

NRECA Cybersecurity Update

AMEC-ITA Annual Meeting 2024

AGENDA

- **Introductions\Program Overview**
- **NRECA Threat Analysis Center**
- **NRECA Co-op Cyber Goals**
- **Co-op Cyber Tech**
- **Cyber Risk Quantification Pilot**
- **Federal Funding**
 - ICS-REC
 - TICCC-TAC\SPARK Update
 - Project Guardian 617A
- **Government Relations Update**

THE NRECA CYBERSECURITY TEAM

Business and Technology Strategies (BTS)



Carter Manucy
Director, Cybersecurity
NRECA



Justin Luebbert
Principal, Cybersecurity
NRECA



Meredith Miller
Principal Data Scientist, Cybersecurity
NRECA



Ryan Newlon
Principal, Cybersecurity
NRECA



Adrian McNamara
Program Manager for Outreach
and Cloud Security
NRECA

NRECA'S CYBERSECURITY PROGRAM

Solutions Development Efforts

- Help Cooperatives Establish Fundamental Cybersecurity Measures
- Improve Incident Response & Resilience to Events
- Grow Co-op and Industry Collaboration
- Improve Workforce Development and Training Efforts
- Help Cooperatives take advantage of Federal Funding

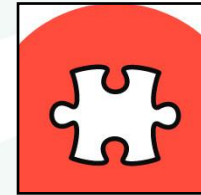
Tools, Technology and Program Efforts

- NRECA Co-op Cyber Goals Program, NRECA Threat Analysis Center
- Co-op Cyber Tech Conference, Conduct National Tabletop Exercises
- Additional Federal Funding Programs and Research Efforts
 - Project Guardian 617A, TICCC-TAC\SPARK, ICS-REC, RC3 (Legacy)

Outreach, Awareness & Advisory Services

- Webinars, Guidebooks, Speaking Engagements
- Government & Industry Partnerships

Guiding Principles



Autonomy & Independence



Education, Training & Information



Cooperation Among Cooperatives



Concern for Community

CYBERSECURITY MEMBER ADVISORY GROUP (CS MAG)

Mission Statement: The primary mission of the Cybersecurity Member Advisory Group is to advance the cybersecurity capabilities of NRECA's members through research, development, and education.

- Consist of about 20 personnel from NRECA member cooperatives interested in cyber efforts and initiatives
 - Identify, evaluate, and help prioritize NRECA cybersecurity research and development efforts.
 - Provide feedback on research projects and ideas
 - [Cybersecurity Members Advisory Group Information](#)

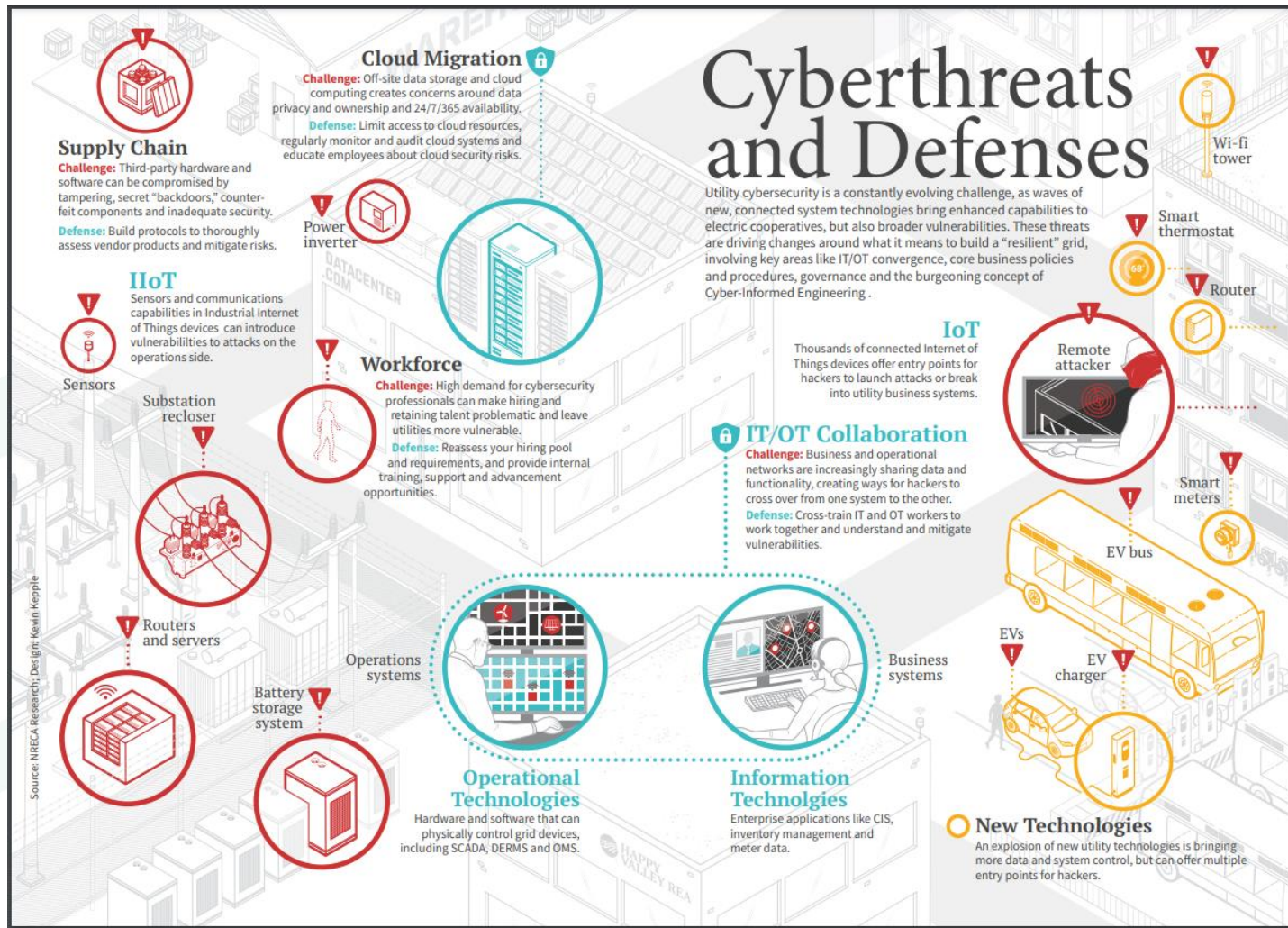
“OUR MEMBERS' OPINIONS MATTER”

NRECA's Cybersecurity Member Advisory Group was in town this week to discuss cybersecurity issues and advocate for electric cooperatives. They were able to engage with Members of Congress and federal partners from DOE, CISA, and DOD on their efforts to provide safe, reliable, and secure electricity to co-op communities.



THREAT LANDSCAPE OVERVIEW

INCREASING THREATS & CHALLENGES



MIGRATION TO THE CLOUD
Data Privacy, Data Ownership, Contracts, Connectivity Implications

IT/OT COLLABORATION
Increasing Threats & Landscape, IT and OT Teams must work together on overall security strategy

WORKFORCE
Job Shortage, Aging Infrastructure, Challenges with hiring and retaining talent

DISTRIBUTED ENERGY RESOURCES
Growth of DERs: rooftop solar, wind, battery storage, and electric vehicles.

