PARAGON
SYSTEMS

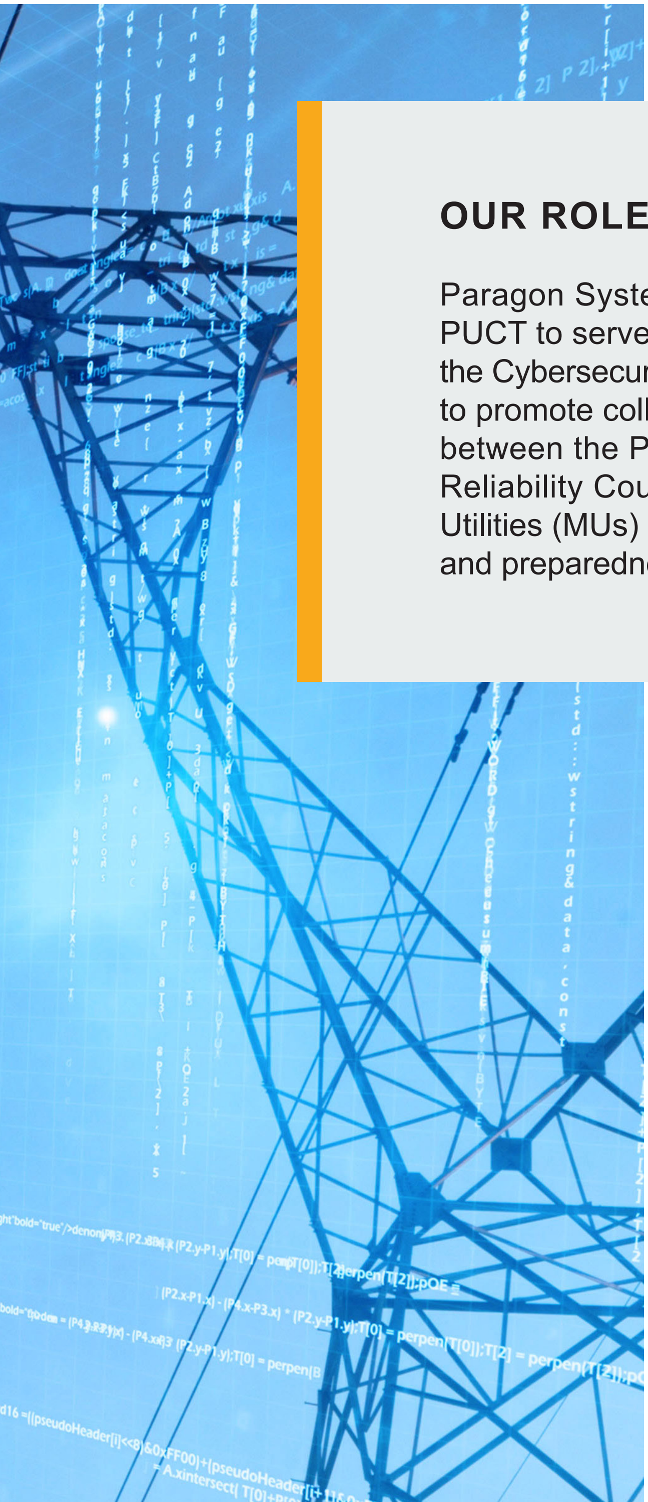
Texas Cybersecurity Outreach Program

COLLABORATE ▪ PROTECT ▪ STRENGTHEN

Program Overview & History

BACKGROUND

In May 2019, Texas State Senate Bill 936 was passed, which required that the Public Utility Commission of Texas (PUCT) and the Electric Reliability Council of Texas (ERCOT) foster a more collaborative, strategic approach to identifying vulnerabilities and finding areas to improve security measures across Texas's critical electric infrastructure.



OUR ROLE

Paragon Systems was selected as an independent agency by the PUCT to serve as the state's Cybersecurity Monitor. The purpose of the Cybersecurity Monitor is to develop a voluntary Outreach Program to promote collaborative discussion on cyber and physical security between the Public Utility Commission of Texas (PUCT), Electric Reliability Council of Texas (ERCOT), and participant Monitored Utilities (MUs) by which Monitored Utilities can express awareness and preparedness through their governance, practices, and training.

