FINAL REPORT:
Improving the Cyber and Physical Security Posture of the Electric Sector

Rural Cooperative Cybersecurity Capabilities Program (RC3)

National Rural Electric Cooperative Association

Federal Agency: United States Department of Energy

Identifying Number: DE-OE0000807

Date: 31 March 2021

Table of Contents

List of Figures

Legal Notice

This work contains information that is general in nature. Readers are reminded to perform due diligence in applying this information to their specific needs as it is not possible for NRECA or its suppliers to have sufficient understanding of any specific situation to ensure applicability of the information in all cases. This document is provided "as is," and NRECA and its authors make no warranties or representations, either express or implied, about the information contained herein, including warranties of accuracy, completeness, or usefulness. NRECA further makes no guarantee regarding any outcome or particular result based upon your use of the information. NRECA is committed to complying fully with all applicable federal and state antitrust laws. NRECA and the authors are not endorsing any particular vendor or cybersecurity practice featured in this document and not suggesting any particular cybersecurity practice is appropriate for every cooperative. Electric cooperatives are: (1) independent entities; (2) governed by independent boards of directors; and, (3) affected by different member, financial, legal, political, policy, operational, and other considerations. For these reasons, electric cooperatives should make independent decisions and investments based upon their individual needs, desires, and constraints.

Neither the authors nor NRECA assumes liability for how readers may use, interpret, or apply the information, analysis, templates, and guidance herein or with respect to the use of, or damages resulting from the use of, any information, apparatus, method, or process contained herein. NRECA is not undertaking any responsibility for cybersecurity measures at your cooperative by making this information available as your cooperative is solely responsible for providing and continuously ensuring the security of your assets. In addition, the authors and NRECA make no warranty or representation that the use of this document does not infringe on privately held rights.

This work product constitutes the intellectual property of NRECA and its suppliers, and nothing contained herein grants any ownership interest of this content to those accessing this document. NRECA has granted certain license rights to entities or individuals that download this document from its website.

Disclaimer

This material is based upon work supported by the Department of Energy National Energy Technology Laboratory under Award Number DE-OE0000807.

Executive Summary

Cooperative electric utilities represent an integral part of the larger electric grid and are part of the nation's critical infrastructure. The National Rural Electric Cooperative Association (NRECA) has a unique relationship with approximately 900 cooperatively owned and operated electric utilities, and engaged in a program with the Department of Energy (DOE) to promote a culture of cybersecurity and resiliency within the electric cooperative community. The Rural Cooperative Cybersecurity Capabilities (RC3) Program, funded under a Cooperative Agreement with DOE (Project DE-OE-0000807), focused on improving the cybersecurity and resiliency capabilities of small and mid-sized electric distribution cooperatives. This segment of electric utilities faces many challenges, but also embraces a culture of cooperation that presents opportunities. A customized approach is needed to reach these utilities – one that emphasizes collaboration, more focused and personalized training, use of trusted and familiar experts that can be deployed as needed, software security services that require limited in-house cybersecurity expertise, and shared resource models that enable access to more expensive cybersecurity options.

Between July 2016 and December 2020, the RC3 Program provided outreach, training, educational materials, exercises, workshops, site assessments, and technical assistance via in-person or on virtual platforms to hundreds of electric cooperatives. The RC3 Program also researched, evaluated, and demonstrated emerging technologies (e.g. C4) that could be used to protect utilities against cybersecurity vulnerabilities. RC3 Program efforts were organized within four technical task areas, and many of the RC3 Program efforts coordinated actions across the technical tasks in order to accomplish the larger mission of creating stronger internal cyber resiliency and security programs.

The RC3 Program has had an impact. RC3 Program products and resources were used by more than 750 of NRECA's member cooperatives, approximately 82 percent of NRECA's membership, during the RC3 Program's period of performance. The website landing page for the RC3 Cybersecurity Self-Assessment Toolkit received 3,827 visitors since it launched in December 2018, and the Toolkit was downloaded by more than 390 cooperatives. Similarly, the RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit website received 2,390 visitors since it launched in August 2019, and the TTX Toolkit has been downloaded by more than 216 cooperatives. Cooperatives used the RC3 Program offerings to improve the security of their systems. For example, approximately 45 percent of evaluations from cooperative staff participating in the RC3 SANS Voucher Program said they had already completed changes to harden their cooperative's systems as a result of the training they received in the RC3 SANS Voucher Program, 19 percent had changes in progress, and 25 percent had changes planned.