SUPPLY CHAIN
Vendor Attacks, Vendor Vetting

NRECA Threat Analysis Center

A Technology and Community for Co-ops

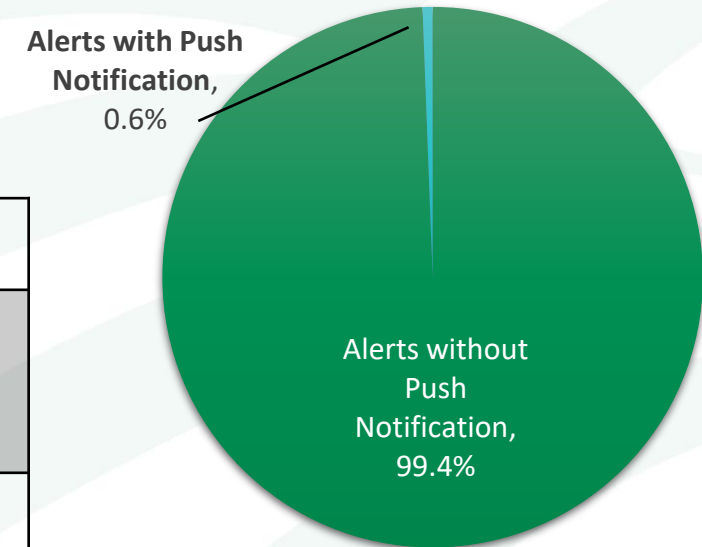


THE NRECA THREAT ANALYSIS CENTER (TAC)

Vision: TAC is a **technology and community** that enables Co-ops to focus on the cyber threats that matter, respond quickly with the necessary expertise, and engage with the broader intelligence community without sacrificing privacy.

Problem	Solution
Alert Fatigue	Threats enriched, tagged, and prioritized by relevancy to the Co-op, to allow each co-op to focus on the alerts and information that is most relevant to them.
Cyber Expertise	Establish a platform for centralized expertise and peer-to-peer assistance, with the necessary tools for alert enrichment and event triage.
Communication	Threat intelligence shared by cooperatives is aggregated, deidentified, and shared with the cooperative community and to external reporting agencies. The platform includes messaging and other tools that enable cooperatives to communicate and collaborate with each other.

Alerts in Last 3 Months



Over the last 12 months:

- > 3,000 alerts total
- 90 unique vendors tagged to alerts
- 2,700 alerts with associated vendor tags



Threat Analysis Center (TAC) addresses deficiencies in the ***threat detection, communication, and response pipeline.***

TAC Integrated Communication

E-ISAC

- NRECA & E-ISAC have finalized an MOU detailing coordination and collaboration efforts.
- TAC & E-ISAC are now integrated with backend data feeds for automated bi-directional threat alerting

Press Release



FOR IMMEDIATE RELEASE
May 28, 2024

Contact: Dan Riedinger | 202-403-7517
electric.coop | @NRECAnews

NRECA Signs MOU with Electricity Information Sharing and Analysis Center to Bolster Cybersecurity Collaboration

ARLINGTON, Va. – The National Rural Electric Cooperative Association has signed an agreement with the North American Electric Reliability Corporation's Electricity Information Sharing and Analysis Center to enhance electric sector cybersecurity through increased information sharing and collaboration. The memorandum of understanding prioritizes the sharing of intelligence about security threats, vulnerabilities and cyber incidents through heightened coordination between the E-ISAC and NRECA's Threat Analysis Center. "Electric sector cybersecurity challenges and threats are increasingly complex and require seamless coordination between industry partners," NRECA CEO Jim Matheson said. "This MOU will facilitate enhanced collaboration



CISA

- TAC has finalized an automated bi-directional data feed with CISA

Private Industry Feeds

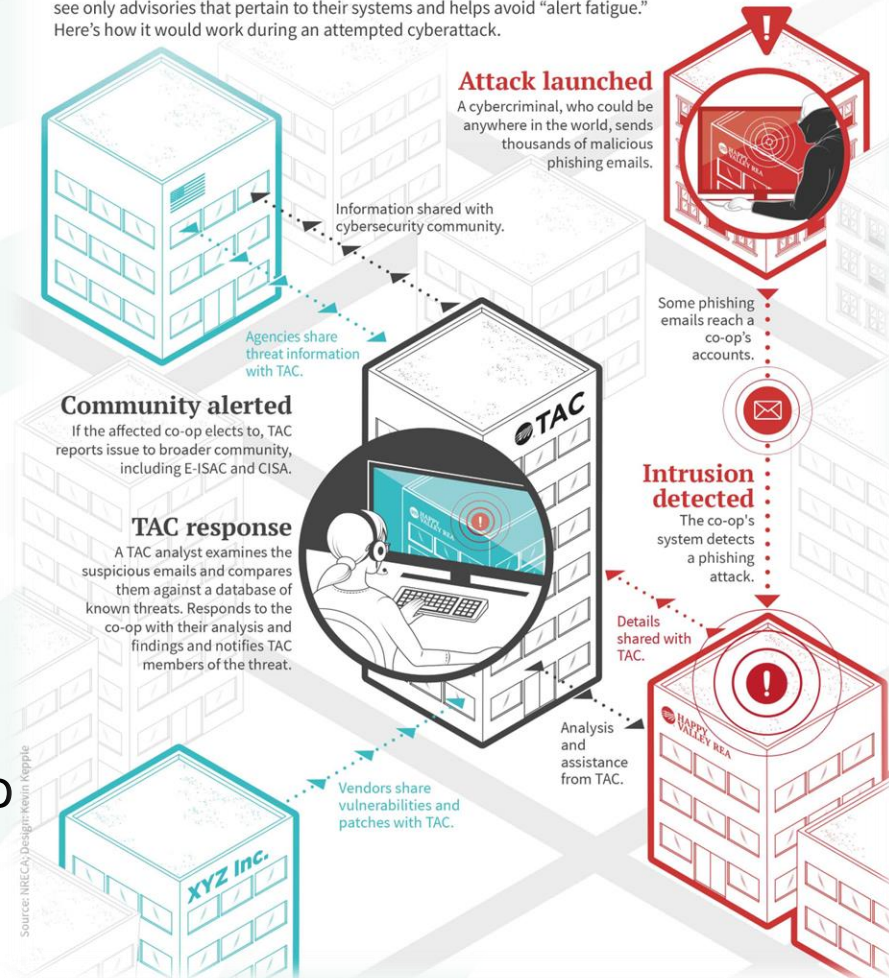
- Federated vulnerability scan aggregated results
- Proprietary threat intelligence feeds.

Member Cooperatives

- STIX/TAXII feed to member utilities for automatic ingest into TIP/SIEM tools.

What Is the TAC?

The NRECA Research Threat Analysis Center was created to serve as a one-stop shop for electric cooperatives to learn what cybersecurity threats are out there, which systems could be affected and how to mitigate those threats. It can also help co-ops respond to suspicious activity and acts as a conduit to share information with the broader cybersecurity community. A dashboard with filters allows co-ops to see only advisories that pertain to their systems and helps avoid "alert fatigue." Here's how it would work during an attempted cyberattack.



What is the Threat Analysis Center (TAC)?