> " Learn about real world attacks and how to defend against them. "
>
> - PROGRAM FEEDBACK

Program Overview & History

PROGRAM GOALS

1. Independent Self-Assessment & Recommendation’s Report
    - Not a compliance exercise
2. Information Sharing
    - Examples include: Threat’s & Trends, Statewide Resource Needs, etc.
3. Cybersecurity Training
    - Provide recommendations and identify available resources related to self-assessment identified focus areas
    - Biennial Incident Response Tabletop Exercise

PROGRAM COMPONENTS

Security Meetings

Discuss Threats, Vulnerabilities, and Hot Topics

Tabletops

Remote and in-person incident response exercises

Internal Benchmarking

Conduct a self-assessment on cybersecurity posture

Education

Keynote speakers from the public and private sector best-practice lectures

Security Meetings

Security Meetings are held quarterly between Paragon Systems and participating utilities to provide opportunities for utilities to interact with one another to discuss concerns, emerging threats, and trends facing Texas electric utilities. These meetings also include industry specific security briefings and training sessions, designed to inform and educate.

PURPOSE

The purpose of Quarterly Security Meetings are to provide a secure environment for utilities to share information regarding threats and best practices.

PARTICIPANTS

Participants include a variety of technical and non-technical analysts and decision makers, e.g., CISOs, Cybersecurity Analysts, City Managers, General Managers.

TIME & PLACE

Security Meetings are quarterly affairs held in March, June, September, and December. They are virtual meetings and participants are pre-screened prior to entry.

KEYNOTE SPEAKERS

Security Meetings are forums for expert speakers to delineate valuable information and resources. Past speakers include:

- Leach Strategic Partners
    - Counter Unmanned Aircraft Systems
- Michael Best, LLP
    - Top Ten Steps to Building a Cyber Incident Response Plan and Procedure

Security Meetings

TOPICS COVERED:

2021

- Impact of IT breaches on OT Operations – Colonial Pipeline Ransomware Hack
- Presidential EO 14028 on Improving the Nation's Cybersecurity
- 2021 Massive Data Breach – The T-Mobile Hack
- Proliferation of Ransomware

2022

- Introduction to Counter Unmanned Aerial Systems (Leach Strategic Partners)
- The State of Utility Cybersecurity in Texas (Elizabeth Rogers, Michael Best LLP)
- Key Risk Mitigation Steps to Take for Breach Prevention
- 8 Key Questions to be Immediate Addressed When Faced with a Cyber Incident
- Top Ten Steps to Building a Cyber Incident Response Plan and Procedures

2023

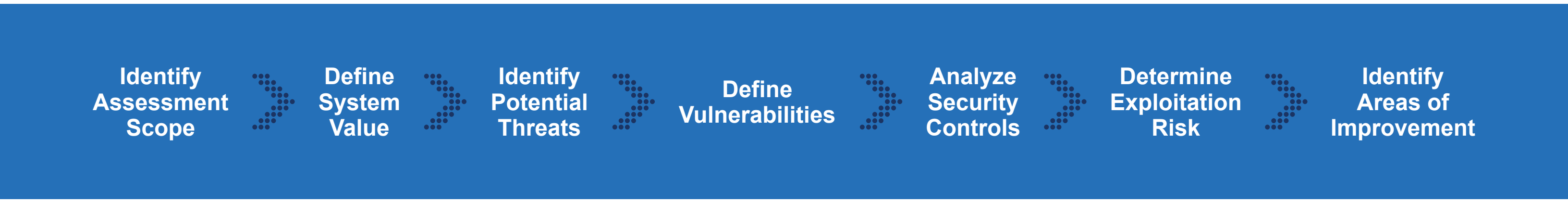
- Managed Detection and Response (Texas A&M Security Operations Center)
- Emerging Social Media, Opportunities for Threat Intelligence (LifeRaft)
- Leveraging DIR Resources (Texas Department of Information Resources)
- Cyber Threat Intelligence (Joe Slowick, Paralus)
- Social Engineering Awareness (TNMP)
- Creating and Negotiating Service Level Agreements (Elizabeth Rogers, Michael Best LLP)
- CyberStrike Lights Out Training
- Artificial Intelligence - Usage, Risks, and Safeguards (Oncor)
- Cybersecurity Insurance – Best Practices (Elizabeth Rogers, Michael Best LLP)
- Workforce Development – Best Practices in the Muni Space (Bryan Texas Utilities)