Throughout the RC3 Program the level of engagement with NRECA's member utilities remained high. The RC3 Program created 19 different written products that have been downloaded more than 3,200 times, averaging 169 downloads per product. Six different articles were written about the RC3 Program for NRECA's *RE Magazine*, and each article received on average of 450 page

views. The RC3 Program website has had 7,158 visits since it was launched, and averaged 500 visits per quarter in calendar year 2020. The landing page for the most recent offering, the RC3 Online Self-Assessment training videos, received 678 visits between July and December 2020.

From the beginning, the RC3 team knew it had to build and encourage an infrastructure, an ecosystem, that would enable the RC3 Program to scale beyond the cooperatives that were directly participating in the Program. A number of initiatives have begun by cooperatives to build on the RC3 Program's success utilizing the resources and tools the RC3 Program created. For example, cooperatives in both Iowa and Illinois now have access to skilled facilitators who will come out and help facilitate completion of the RC3 Cybersecurity Self-Assessment and/or the RC3 Cybersecurity TTX. And cooperatives in South Carolina have launched the Rural Electric Cybersecurity Advancement Program (RECAP). This Program uses a peer-to-peer model where a staff member from the Electric Cooperatives of South Carolina, Inc., pairs with an information technology (IT) staff member from one of the South Carolina cooperatives, and together they facilitate an RC3 Self-Assessment for another member cooperative within the state. The work these cooperatives are doing is a testament to the cooperative community's commitment to the Seven Cooperative Principals, and will ensure the RC3 Program's impact extends well beyond the period of performance and benefits a much larger audience than the RC3 Program could reach on its own.

Introduction

Today's electric grid is expected to have a wide range of attributes including: safety and security; clean and sustainable; affordable and equitable; and, reliable and resilient.[1] Innovations in technology are creating novel opportunities to enable grid owners and operators to meet these diverse demands. In achieving these goals, however, an increasing number and diversity of electric grid stakeholders are growing more dependent on digital communication technologies and supply chains that expose systems to new cybersecurity vulnerabilities and risks. Threat agents are opportunistically exploiting these vulnerabilities and cybersecurity threats have increased dramatically in frequency and sophistication over the past decade.[2] This trend is expected to continue.

Figure 1: U.S. landmass covered by cooperatives

Source: National Rural Electric Cooperative Association

https://www.electric.coop/electric-cooperative-fact-sheet

Electric cooperatives are part of this system and part of the solution. For more than 75 years, electric cooperatives have served their communities, providing energy and economic growth opportunities to more than 42 million, or 1 in 8 Americans. Electric cooperatives own and maintain 42% of the electric distribution lines in the United States. Their size and remote locations do not protect them from cyberattacks. This segment of electric utilities faces many challenges, but also embraces a culture of collaboration that presents opportunities. A

[1] *The Future of Electric Power in the United States*, National Academies of Sciences, Engineering, and Medicine. 2021. Washington, DC: The National Academies Press. https://doi.org/10.17226/25968.

[2] For example, see: *Grid Resilience: Priorities for the Next Administration*, National Commission on Grid Resilience, 2020, https://gridresilience.org/wpcontent/uploads/2020/11/NCGR-Report-2020-Full-v2.pdf; *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence*, Defense Science Board, 2017, Washington, DC, Department of Defense, https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf; *Worldwide Threat Assessment of the U.S. Intelligence Community*, D.R. Coats, 2019, Statement for the Senate Select Committee on Intelligence, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf; and, *Homeland Threat Assessment October 2020*, Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

customized approach is needed to reach these utilities – one that emphasizes peer-to-peer collaboration, more focused and personalized training, use of trusted and familiar experts that can be deployed as needed, software security services that require limited in-house cybersecurity expertise, and shared resource models that enable access to more robust cybersecurity options than any single cooperative utility might be able to afford.