Subscribe



Alerts



Portal Resources



Collaboration

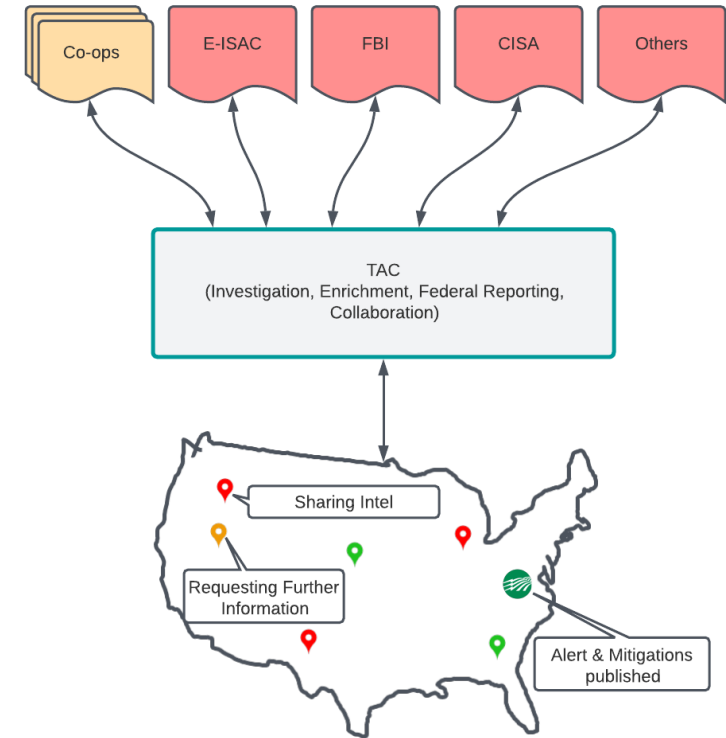
Customizable Alert Inbox	Modern interface with a customizable Alert Inbox that aggregates public, private, and industry-specific threat feeds into a unified repository, with fine-grained filters and search features.
Custom Alert Channels & Notification Settings	Reduce alert fatigue by tuning your settings for platform, email, and mobile app notifications with alert categories and custom channels that filter using an extensive tag library.
Secure Messenger	In-platform messenger provides direct communication within and between cooperatives, broken into Alert-specific channels, custom group threads, 1-to-1 messages, and topic-based conversations.
Knowledge Hub & Document Library	Cybersecurity resources disseminated to the community through a secure Knowledge Hub and Document Library. Cooperatives have a private space within the Document Library for their own resources.
Threat Defender Library	TAC analysts provide and cooperatives can share threat defense and detection artifacts for common network security tools through a central repository.
Centralized Reporting & Community Alerting	Intelligence shared with the TAC will be investigated, enriched, and aggregated with other similar intelligence to alert the cooperative community and submit to reporting agencies.
Event Calendar	Unified calendar for cybersecurity events and training opportunities. TAC users can submit their own events to have them listed on the calendar and invite the community.

TAC Workforce Development Vision

The TAC is a ***Technology Platform*** that empowers ***People***

Vision/Roadmap for TAC staff:

- Full-time, dedicated analysts and portions of time from Co-op cybersecurity professionals
- TAC/Co-op staff will be cross-trained on TAC, their “home” co-op systems, neighboring co-op systems, and on the power system in general to build a network of cyber mutual assistance personnel.
- Small Co-ops can rely on a network of professionals to meet some of their cybersecurity personnel goals.
- And ultimately: The TAC is largely run of, by, and for the Co-ops.



Growing TAC Through Federal Funding

NRECA Federal Funding Program Efforts & Roadmap

ICS-REC OT Monitoring

- NRECA is working with DOE under a cooperative agreement to deploy cyber and cyber-physical solutions for rural electric cooperatives that will provide cyber visibility, detection, and response capabilities for industrial control systems (ICS).

Project Guardian 617A

- A five-year cooperative agreement with DOE based on the idea that our rural utilities (Guardians), working together, can guard against cybersecurity threats. Project Guardian 617A will help develop TAC Content Expansion, including incident response templates, supply chain resources, and crisis communications guidelines.

TICCC-TAC

- NRECA Research submitted a pre-application for federal funding to cover platform costs, called Trusted Industrial Control Cybersecurity Community – Threat Analysis Center (TICCC-TAC). DOE has invited NRECA Research to move forward to the Full Application phase with this project.

Current Status

Cooperatives can join TAC for 2024 beta testing (extended through Q1 2025): www.cooperative.com/tac

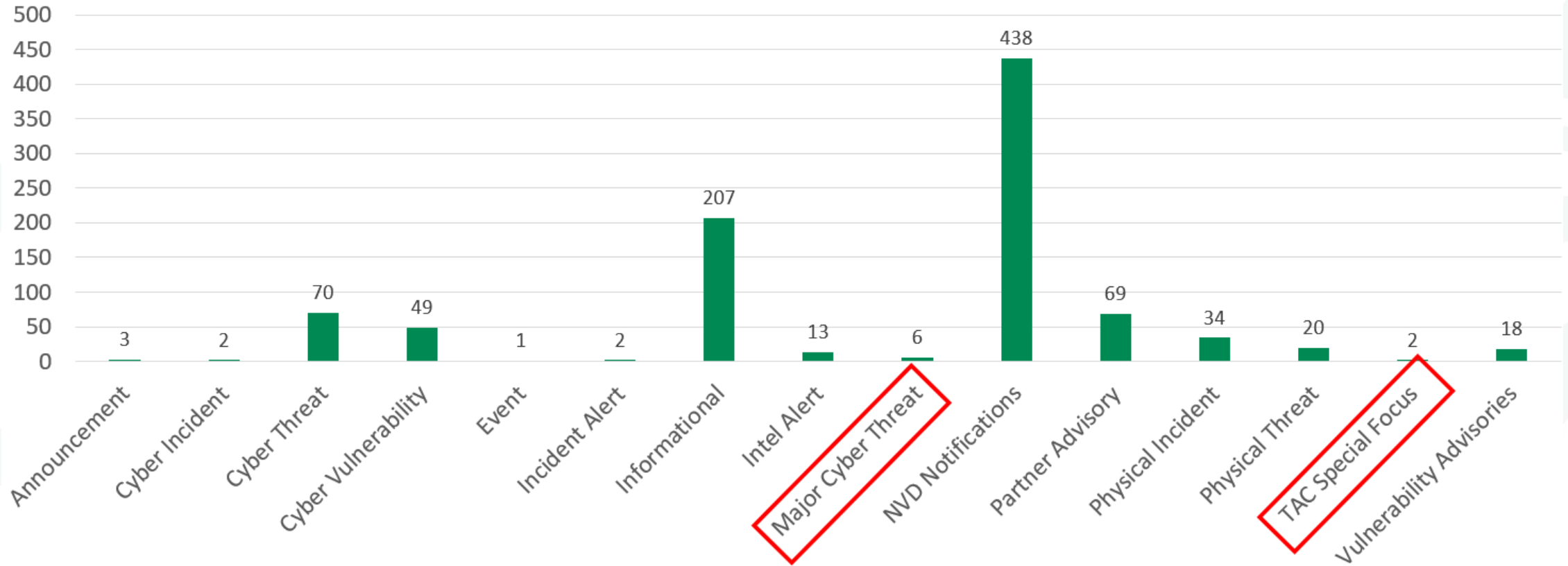
- No cost until Q2 2025
- Subscription pricing to be published shortly
- TIOCCC-TAC participating utilities will receive significant discount

Current Member Cooperatives Enrolled

155+

Threat Briefing Overview

Alerts by Category: Sept 19 – Nov 19 (2024)



Threat Briefing

Commonalities & Recommendations

- **Major Cyber Threats**

- FortiJump and FortiJump Higher
- Akira Ransomware
- Vishing Events In Electric Sector
- Volt/Salt Typhoon

- **TAC Special Focus**

- TAC Special Focus: Multi-factor Authentication
- Rise in the Abuse of Security Appliances: Cisco, Fortinet, Palo Alto

- **Common Threads**

- IT pivots to OT
- Edge Devices are a target

- **Common Mitigations and Remediations**

- Multi-factor Authentication
- Publicly Accessible Management Interfaces

NRECA Co-op Cyber Goal Program

Establishing a baseline of co-op cybersecurity



NRECA CO-OP CYBER GOALS PROGRAM

- The Co-op Cyber Goals Program is comprised of cybersecurity goals aimed at helping co-ops work toward achieving high priority security measures and creating a benchmark to help establish basic cybersecurity fundamentals are in place.