2024

- GridEx In A Box: Exercise Deployment with Manageable Resources (E-ISAC)
- Procurement Best Practices & Navigating Cooperative Purchasing Challenges (Signature Advisory Partners)
- BCSI Cloud – Best Practices (Austin Energy)
- Global Security Risks in Cyber and Physical Security (SCIS/Paragon)
- Navigating ERCOT Market Ruling NPRR 1199
- Artificial Intelligence: Opportunities & Threat (Austin Energy)

Self-Assessments

Self-assessments are comprehensive surveys designed to evaluate a utility's cyber and physical security efforts. The average time to complete and submit a self-assessment is expected to be one to two weeks of part-time work. The Cybersecurity Monitor is available to assist utilities with the self-assessment should they run into any issues, however, the process is intended to be completely self-sufficient. Self-assessments and any related information will be kept secure and confidential. They are submitted to the Cybersecurity Monitor through secure means and individual assessments will be kept secure and confidential.



Identify Assessment Scope → Define System Value → Identify Potential Threats → Define Vulnerabilities → Analyze Security Controls → Determine Exploitation Risk → Identify Areas of Improvement

1 The **Incident Management and Response Survey** both questions and best-practice recommendations pertaining to Incident Response and Planning.

2 The **Cyber Insurance Survey** asked utilities about their cyber insurance opinions on policy coverages, claims reimbursement, and cybersecurity breach concerns which warrant the purchase of insurance coverage.

3 The **Personnel Resources Survey** helped to better understand cybersecurity workforce development challenges such as prioritizing tasks and determining how to provide additional training for workforces that are limited in number.

4 The **Asset and Risk Management Survey** focused particularly on utilities' ability to monitor IT and OT equipment as well as managing their supply chain.