Beginning in July 2016, the National Rural Electric Cooperative Association (NRECA), the trade association representing approximately 900 cooperatively owned and operated electric utilities, started working in partnership with the U.S. Department of Energy (DOE) on Improving the Cyber and Physical Security Posture of the Electric Sector (Project DE-OE-0000807). With the funding provided by DOE, NRECA launched the Rural Cooperative Cybersecurity Capabilities (RC3) Program (Figure 1). The RC3 Program is focused on promoting "a culture of security and resiliency within the electric cooperative community," with a specific emphasis on improving the cybersecurity capabilities and posture of America's small and mid-sized electric distribution cooperatives. The RC3 Program has four technical task areas:

Task 1: Advancing Cyber Resiliency and Security Assessments
Task 2: Onsite Vulnerability Assessments
Task 3: Extending and Integrating Technologies
Task 4: Information Sharing

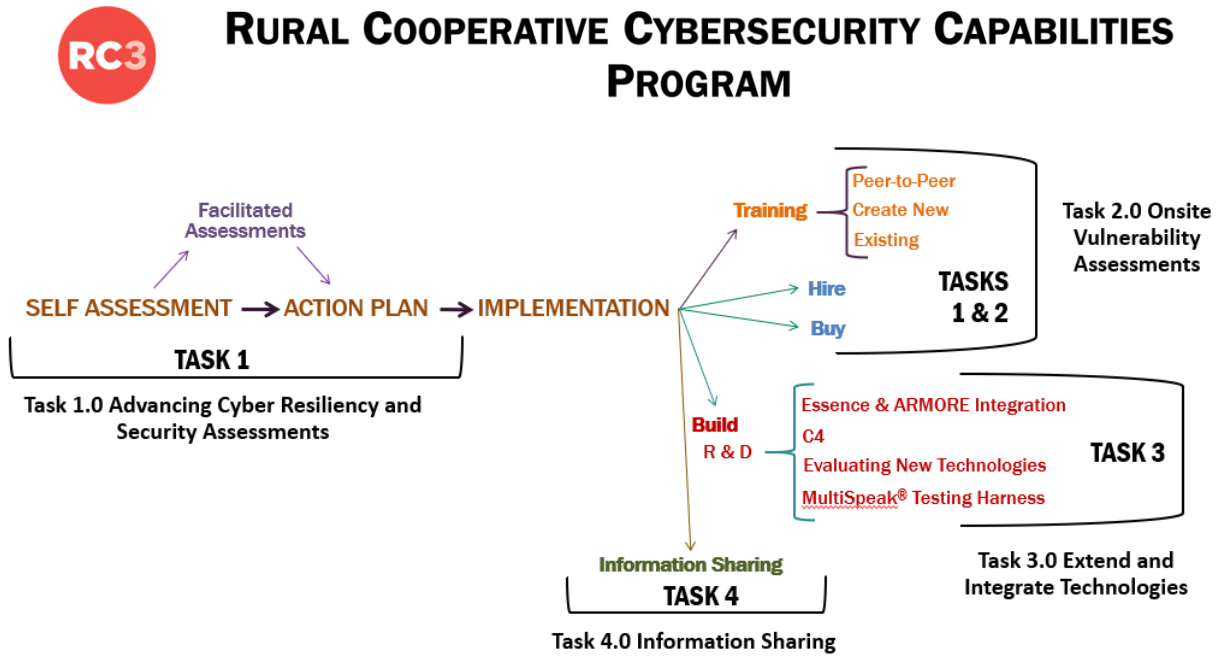

Figure 2: Major RC3 Program efforts associated with the four technical tasks

.

Recognizing that cybersecurity is not a product and that it requires an ongoing commitment of resources and effort, the RC3 Program created a series of initiatives to tackle the challenge on multiple levels across the four technical tasks. The remainder of this report covers the guiding principles and design of the RC3 Program, how the RC3 Program scoped its efforts to meet each of the technical task goals, a discussion of the RC3 Program's success and impact, and suggestions for future work. The Appendices provide more detailed descriptions of some of the major RC3 Program initiatives and how the design principles and insights were used to shape each initiative.