Objectives

- Launched Level 1 Goals in January 2023 at CEO Closeup
- Launched Level 2 Goals in June 2024 at Co-op Cyber Tech Conference
- Considerations: Goals tailored to co-ops, Cyber Insurance, DHS CISA Cyber Performance Goals, RC3 Self-Assessment
- Co-op Recognition, Physical Coin and Digital Badge, Co-op Cyber Tech
- Member feedback upon goal completion: Utilize program metrics to understand where co-ops are struggling related to size and need additional guidance or resources when completing goals. Drives future initiatives.
- **Self-paced and self-administered program**
- The program highlights to industry and government that co-ops are being proactive across the country in the cybersecurity space.



Digital Badge



Completion Coin



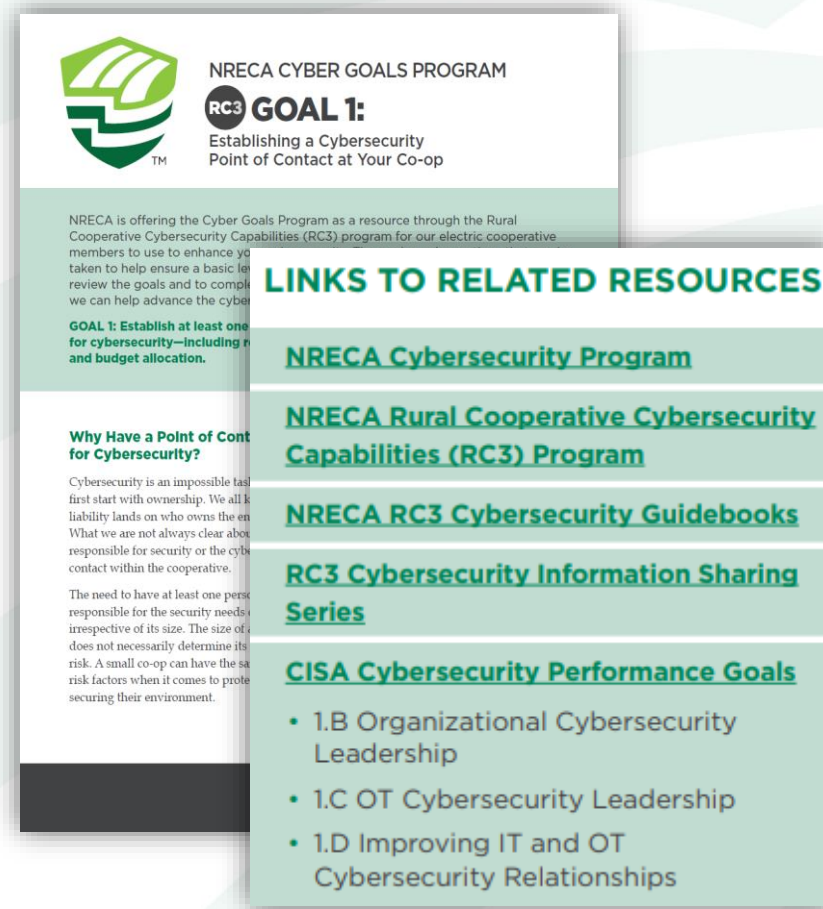
2024 Co-op Cyber Tech Recognition

NRECA CO-OP CYBER GOALS PROGRAM

Level 1 Cyber Goals

- Goal 1 - Cyber Point of Contact
- Goal 2 - Self-Assessment
- Goal 3 - Contract Review
- Goal 4 - Multi-Factor Authentication
- Goal 5 - Default Password Policy
- Goal 6 - Leadership Training
- Goal 7 - Employee Training
- Goal 8 - IT\OT Segmentation
- Goal 9 - Cyber Incident Response Plan
- Goal 10 - Backups

Example Goal Summary & Resources



The image shows a document titled "NRECA CYBER GOALS PROGRAM" with a green logo. It details "GOAL 1: Establishing a Cybersecurity Point of Contact at Your Co-op". The text explains that NRECA offers this program as a resource through the Rural Cooperative Cybersecurity Capabilities (RC3) program. It includes a section titled "GOAL 1: Establish at least one for cybersecurity—including n and budget allocation." and another titled "Why Have a Point of Contact for Cybersecurity?" which discusses the importance of having a designated person responsible for security. A list of "LINKS TO RELATED RESOURCES" is provided, including:

- [NRECA Cybersecurity Program](#)
- [NRECA Rural Cooperative Cybersecurity Capabilities \(RC3\) Program](#)
- [NRECA RC3 Cybersecurity Guidebooks](#)
- [RC3 Cybersecurity Information Sharing Series](#)
- [CISA Cybersecurity Performance Goals](#)

The CISA link is followed by a bulleted list:

- 1.B Organizational Cybersecurity Leadership
- 1.C OT Cybersecurity Leadership
- 1.D Improving IT and OT Cybersecurity Relationships



Level 1 Coin

GOAL 6: LEADERSHIP TRAINING

Summary: Leadership Training: Board of Directors should be appropriately educated and trained on cybersecurity.

Setting the “Tone at the Top”

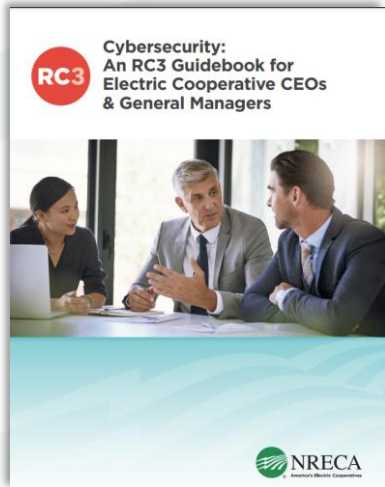
Top-Down Approach
Cybersecurity Culture

Cyber Risk Strategy Board
and CEO level.

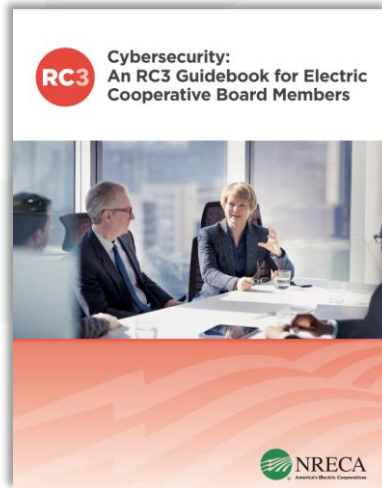
Cyber Risk

- Operational risk, financial risk, reputational risk.
- Legal Implications
- Cyber Insurance
- Business Continuity
- Incident Response Planning

Does the board allocate funds in the budget for cybersecurity resources and training?



CEO Guidebook
(NRECA RESOURCE)



Board Guidebook
(NRECA RESOURCE)

Additional NRECA Cybersecurity Guidebooks

- Cooperative Attorneys
- *Guidebook for Human Resources Staff*

NRECA Directors
Security Course

Cybersecurity: The Board’s
Oversight Role

Board Guidebook: Chapter 2: Risk Assessment and Management
“What is the Board’s Sphere of Cyber Responsibility”

NRECA CO-OP CYBER GOALS PROGRAM

Level 2 Cyber Goals

- Goal 11 - Separate User Accounts and Permissions
- Goal 12 - Asset Inventory
- Goal 13 - Logging
- Goal 14 - Internet-Facing Systems
- Goal 15 - Business Continuity Plans
- Goal 16 – Information Sharing
- Goal 17 – Endpoint Security
- Goal 18 - Unique Passwords
- Goal 19 - Network Topology
- Goal 20 - Unauthorized Devices

Example Goal Summary & Resources



NRECA CO-OP CYBER GOALS PROGRAM
GOAL 11:
Separate User Accounts and Permissions
(Version 2.0)

NRECA is offering the Co-op Cyber Goals Program as a resource through our Cybersecurity Program for our electric cooperative members to use to enhance your cybersecurity. The goals are fundamental actions that can be taken to help establish a basic level of cybersecurity. We encourage all co-ops to review the goals and to complete any not yet in place within your organization. Together, we can help advance the cybersecurity posture of our nation's electricity grid.