Self-Assessments

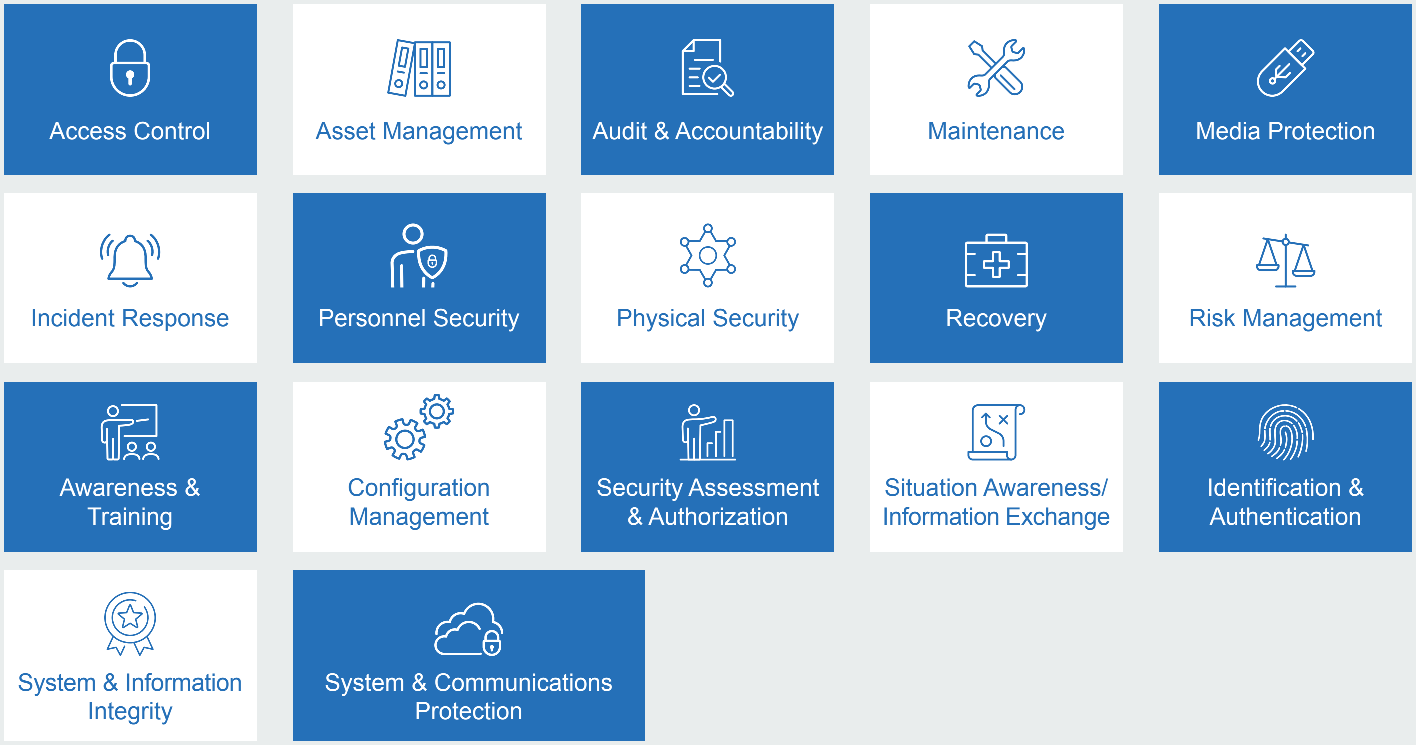
FRAMEWORK

Utilities are measured based on a modified version of the Cybersecurity Maturity Model Certification (CMMC) which comprises 17 cybersecurity domains (see graphic below). All self-assessments are distributed and collected via secure mail using two-factor authentication. To minimize complexity and the volume of questions, our modified framework utilizes three levels of increasing maturity instead of five. The assessment is mapped to the three most popular frameworks among utilities:

- NIST CSF - National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- NERC CIP - North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection
- C2M2 - U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model

TOOLS & CONTROL

The self-assessment tool is an accessible Excel workbook developed specifically for Texas electric utilities, that emphasizes ease of use, and clarity, while ensuring it objectively captures cyber and physical security maturity. The workbook asks control questions, provides extensive help and includes a real-time implementation scorecard.



Access Control

Asset Management

Audit & Accountability

Maintenance

Media Protection

Incident Response

Personnel Security

Physical Security

Recovery

Risk Management

Awareness & Training

Configuration Management

Security Assessment & Authorization

Situation Awareness/ Information Exchange

Identification & Authentication

System & Information Integrity

System & Communications Protection

Maturity Improvement Reports

Maturity Improvement Reports (MIRs) are analytical reports that provide utilities with both a baseline analysis of the self-assessment results along with best-practice recommendations. Reports are authored and circulated to individual utilities upon completion of the self-assessment.

REPORT COMPONENTS

Charted Self-Assessment Responses by Practice Area

- Control Area Scorecards
- Graphical representation of the maturity based on responses

General Cybersecurity Awareness Recommendations

Examples Include:

- Ransomware
- Social Engineering

Recommendations Based on Control Area Response

- Scorecard Result
- Recommendation
- Other Framework Mappings

Resource and Tools

Zero-cost best-practice resources for areas of improvement such as Frameworks, Tools, & Templates

REPORT DELIVERABLES

- Self-Assessment Charts
- Recommendations Based on Response Thresholds
- Resources for Continuous Education
- Cross-Reference Responses to Other Frameworks
- General Recommendations
- Additional Resources & Tools to Promote Cyber Maturity

Tabletop Exercises

The Cybersecurity Monitor holds a recurring Cybersecurity Tabletop Exercise, similar in purpose to the biennial NERC Grid Security Exercise (GridEx). It is intended to be a cybersecurity-focused incident response (IR) training opportunity, designed to simulate a realistic scenario that focuses on a utility's capability to detect, identify, protect, respond, and recover from an attack.