Meet Them Where They Are: Program Design

General Strategic Approach

The RC3 Program approached the challenge of improving the cybersecurity posture of cooperatives using a multifaceted strategy. While different tactics were used for each effort, there were some common design principles in all of the RC3 Program initiatives:

- Cybersecurity requires alignment of effort across three pillars: people; processes/policies; and, technology. Technology alone will not be sufficient.
- Cybersecurity is not an IT-only responsibility. The entire cooperative staff need to recognize how their unique job responsibilities open up their cooperative to vulnerabilities, understand what their unique roles are in protecting their cooperative, and have an ability to actively contribute to a culture of security that supports the ongoing implementation of actions needed to build a strong security posture.
- There is an extreme workforce shortage in cybersecurity talent, especially industrial controls systems (ICS)/operational technology (OT) cybersecurity talent.
- Tone at the top matters. Support and leadership from senior management and the cooperative's Board of Directors can strongly influence a cooperative's current and future cybersecurity posture.

Understanding and Defining the Audience

The RC3 Program focused heavily on creating ongoing opportunities for the RC3 Program team to understand the barriers and challenges facing the target audience of small and medium-sized cooperative distribution utilities. There were certain attributes that could be discerned from existing information. For example, more than 75 percent of NRECA's distribution utility members have less than 30,000 meters each. These consumer-owned, not-for-profit electric cooperatives are not just energy providers, they are engines of economic development in their communities, responsible for ensuring the well-being of more than 20 million American homes, businesses, farms, and schools in 48 states. They are vital to their communities, they take their role as a member service organization seriously, and they are tightly tied financially to their communities. For example, NRECA members serve 92% of counties and county-equivalents defined by the U.S. government as Persistent Poverty Counties (PPCs). Even in counties that are not PPCs, financial resources in rural communities can be very limited. Cybersecurity solutions need to be affordable and accessible based on the resources available within the cooperative and its community.

To be effective in creating resources and tools that would resonate with this population, the RC3 team used other methods to collect insights. One of the primary mechanisms was using an actively engaged Industry Advisory Group (IAG) of cooperative staff who volunteered to help. The IAG met regularly, provided critical insights, suggested changes in program directions, identified potential project areas, and reviewed the RC3 Program progress from start to finish. The other main method used to understand the audience was the RC3 Cybersecurity Summit

series consisting of 11 one-day training events scattered across the country. The RC3 Program used the Summits, which provided intensive and invaluable ongoing contact with members over 2 years, to get insights into what the members knew they needed, what methods they preferred to use to receive information or training, and what risks the RC3 team could identify that the members might not recognize as risks. The RC3 team gained insights on where cooperatives were in their cybersecurity programs. Below are some of the lessons we learned, both challenges and opportunities, through the IAG and the RC3 Cybersecurity Summits that shaped the design and goals of the RC3 Program efforts.

Potential Challenges and Barriers

Rural Challenges

Most electric cooperatives operate in remote areas of the country and often have limited information technology (IT) staff. In many cases, cooperatives contract out different IT and cybersecurity responsibilities to third parties and are entirely dependent on the sophistication and training of the local IT/cybersecurity providers that are willing to serve their area. This severely limits their access to the level of cybersecurity expertise available to larger utilities or utilities located closer to metropolitan centers. Those staff that do have IT responsibilities often have many other responsibilities within the cooperative, especially in cooperatives with a small number of staff. Rarely does their IT training include cybersecurity skills training.

Risks Inherent in Technology Changes Exacerbated by Inadequate Skills Training

Historically utilities did not demand the level of IT expertise needed today. Similar to other utilities, existing cooperative engineering and operations staff were never required to learn about IT or cybersecurity. As more and more new technologies are adopted that require digital communications, and more and more IT equipment is integrated into environments that were once dominated by proprietary operational technology (OT) equipment, the security that was inherent in the historical architecture of these systems is no longer sufficient. Most staff who have been working in these systems for many years have received no formal training to appreciate the risks that are created with the changing technologies being used. And it is rare for vendors to clearly articulate security issues that might be associated with their products or systems. There are tools available to identify and mitigate these risks, but most of these tools cannot be effectively installed and managed without significant retraining, and most rural areas do not offer that kind of unique training. In addition, some mitigation controls require significant modifications to the underlying architecture of the system. These deeper levels of architectural change require both financial resources and new skills to design, implement, and maintain.