Note: The goals in this program are of equal importance. They do not need to be considered in any certain order. The numbering is solely for identifying them in the Co-op Cyber Goals Program.

Goal 11 – Create and Maintain Separate User Accounts and Permissions

Prevent Unauthorized Access by Managing Sensitive Accounts
Managing user accounts and permissions is a core aspect of cybersecurity. If a malicious actor gains access to an employee's user account, they will have the same rights and access that the employee does. For this reason, it is vitally important to structure user accounts and privileges to limit the damage that can be caused by a single compromised account.

User accounts fall into two broad categories:

- **Standard User Accounts:** These are used for everyday tasks such as email and timecards. Every employee accessing your network needs a unique user account.
- **Administrator-Level (Privileged) Accounts:** These accounts have elevated access and rights to manage computer systems. This allows for changing security settings, accessing sensitive information, and creating or deleting other user accounts. IT staff often have one or more administrator-level accounts in addition to their standard user accounts for normal business functions.

To minimize risk, restrict administrator accounts to as few employees as possible and use these accounts only for necessary tasks. Administrator-level accounts should not be used for activities like accessing emails and browsing the internet, as these increase exposure to malicious activity. A compromised administrator account can give an attacker access to sensitive or operational assets.

Avoid Shared Administrator Accounts
Given the complexity of managing accounts and limited IT staff, it may seem easier to create a single administrator-level account shared by multiple users. However, this approach is risky. If the shared account is compromised, identifying the source of the breach becomes difficult. Additionally, if an

Conduct Ongoing Account Maintenance
Because staff and job roles change over time, establish a procedure or policy to periodically review – preferably once every six months – the privileges assigned to each account to make sure they match that user's current job responsibilities. Remove accounts and privileges that are no longer necessary, including disabling and/or removing accounts as individuals leave or retire from the organization. Creating groups based on job roles with permissions set based on group membership helps tremendously with account maintenance, but can complicate smaller systems.

LINKS TO RELATED RESOURCES

[NRECA Cybersecurity Program](#)
[NRECA Rural Cooperative Cybersecurity Checklist \(RCCS\) Version 1.0](#)
[Questions within the RCCS Self-Assessment that align with this goal.](#)
[DOI 5748](#)

Related Co-op Cyber Goals
Goal 4: Multi-Factor Authentication
Goal 5: Default Password Policy
Goal 13: Log Files
Goal 18: Unique Passwords

[Cybersecurity Checklist: Monthly Model \(CCTM\) v1.0](#)
ACCESS-1a, ACCESS-1b, ACCESS-1c, ACCESS-1d, ACCESS-1e, ACCESS-1f, ACCESS-1g, ACCESS-1h

CISA Cybersecurity Performance Goals
2.0 Unique Credentials
2.0 Revoking Credentials for Departing Employees
2.2 Separating User and Privileged Accounts

[NIST Cybersecurity Framework \(CSF\) v1.0](#)
PR.AA-01, PR.AA-02, PR.AA-05, PR.AA-07, PR.AA-08

[Center for Internet Security \(CIS\) Controls, v4](#)
3.3, 4.7, 5.1, 5.3, 5.4, 5.5, 6.1, 6.2, 6.6, 6.8

LEVEL TWO GOAL
NRECA
America's Electric Cooperatives
membersecurity@nreca.coop



Level 2 Coin

Co-ops Participating in the Cyber Goals Program for Level One Automatically Have Access to Level Two

WHY SHOULD YOUR CO-OP PARTICIPATE

- Advances your co-op's cybersecurity posture with specific recommended measures
- Helps create a culture of cybersecurity at the co-op
 - Top-down and bottom-up approach
- Provides clear initiative to gain support across your organization
- Helps to prioritize cyber tasks and enhance decision-making skills
- Guides co-op staff to work collaboratively in improving the co-op's security maturity
- Shows measurable progress to motivate employees
- Provides you the means to publicize your achievement to support consumer-member confidence
- Documents demonstrated effort by co-ops to advance the cybersecurity of our electric grid
- Help avoid or reduce regulations by showing cooperatives are being proactive.

LATEST PROGRAM DEVELOPMENTS

- **"Level 2" (Goals 11-20) to advance maturity**
- Expanded resource lists that include cross-references to additional industry frameworks, Level One Goals and other NRECA Resources
- Opportunity to volunteer to help other co-ops with specific goals
- Improved feedback mechanism and voice for cooperatives
 - Expanded Participant Survey Questions
 - Challenges/barriers with the goal
 - Tools (software, etc.) used to complete the goal
 - Enables NRECA to measure impact of Federally funded programs.
 - Helps NRECA communicate co-ops' cybersecurity progress to policymakers.
 - Provide NRECA with direction on where to build programming.
 - Alerts the Program Team of challenges faced by multiple co-ops so that new resources can be developed to target the highest priority needs.

LINKS TO RELATED RESOURCES

[NRECA Cybersecurity Program](#)

[NRECA Rural Cooperative Cybersecurity Capabilities \(RC3\) Program](#)

[Questions within the RC3 Self-Assessment that align with this goal:](#)
IDE 57-58

[Related Co-op Cyber Goals](#)

Goal 4: Multi-Factor Authentication

Goal 5: Default Password Policy

Goal 13: Log Files

Goal 18: Unique Passwords

[Cybersecurity Capability Maturity Model \(C2M2\) v2.1](#)

ACCESS-1a, ACCESS-1b, ACCESS-1c, ACCESS-1e, ACCESS-1f, ACCESS-1h, ACCESS-1j

[CISA Cybersecurity Performance Goals](#)

2.C Unique Credentials

2.D Revoking Credentials for Departing Employees

2.E Separating User and Privileged Accounts

[NIST Cybersecurity Framework \(CSF\) v2.0](#)

PR.AA-01, PR.AA-02, PR.AA-05, PR.AT-02

[Center for Internet Security \(CIS\) Controls, v8](#)

3.3, 4.7, 5.1, 5.3, 5.4, 5.5, 6.1, 6.2, 6.6, 6.8

CYBER GOALS SUMMARY ADVISORY

- Year 2 Summary “Coming Soon”
- Highlights National and Regional Recognition
 - NRECA Co-op Cyber Goals recognized as Cybersecurity Assessment Tool in RMUC ACT 1 Prize

Co-op Cyber Goals Program: First Year Summary

In January 2023, NRECA launched the [Co-op Cyber Goals Program](#) to help co-ops improve cybersecurity. This first phase of the voluntary program included 10 basic, actionable goals for NRECA members to complete individually, at their own pace, and in any order. NRECA member participation in the program underscores to both industry and government that cooperatives of all sizes nationwide are taking proactive steps in cybersecurity. After a successful first year, the program will offer additional opportunities for co-ops to advance their cybersecurity postures in 2024 with 10 new goals.

Program accomplishments from January 2023 through January 2024 include:

- 292 NRECA members registered to participate.
- 58 participants completed all 10 goals.
- In total, participants completed 1,561 goals.
- The U.S. Department of Energy (DOE) mentioned the program in its Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology (ACT) 1 Prize literature.



