACRAMENTO
Department of Utilities

PROJECT BACKGROUND

- Over 200 Facilities throughout City (Water, Wastewater, Stormwater, Combined Sewer)
- 67% of hardware at End of Commercialization
- Improvements aligned with Department's Strategic Plan
- Improvements Program Developed
  - $67M over 6 years
  - Replacement of majority of SCADA hardware
  - Upgrades to communications network and cybersecurity
- Program Management Team selected to support program

City of SACRAMENTO
Department of Utilities

WHY WE CHOSE CCE/CIE

- Previous work with INL (DHS assessment)
- Need to address
- Sacramento staff attended INL training (ICS Cybersecurity (301))
- Harvard Business Review (HBR) Article by Andy Bochman
- Program Manager (West Yost) working relationship with INL
- Opportunity to implement recommendations of AWWA Cyber security assessment tool
- Reduce the risks and consequences from potential security breach of SCADA system
- Change the way systems are engineered, versus bolt-on afterwards

City of SACRAMENTO
Department of Utilities

PARTNERING WITH LEADERS IN THE INDUSTRY

SACRAMENTO CIE/CCE PROCESS

- Initial Workshop
  - Presentation on CIE/CCE by INL
  - Review of Standard Specifications (Electrical, Instrumentation and Controls)
- Update Standard Specifications
- Develop CIE Design Guidelines for engineering consultants
- Review SCADA Programming Standards
  - HMI software
  - PLC function blocks
- Review Updated Network Architecture
  - Following NIST 800 framework

City of SACRAMENTO
Department of Utilities

LESSONS LEARNED

Current engineering culture does not consider cybersecurity in traditional design

Standard Specs may not completely cover CIE. Projects are required be evaluated case by case.

Design Guidelines required for successful design and implementation

City of SACRAMENTO
Department of Utilities

LESSONS LEARNED

Technical details involving additional disciplines must be considered to implement CIE

- Electrical- Specify only parameters that are required to be enabled on VFD's and Protective Relays
- Mechanical-Specify parameters for vibration monitoring equipment.
- Process – is ethernet required or is analog, serial, 485 adequate
- Network-Segmented architecture employing zero trust methods.
  - Zero Trust policies following the Kipling Method, answering the who, what, when, where, why, and how of network and policies.
- Operations-Staff trained to not be solely reliant on automation.
- Conduct drills on incident response and "A Day without SCADA"

City of SACRAMENTO Department of Utilities

RESOURCES

https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

https://www.us-cert.gov/ics/alerts

https://www.sans.org/

https://www.waterisac.org/

https://www.awwa.org/

https://inl.gov/

https://www.infragard.org/

City of SACRAMENTO Department of Utilities

RECOMMENDED READING

https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1521570876.pdf

https://www.osti.gov/servlets/purl/1341416

David Sax | Bloomberg Businessweek | "In the Age of Cybercrime, the Best Insurance May Be Analog" | 10 March 2016]

City of SACRAMENTO
Department of Utilities

QUESTIONS?

City of SACRAMENTO
Department of Utilities