Perception Challenge: Small and Isolated Doesn't Mean Secure

Low probability, high impact risks are difficult for most leaders to integrate into their thinking and budgets. Some cooperatives mistakenly believed that they were too small to be of interest to cyber criminals; cyber-attacks were considered an issue for big utilities that were more attractive targets for nation state actors or criminals. The perception that a utility that is small and isolated is safer makes it even harder to justify prioritizing a low probability incident. While

cybersecurity threats are as relevant to small, rural utilities as large, urban utilities, this misperception was a challenge for the RC3 Program. Helping cooperative staff understand cybersecurity issues and how cooperatives, like all companies using a digital network that are a part of critical infrastructure, are at risk was essential. A second challenge was helping the cooperative's senior leadership appreciate the risk. Only with upper management understanding would cooperatives dedicate the appropriate resources to security. With the increase in cyber-crime, convincing smaller remote utilities they can be a victim of a cyber-attack is easier but still remains as a perception issue.

Cybersecurity as a Responsibility of Everyone – A Culture Change

Another challenge for the RC3 Program was to create an understanding within a cooperative's staff that cybersecurity is not just a responsibility for IT staff and IT service providers. Every staff member in a cooperative has both a responsibility and opportunity to help defend their cooperative. Most staff believe that as long as IT is focused on cybersecurity, the rest of the staff are off the hook and can proceed as usual. From the very top of management to workers in daily operations, everyone at the cooperative must be aware that their interactions with hardware and software components, and their daily actions to implement physical security controls that limit physical access, are essential steps in minimizing cybersecurity risk. An organization-wide commitment to cybersecurity requires a cultural change. Creating program offerings that result in every person in the organization understanding and taking responsibility for security is not easy. Fortunately, cooperatives have experience with what it has taken to build a culture of safety. Making analogies between a culture of safety and what will be needed to build a similar culture of security often resonates with cooperatives.

Investing to Help Ensure Something Will NOT Happen

Cooperatives are committed to providing affordable energy for their members. Costs are continually scrutinized to ensure efficiencies. Another challenge for the RC3 Program was to convey the importance of investing in resources in order for something NOT to happen. Investments are traditionally prioritized based on the results they will provide and the return on investment. There is no concrete measure currently used in cooperatives to evaluate the benefits of investing to prevent a cyber-attack. The RC3 Program needed to raise awareness and understanding of the risks associated with a cyber incident, including impacts to operations, legal actions, reputation, and more. This information could then be used from the bottom up, for staff responsible for cybersecurity to make a case for resources to their management and boards, and from the top down, to educate leadership so they were more knowledgeable and comfortable weighing the need for cybersecurity preparedness and response against other competing resource demands.

Access to Cybersecurity Expertise – the Limited Cyber Workforce

Even when cooperatives have an appreciation for the risks and importance of cybersecurity, one of the largest challenges remains – access to the necessary expertise. As noted, many small and medium-sized electric cooperatives have limited IT personnel on staff. In addition, they are located in remote areas of the country that are not appealing to high technology job applicants

that historically gravitate to companies in larger cities. Hiring talent was not going to be a solution most cooperatives could use. A more appropriate path was finding ways to improve the skills of the existing workforce, and/or creating a stronger local/regional ecosystem of well-trained cybersecurity resources that would be accessible to cooperatives.

Strengths of the Cooperative Community

In addition to understanding the barriers faced by cooperatives, it was also important for the R3 Program team to understand the incumbent cooperative culture and infrastructure. Building program efforts that could leverage and strengthen existing cultural norms and systems was a central part of the RC3 Program's design thinking.

Understanding the Cooperative Culture and Infrastructure

One of the most critical perspectives to understanding the cooperative community's culture is understanding the Seven Cooperative Principles[3] that form the core principles and values of the electric cooperative community:

1) Open and Voluntary Membership
2) Democratic Member Control
3) Members' Economic Participation
4) Autonomy and Independence
5) Education, Training, and Information
6) Cooperation Among Cooperatives
7) Concern for Community

In addition to the Seven Cooperative Principles, the cooperative community also has an existing infrastructure, a hierarchical organization of relationships that are somewhat nested in terms of scale. These layers consist of:

- Distribution cooperatives, their consumer-members including residential, industrial, and commercial members, and their community.
- Generation and Transmission (G&T) cooperatives that provide power and services to their member distribution cooperatives. Not all distribution cooperatives purchase power from a G&T cooperative, and some purchase only a portion of their power from a G&T cooperative. And the relationships between distribution cooperatives and their G&Ts vary widely.
- Statewide associations that provide lobbying and other services to member G&T and distribution cooperatives. Not all states have a statewide association, and the level of staffing at a statewide and its level of engagement and relationships with member cooperatives vary widely across the cooperative community.
- Service Members, including statewide associations, are organizations that were formed over time to create economies of scale. These organizations are member owned and offer

[3] Co-op 101: Understanding the Seven Cooperative Principles, https://www.electric.coop/seven-cooperative-principles%E2%80%8B

banking, insurance, billing, emergency phone services, engineering, cybersecurity, and many other services to their member owners.

Eagerness to Learn and Improvise

Cooperatives are wonderfully progressive and creative in pursuit of operational improvements that will benefit the cooperative and its members. Often the first to demonstrate new technologies, cooperatives have a spirit of ingenuity. While some of this ingenuity might be driven by necessity, the result is a community that has a relatively open, experimental mindset that will listen to new options. There is an abundance of ground-breaking leaders within the cooperative community who are interested in making changes to improve their cooperative and willing to chart a new path and lead the way. If the RC3 Program could produce resources and services that had value, finding champions that would test, refine, and promote successes within the cooperative community was very likely to happen.

Peer-to-Peer Learning – Cooperation Among Cooperatives

A unique aspect of cooperatives is their commitment to not just their own success but the success of their peers and the Cooperative Nation as a whole. One of the Seven Cooperative Principles is 'Cooperation Among Cooperatives.' It is hard to describe how strongly this principle is embedded in the culture of electric cooperatives. Staff members are not just eager to learn about cybersecurity for the betterment of their operations and service to their consumer-members, but they also readily participate in group discussions and support each other's learning. Given an opportunity, there will almost always be a cooperative staff who will volunteer to fill a role if it will help other cooperatives advance their cybersecurity. And, provided with a secure and trusted environment, cooperatives freely share details and information about their cybersecurity challenges and solutions. Information sharing is a part of the cooperative culture and will happen readily if the right infrastructure is created to facilitate it.

Additional Program Design Insights and Principles

Using the insights gained from the IAG, the RC3 Cybersecurity Summits and other engagements with NRECA's members, the RC3 team created the RC3 Program and designed resources and offerings around the following additional observations and principles:

- The three A's: Affordable, Appropriate, and Accessible.
    - RC3 Program products and opportunities need to be affordable.
    - Appropriate. Cooperatives are at varying levels of maturity in their cybersecurity programs. Solutions need to be appropriately scaled to the skill levels and resources of small and mid-sized distribution utilities, flexible and tailored to meet them where they are.
    - Accessible to rurally located staff with limited travel funding and time.
- The design and maturity of a cooperative's cybersecurity program is related to the level of leadership support, and organizational and financial support from the CEO/General Manager (GM). Most IT staff in distribution cooperatives are not in senior management positions and have relatively little power to impact policies, procedures, and financial

allocation decisions. They may have a very good idea of what needs to happen but very little ability to implement on those ideas. Two key audiences are cooperative CEOs/GMs and members of the Board of Directors.

- Few of the staff that are responsible for IT have IT as their only job responsibility. This leaves limited opportunities for ongoing exposure to threat information and cutting-edge cybersecurity practices and techniques, or time and funding to improve their cybersecurity skills through courses or attending cybersecurity conferences.
- Rural communities face unique challenges in accessing highly skilled IT and cybersecurity talent. It is hard to recruit people with these skills into very rural areas in competition with job opportunities in more desirable locations and at more lucrative pay rates. This means it's hard to hire these professionals directly ***and*** it's hard to find local service providers and resources with these skills.
- Resources are needed to support cybersecurity progress that are relevant to all of the cooperative staff, especially for cooperatives that outsource IT and security functions. Many existing cybersecurity resources and tools require a high level of skill or large amounts of time to fully utilize them.
- Distribution cooperatives rely very heavily on third-party partners and vendors for IT, security, engineering, and operations functions. There is rarely a clear understanding of who its responsible for cybersecurity in these arrangements.
- Whenever possible, create solutions with the highest chance of continuing and expanding beyond the RC3 Program period of performance.
- Whenever possible, leverage existing cooperative principles and strengthen existing cooperative infrastructures.
- Cooperatives enjoy peer-to-peer learning opportunities, and peer-to-peer sessions are generally ranked more positively than other session formats.