Program website:
www.cooperative.com/cybergoalsprogram

Program Overview

NRECA's Co-op Cyber Goals are high-priority, fundamental cybersecurity measures intended to help co-ops establish solid foundations that future cybersecurity efforts can build upon. The program team selected goals from industry-standard cybersecurity performance goals.

- | | |
|--|--------------------------------------|
| Goal 1: Establish a Cybersecurity Point of Contact | Goal 6: Leadership Training |
| Goal 2: Self-Assessment | Goal 7: Employee Training |
| Goal 3: Contract Review | Goal 8: IT/OT Segmentation |
| Goal 4: Multi-Factor Authentication (MFA) | Goal 9: Cyber Incident Response Plan |
| Goal 5: Default Password Policy | Goal 10: Data Backups |

Participants registered for the program, accessed descriptions and resources for each goal, and tracked their progress on each goal through a secure, private online registration system. Participants were also encouraged to provide feedback on the goals, including tools used, challenges, and recommendations for other co-ops. The program team will share these insights to help more co-ops participate and progress in the program.

National and Regional Recognition

During its first year, the program received national and regional attention. The U.S. DOE named this program, along with NRECA's RC3 Self-Assessment and others, in its RMUC ACT 1 Prize rules, as a cybersecurity assessment tool that could be used in the application.

NRECA CO-OP CYBER GOALS PROGRAM



43

Number of States Participating



420+

Current Co-ops Participating

14 Missouri Co-ops Participating



115+

Completed Level
One Goals

THANK YOU FOR PARTICIPATING

- Participation in the NRECA Cyber Goals program highlights to industry and government that co-ops are being proactive across the country in the cybersecurity space.
- We are making progress and utilizing metrics to measure our successes.

DON'T FORGET TO UPDATE YOUR GOAL PROGRESS

Join the Co-op Cyber Goals Program

COOPERATIVE.COM

[Sign Up Link](#)

- The goal of this conference is to build a community of cyber practitioners specific to the cooperative space, with professional development and innovative approaches for collaboration built into the program.
- Coop participants will take home the skillset needed to optimize and improve their existing or emerging cyber security programs. Attendees will get to network with top security experts and build lasting relationships with both industry experts and peers.



Photo Credit: Denny Gainer/NRECA

Keynote Speaker CISA Executive Director Wales



2024 Highlights

- Over 450 Attendees
- Attendees from 40 states represented
- Focus on Engagement and Interaction
 - Peer-to-Peer
 - Industry-to-Peer
- IT\OT Collaboration
- Technical Training
- Brian Krebs (Krebs on Security)

Focused tracks on

- Co-ops
- Government
- Vendors
- NRECA

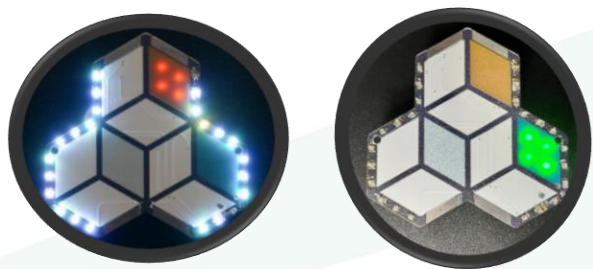


[Co-op Cyber Tech Webpage](#)

NRECA CO-OP CYBER TECH

#COOPCYBERTECH 2024 Highlights

DIGITAL INTERACTIVE BADGES



#BADGELIFE

SOLDERING STATION



INL ESCAPE ROOM



Photo Credit: Beatty Gainer/NRECA

CAPTURE THE FLAG EVENT (CTF)

1. Main Entrance



Play 'Capture the Flag' and solve a series of cyber challenges with our interactive badges.

CS-MAG: TABLETOP PRE-CON



'Tabletop Exercise Card Game' to improve incident response.

SCIENCE FAIR

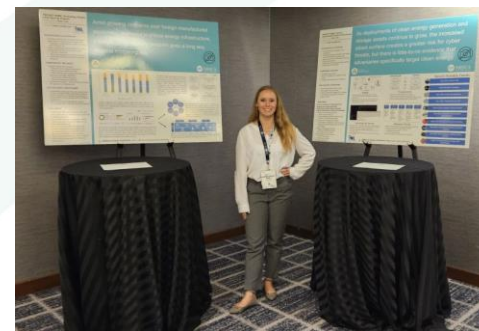


Photo Credit



MARK YOUR CALENDAR

2025 Co-op Cyber Tech: June 24-26, Denver, Colorado

CYBER MUTUAL ASSISTANCE (CMA)

The ESCC's Cyber Mutual Assistance Program



Cyber Defense: Building on the Industry's Culture of Mutual Aid

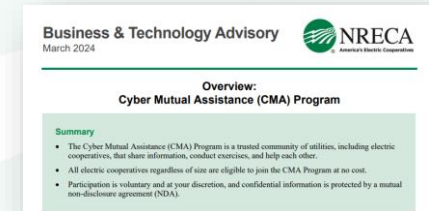
- The Cyber Mutual Assistance (CMA) Program is a trusted community of utilities, including electric cooperatives, that share information, conduct exercises, and help each other.
- All electric cooperatives, regardless of size, are eligible to join the CMA Program at no cost.
- Participation is voluntary and at your discretion, and confidential information is protected by a mutual non-disclosure agreement (NDA).

Why should your cooperative join the CMA?

- More than Cyber Mutual Assistance
- Sharing best practices
- Provides value both left and right of an incident
- Networking & Engagement
- Learning Opportunities: Watercooler Discussions
- Virtual and In-Person Meetings Opportunities
- Broader Industry Engagement
- NDA Assurances

Joining the CMA Program

- Voluntary Participation
- No Cost to Join
- Designate CMA Coordinator at your Cooperative
- **Proxy Participation**
- Sign a Non-Disclosure Agreement (NDA)



[Cyber Mutual Assistance Program Link](#)

CYBER RISK QUANTIFICATION PILOT

What is this pilot all about?

- Providing a financial quantification of risk that can be translated back to the co-op Cyber Goals
- Understanding what risks to prioritize based on financial risk
- Example: Your cooperative shows a \$1M overall financial risk, but if you implement NRECA Cyber Goals 1-10, that drops to \$250K.
- Possible opportunities to benchmark against other cooperatives.
- NRECA (with permission) can use this data to show impact to DOE for our other programs.



Federal Infrastructure Cybersecurity Funding

Helping co-ops improve cybersecurity thru federal funding

ICS-REC: Cyber Protection of Industrial Control Systems

In November 2022, NRECA was awarded \$15M from the Department of Energy (DOE) to help our member electric cooperatives deploy industrial control system monitoring technologies that will provide cyber visibility, detection, and response capabilities of their industrial control facilities.

- 3-Year Program

Current Status: NRECA is currently working with co-op members to deploy OT monitoring and detection technologies

- Co-op Member Working Group
- ICS-REC Dedicated Portal and Resources
- OT Monitoring Tools Vendor Matrix
- Continuing to add new OT vendor resources

NRECA is technology-agnostic

New Updated Eligibility: Previous requirements such as number of meters have now been removed, and any cooperative that has operational technology (SCADA System) may join the ICS-REC Program to take advantage of the potential funding to deploy technologies that protect, defend or harden their Operational Technology (OT) environment.