PURPOSE

- Provide a forum for participants to test their incident response plan
- Provide an opportunity for utilities to work with one another on a simulated attack scenario
- Obtain documented exercise feedback that can be easily digestible across the organization

BENEFITS

- Identifies potential issues with IR strategy without causing any disruption to production systems
- Enables staff to better understand their individual roles and responsibilities
- Facilitate better coordination
- Help to inform decision-making

VIRTUAL

- In April and June of 2022, we ran two exercises in collaboration with NUARI
- Participants played via the DECIDE platform which utilized email and chat functions to drive the scenario and injects
- Post-Exercise, participants were given an After-Action Report which emphasized observations at the group level and offered recommendations

IN-PERSON

- On November 9th, 2022, we hosted a tabletop exercise on the campus of Texas A&M
- Over 40 participants across dozens of utilities engaged in a progressively unfolding cyber incident scenario consisting of a phishing and ransomware attack
- Post-Exercise, an After-Action Report, which provided in-depth coverage of the scenario and questions, was circulated to participants

Biennial Cybersecurity Summits

RED TEAM-BLUE TEAM EXERCISES

As part of the October 2024 2nd Biennial Cybersecurity Summit, a Red Team-Blue Team exercise was executed.

Red Team players were given access to their own Virtual Machine where they identified, analyzed, and hacked into as many systems as possible.

Blue Team players were tasked with determining how the systems were compromised, where the attacks came from, and what sensitive or proprietary information was taken. Participants also removed malware, backdoors, and persistence mechanisms left by the intruders.

INCIDENT RESPONSE TRAINING

During the Cybersecurity Summit, non-technical participants engaged in a Community Cybersecurity Preparedness Simulation course (MTG-301).

Developed by National Cybersecurity Preparedness Consortium, the course utilizes a gamified approach to augmenting Incidence Response where participants strategize with a diverse group of stakeholders to plan for and respond to a cybersecurity incident that could have cascading effects across a community.

The course is designed to assist leaders and managers with cybersecurity preparedness.

COLLABORATING WITH PUBLIC UNIVERSITIES

We partner with Texas public universities which serve as host sites for our Cybersecurity Summits. These institutions provide the space, technology, and expertise needed to make the events successful. Their cybersecurity programs offer valuable resources, including research, simulation environments, and expert-led workshops, giving utilities a chance to learn from both academic and industry leaders.

Participant Feedback

Program Feedback

"Learn about real world attacks and how to defend against them"

"Understand government agencies and their overlapping roles"

Tabletop Feedback

"Objectives and scenarios were realistic and applicable to what we do"

"The training was very good and always an important item to practice on a regular basis"

Self-Assessment Feedback

"Useful and easy to understand"

"The information received improved my understanding of best practices and available resources"

Texas Cybersecurity Monitor Team

TERENCE GILL

Project Manager/Business Analyst (PM/BA)

Prior experience includes: Banking, Insurance, and Information Technology

ROGER SIMMONS

Cybersecurity Subject Matter Expert (CSME)

Prior experience includes: Cooperative Utility, Department of Defense, State Government, Healthcare and Cloud Software

Paragon Systems is a subsidiary of SCIS (Securitas Critical Infrastructure Services, Inc.) with over 12,000 professionals specializing in security, fire, emergency response, investigations, inspections, cybersecurity, and mission support services to the US Federal Government and other critical infrastructure clients. Paragon Energy is the longest running specialized nuclear security provider in the industry with current contracts at operating and decommissioned plants across the country. Our clients are some of the largest utilities in the country, including Entergy, First Energy, Honeywell, and Duke Energy.

PARAGON
SYSTEMS

STAY INFORMED, STAY SECURE.

Connect with us for more details on the Cybersecurity Outreach Program.

🌐 www.parasys.com/cybermonitor ✉ TXCSM@parasys.com