Scoping the RC3 Program

One of the most important factors to the success of the RC3 Program was the enormous flexibility DOE built into the original Statement of Project Objectives (SOPO). The primary goal of the SOPO was to utilize NRECA's expertise in understanding its membership, "as well as its unique position as an electric cooperative convener to promote a culture of security and resiliency within the electric cooperative community." As the RC3 Program matured and the RC3 team learned new lessons during the implementation of each program effort, appropriate changes were made to the Program direction. The RC3 team recognized opportunities that overlapped across the four technical tasks, and rather than narrowly defining efforts under only one task, the RC3 Program aimed to accomplish the bigger picture: "enhance organizational capacities" that would support electric cooperatives in the primary objective "to develop an internal cyber resiliency and security program at electric cooperative utilities."

Recognizing that cybersecurity is not an achievable state, but instead requires constant focus on improving an organization's cyber maturity, the RC3 program focused on a few key tactics to reach this goal:

- Creating new cybersecurity tools, the RC3 Cybersecurity Self-Assessment and the RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit, and developing programs grounded in the design insights and principles to create, market, and disseminate the tools.
- Utilizing NRECA's convening strength to create opportunities for cooperatives to learn from each other in peer-to-peer formats, and from subject matter experts.
- Investing in developing the knowledge, skills, and abilities of existing staff rather than purchasing solutions off the shelf.
- Advancing existing relevant NRECA cybersecurity research and development efforts.
- Empowering participants to 'own' the RC3 Program and request changes to Program direction when needed.

Below is a brief summary of some of the major RC3 Program efforts and results under each of the four technical tasks. Many of the RC3 Program efforts stretched across the technical tasks and, whenever relevant to accomplishing the larger mission of creating stronger internal cyber resiliency and security programs, the RC3 Program team wove together multiple task goals within a single Program effort. The Appendices provide more details on the major efforts, along with a detailed description of the motivations and design principles and insights that shaped the individual program efforts.

Task 1: Advancing Cyber Resiliency and Security Assessments

> *The Recipient will utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework, DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) tool, or equivalent as a baseline, to work with its membership to conduct assessments and develop a database to support ongoing benchmarking. The assessments will result in the development of guidelines, educational material, and the*

advancement of resiliency and security tools for electric cooperatives and public power districts.

There are many security assessment resources and security frameworks to help utilities evaluate and improve their cybersecurity capabilities, including the NIST Cybersecurity Framework (NIST CSF), the ES-C2M2, and the Center for Internet Security Controls (CIS Controls). Many of these are used extensively by larger utilities with dedicated IT and security staff. In contrast, there is a very limited selection of assessment resources and tools that are appropriate for utilities with no or only part-time IT staff located in regions with limited access to professionals with ICS cybersecurity skills.

During the scoping efforts to develop the RC3 Program, feedback from distribution cooperatives indicated that the existing cybersecurity frameworks, like the ES-C2M2 and NIST CSF, were too challenging. It was clear from the scoping results that the cooperative community needed a tool that was easier to use; something that could be used by the smallest to the largest distribution cooperative.

The RC3 Program envisioned an introductory self-assessment tool that any cooperative could use regardless of their starting point. The questions should be granular and detailed enough that they could make progress within a 3-month period, quarterly updates would show visible progress in the reporting graphics, and by the end of three years they would have implemented most of the controls and continued use would no longer be beneficial. At that point the goal would be for those cooperatives to 'graduate' to use a more comprehensive self-assessment tool, like the ES-C2M2 or NIST CSF. With this vision in mind, the RC3 team designed the RC3 Cybersecurity Self-Assessment and a comprehensive set of program efforts to address the people, process, and technology challenges distribution cooperatives were facing, all of which could impact the success of the self-assessment tool. This included creating specific efforts focused on the people who would be using the tool, the leadership who would be creating the processes needed to authorize and support its use, and the selection of a technology that could be used by people with a wide range of technical skills. The RC3 Cybersecurity Self-Assessment was created in two phases. The first phase focused on developing a hard copy version and, as of the end of the RC3 Program's period of performance, there were 672 download of the hard copy version. The second phase focused on developing an online version and, as of the end of the RC3 Program's period of performance, there were 533 cooperatives participating in a program to access the online version.