[Click here to learn more](#) or email ICS-REC@nreca.coop



**Are you considering deploying OT technologies?
Be sure to express interest now!**

Infrastructure Funding Efforts

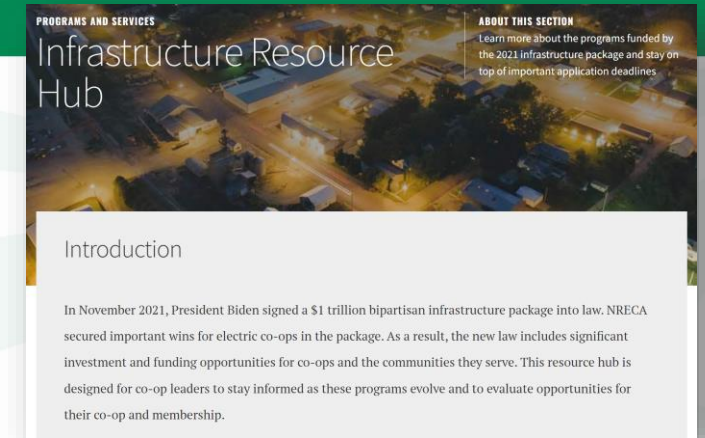
NRECA-Wide Priority

President Biden signed a \$1.2 trillion bipartisan infrastructure package into law.

The **Bipartisan Infrastructure Law (BIL)** includes significant investment and funding opportunities for co-ops (and the communities they serve).

NRECA has identified over **30 programs** that co-ops will be eligible to participate in

- **NRECA Infrastructure Hub:** NRECA has created a resource hub designed to educate and inform members of the new programs as they evolve and to give our members a “one stop shop” to help them evaluate BIL opportunities.



www.cooperative.com



CYBER AND
PHYSICAL
SECURITY



ELECTRIC
VEHICLES



MICROGRID

NATURAL
HAZARDS

SMART GRIDS
AND DATA

Featured Resources

Infrastructure Bill Funding Guidebook

This comprehensive guidebook provides NRECA members with an overview of the bipartisan infrastructure law and information on how they can prepare to secure funding.

DOWNLOAD PDF

Grant Writing Assistance Request

NRECA has coordinated grant writing resources that members may use in support of their applications for federal infrastructure funding opportunities.

SEE QUESTIONNAIRE

[Infrastructure Resource Hub Link](#)

[Funding Opportunities Link](#)

CYBER & PHYSICAL SECURITY CONSORTIUM

Federal Programs:

DHS - \$1B for state and local cyber grant program

DOE - \$250M for grant and technical assistance, and deployment

Funding Opportunities:

Direct funding opportunities for coops or coalitions of coops

Training, RD&D opportunities for NRECA.

Focus on essential security upgrades, people, and process programs

- Create, test, and deploy cyber tools, including self-assessment, vulnerability testing, information sharing, and anomaly detection tools. Cyber security education, training materials, and information sharing focus.

Join the Cyber and Physical Security Consortium Professional Communities



Mission: The Cyber and Physical Security consortium is a coalition of the nation's rural electric cooperatives seeking to develop and maintain a well-rounded cyber and physical security posture for their cooperative. The consortium will partner with federal, state and local stakeholders to identify funding opportunities and develop replicable pathways for advanced cyber and physical security deployment at electric cooperatives.

Click [here](#) to join the NRECA Cyber and Physical Security Consortium for the latest updates.



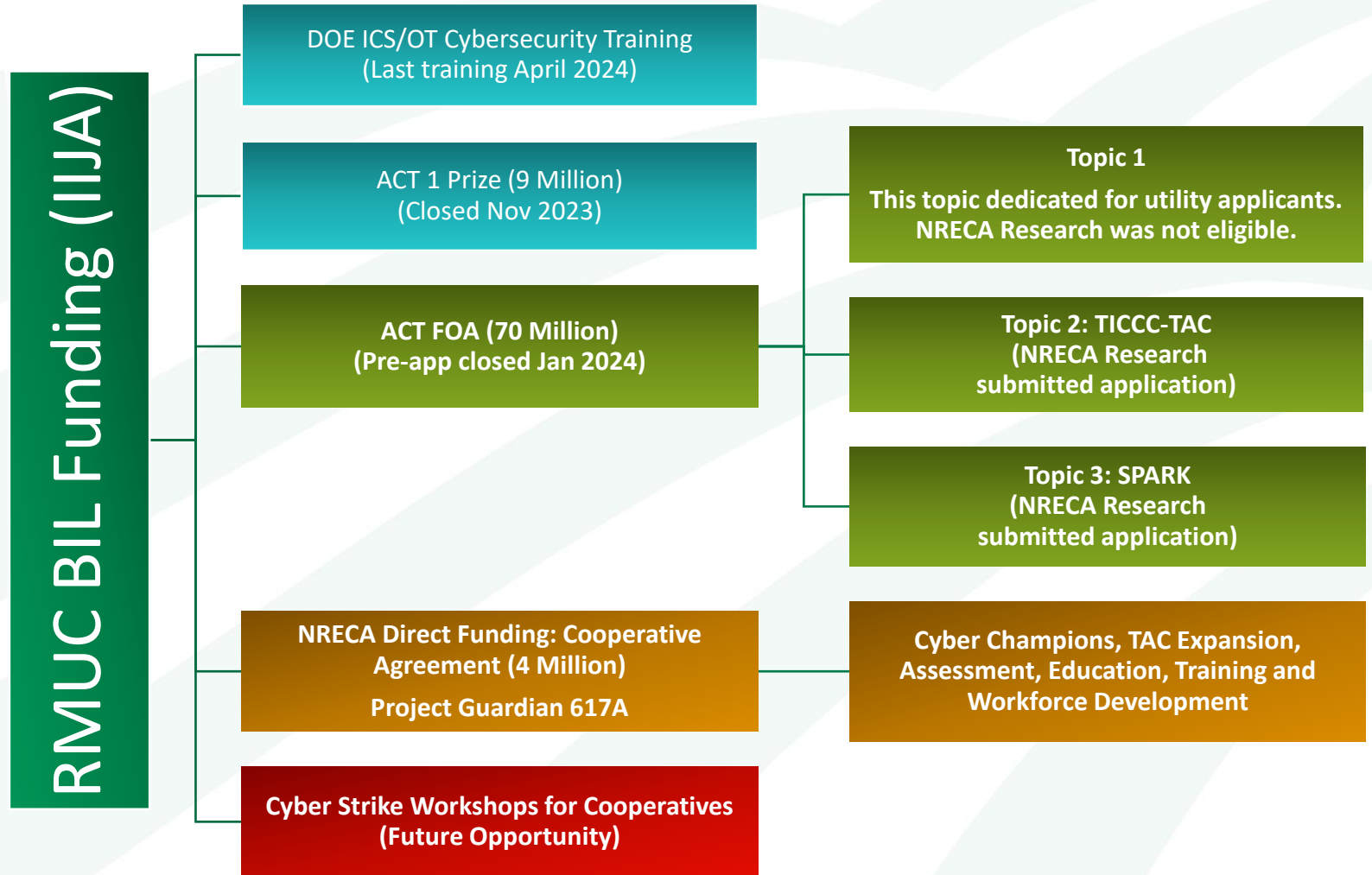
Department of Energy RMUC Funding Update

RMUC: Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance

\$250 million for grant and technical assistance, and deployment

How does the RMUC Funding directly impact Electric Cooperatives' Focused Efforts?

To Stay Up to Date on RMUC News
Join the email list by sending a request to CESER.RMUC@hq.doe.gov.



NRECA ACT FOA Topic 2 and Topic 3 Summary

- **Topic 2 - TISCCC-TAC: Trusted Industrial Control Cybersecurity Community – TAC**
 - Threat Analysis Center: \$3 million, \$50-\$300/year for each participating utility in cost share
 - NRECA Research will propose to cover the costs of the TAC community and collaboration platform for participating members and its growth over 4 years to ensure a smooth transition to a subscription-based model and ensure TAC grows to a self-sustaining user community.
 - ***380+ Cooperative Members have signed up to participate.***
- **Topic 3 - SPARK: Strategic Program for Advancing Rural Knowledge**
 - Cybersecurity Training Offering: Up to \$2 million with no cost share
 - NRECA Research will support rural utilities' efforts to increase the scope and quality of appropriate and affordable security training by providing participating cooperatives with high-quality training on various cybersecurity topics
 - ***400+ Cooperative Members have signed up to participate.***
- NRECA submitted a full application for Topic 2 and Topic 3
- The deadline for Cooperatives to submit letters of commitment has passed.
- Only co-ops listed on the Full Application with a Letter of Commitment are allowed to benefit from awarded funds.
- **Award Notification: *Selected to move into negotiations***

Project Guardian – 617A

Improving cybersecurity maturity, ensuring no cooperative is left behind

Project Guardian 617A

- **Cooperative Agreement between NRECA Research and the Department of Energy (DOE)**
- **Award Amount Received: \$4 Million**
- **5-Year Program: May 2024 to May 2029**
- **Goal:** Improve the cyber posture of electric cooperatives, provide resources to all cooperative sizes, and ensure no cooperative is left behind.
 - 617A is a hexadecimal reference
 - 61 represents “A” and 7A represents “Z” – or A-Z
 - No cooperative left behind



[Project Guardian News Publication Link](#)



[Project Guardian Website Link](#)

Project Guardian 617A Working Group

• Formation of Working Group

- A working group has been formed, consisting of cooperatives of various sizes and maturities, including distribution, generation, and transmission members.
- Representation from the following:
 - At least 5 small distribution cooperatives (under 10,000 meters),
 - At least 3 mid-sized distribution cooperatives (10,001-50,000 meters)
 - At least 2 large distribution cooperatives (over 50,001 meters)
 - At least 2 Generation & Transmission (G&T) cooperative

• Working Group Focus

- Develop the categorization of cooperatives to ensure that program resources are properly aligned with the members' cybersecurity size and maturity to be used throughout the project.
- Ensure that the programming developed under this project hits the priorities and program goals, while also providing feedback from rural utilities on the project's effectiveness.



Project Guardian 617A: 4 Key Focus Areas

Cyber Champions Program

- Create Cyber Champions Framework
- Understand what's working 'regionally'
- Share ideas, Identify Roadblocks
- Create roadmaps/guidance for all to use
- Enhance collaboration with local, state, federal & other entities
- Enhance communication around cybersecurity events with all cooperatives

Cyber Resilience Initiative

- Develop Self-Assessment Framework
- Develop and Improve Incident Response
- Conduct Tabletop and Purple Team Exercises

Education, Training, and Workforce Development

- Develop standardization in job roles and job descriptions to support a variety of co-op sizes, structures, and maturities

Threat Analysis Center Content Expansion

NRECA Cybersecurity Resource Advisory

Check out the regularly updated resources advisory to better understand all of NRECA's cybersecurity programs and resources.

[NRECA Cybersecurity Resources for Cooperatives
Updated Summary](#)

Additional Advisories and Reports
[Cybersecurity Information Sharing](#)
[Managing Your MSP Vendor for Cybersecurity](#)
[Coop Cybersecurity Special Report](#)



Business & Technology Advisory
May 2024



NRECA Cybersecurity Resources for Cooperatives Updated Summary

NRECA has a variety of cybersecurity resources and engagement opportunities available for members to gain understanding of cyber threats to our industry and take steps to advance cybersecurity preparedness.

The following list provides a summary of resources currently available and the corresponding website links. Visit cooperative.com for more information and updates.

Overarching Efforts

NRECA Cybersecurity Program

The NRECA Cybersecurity Program provides a variety of measures aimed to help our members advance their cybersecurity posture. Initiated with NRECA's [Rural Cooperative Cybersecurity Capabilities \(RC3\) Program](#), a former 3-year collaborative partnership between NRECA and the U.S. Department of Energy, we provide resources and actionable advice to our members to establish fundamental cybersecurity measures, educate staff and leadership, and collaborate on threat mitigation, detection, reporting and recovery. Together, we strive to protect cooperatives' organizations and the industry grid.

As noted in the following list of resources, some of NRECA cybersecurity efforts are conducted through [NRECA Research](#), a not-for-profit entity established in 2019 to complement the resources and services provided by NRECA to address the needs of electric cooperatives.

[NRECA Cybersecurity Special Report](#) –
featured first in November 2023 RE Magazine

Topic Websites on cooperative.com:

- [Cybersecurity Overview and Key NRECA Contacts Link](#)
- [Featured Cybersecurity Resources, Fact Sheets and News](#)

Contact our team at: membersecurity@nreca.coop

Federally Funded Projects

[Guardian – 617A](#)

A multi-faceted cybersecurity program funded under the Bipartisan Infrastructure Law from the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). NRECA will work with a co-op steering group to implement parallel efforts focused on establishing cybersecurity champions, self-assessment, and education and training. Guardian – 617A is a project through NRECA Research.

NRECA Cybersecurity Mental Health Webinar



Mental Health in Cybersecurity: Balancing the Scales
December 11, 2024 | 2-3 p.m. ET

Cost: **FREE**

Attend this webinar to:

- Better understand the specific mental health stressors faced by cybersecurity professionals.
- Gain practical strategies for maintaining a healthy mental state.
- Participate in interactive elements designed to enhance understanding and application of mental health strategies.

Mental Health in Cybersecurity Webinar “Today”

December 11, 2024 | 1-2 p.m. CST

Register Now

This webinar dives into the unique mental health challenges faced by cybersecurity professionals and entrepreneurs, emphasizing the need for a proactive approach to managing these issues. We will highlight practical strategies for individuals and organizations to help foster a healthy mental state and offer valuable tools and resources, equipping attendees with the knowledge to help prioritize and manage mental health effectively in their high-stress work environments.

CALL TO ACTION: WHAT CAN YOUR CO-OP DO?

Engage in public-private partnerships and cyber mutual assistance programs.

- Be proactive in establishing relationships with local, state, and federal entities

Take advantage of NRECA Resources

- Join the NRECA Co-op Cyber Goals Program\Update Goals Accomplishments
- Co-op Cyber Tech Conference
- NRECA Threat Analysis Center (TAC)
- ICS-REC
- Cybersecurity Guidebooks\Advisories
- Participate in NRECA Hosted Tabletop Exercises
- Participate in NRECA Webinars
- Stay up to date on the latest developments related to “Project Guardian 617A”

PROACTIVE & VIGILANT

NRECA Government Relations Update

John Ransome
Regulatory Affairs Director
NRECA

Michael Horder
Legislative Affairs Director
NRECA

THE COOPERATIVE COMMUNITY IS:

Changing the game

Driving change

Advancing the cause

Shifting the dial

Making an impact

Leading the charge

Making a difference

Breaking new ground

Making strides

Moving the bar

Creating momentum

Making headway

Changing the landscape

Pushing the envelope

Taking it to the next level

PROACTIVE & VIGILANT

Thank You.

For questions, please reach out
to membersecurity@nreca.coop

NRECA Cyber Team Contacts



Carter Manucy
carter.manucy@nreca.coop



Justin Luebbert
justin.luebbert@nreca.coop



Meredith Miller
meredith.miller@nreca.coop



Ryan Newlon
ryan.newlon@nreca.coop



Adrian McNamara
adrian.mcnamara@nreca.coop