One of the major supporting efforts to build an ecosystem to ensure the success of the RC3 Self-Assessment tool, and the entire RC3 Program, was the RC3 Cybersecurity Summit series. Eleven one-day RC3 Cybersecurity Summits were offered between January 2017 and June 2019. The Summits provided cybersecurity training using a combination of lectures, technical tours, and peer-to-peer interaction and were attended by more than 380 cooperative staff representing 291 cooperatives. The Summits were the RC3 Program's primary mechanism for collecting insights on challenges, increasing awareness of RC3 Program efforts, building a market for RC3 Program resources, and creating and strengthening information sharing networks.

In addition to creating Self-Assessment Program and the Cybersecurity Summits, other accomplishments under this Task included:

- Offering a cybersecurity course, *Foundational Cybersecurity*, created and taught by Acumen Engineered Solutions International, Inc. (AESI), as a pre-Summit course held four times the day before one of the RC3 Cybersecurity Summits: 14 November 2018, 12 December 2018, 29 January 2019, and 5 June 2019. A total of 75 staff representing 61 cooperatives attended the course. It was very well received, with an average score of 4.57 out of 5, where 5 = strongly agree, in response to "Overall this course met my needs," and 4.75 out of 5 in response to "I would recommend this course to a colleague."
- Creation of cybersecurity educational resources and case studies.

Task 2: Onsite Vulnerability Assessments

> *The Recipient will conduct assessments and develop case studies of a segment of member entities. The Recipient will evaluate and integrate the processes and technologies available to alert electric cooperative utilities of threats and vulnerabilities in their cyber and physical systems and share results to drive continuous improvement.*

Within Task 2 the RC3 Program focused on building skills within the existing staff to improve their ability to identify and mitigate vulnerabilities, conduct formal vulnerability assessments, and interpret vulnerability assessments results. Based on conversations with the IAG and internal liability concerns, the RC3 Program shifted from purchasing access to vulnerability assessments to be completed for a few cooperatives, to a focus on helping existing utility staff gain access to training and education that would help them assess vulnerabilities in their systems and implement controls to counter evolving threats. The two flagship efforts under Task 2 were the RC3 SANS Voucher Program, a training program created to help address cybersecurity skills gaps within the cooperative community, and creating an RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit.

The RC3 SANS Voucher Program offered three opportunities for cooperatives to receive free access to online cybersecurity training courses offered by the SANS Institute, a world-renowned cybersecurity training, certification, and research company. The RC3 SANS Voucher Program was launched in March 2018, and over the course of the next two years 122 staff from 114 cooperatives received cybersecurity skills training. The program prioritized access to training for staff from small and medium-sized cooperatives, and more than 70% of the participants were from cooperatives serving less than 50,000 meters. It was highly competitive to get into the Program and only 40 percent of the applicants were accepted.

In addition to providing skills training, the RC3 SANS Voucher Program was structured to facilitate peer-to-peer learning and to build stronger information sharing networks between participants. Program evaluations were returned by 66 percent of the participants. Approximately 45 percent of the staff returning evaluations said they had already completed changes to harden their cooperative's systems as a result of the training they received in the RC3

SANS Voucher Program, 19 percent had changes in progress, and 25 percent had changes planned. The RC3 SANS Voucher Program was one of the most successful RC3 Program offerings that resulted in specific concrete changes made by participants to harden their systems. Both anecdotal comments and evaluation responses indicated that participants benefited from the peer-to-peer support structure of the Program, and there was substantial interest in continuing the Program by both participants and staff that did not get into the program, as evidenced from the consistently high number of applications submitted.

The RC3 TTX Toolkit was an effort initiated by a cooperative staff member who asked for a cybersecurity exercise scenario they could use for their annual TTX. This started a series of discussions over two years that resulted in the RC3 TTX Toolkit. Cybersecurity exercises play an important role in security preparedness by enabling staff to test and validate their cooperative's response plans and capabilities, and to identify capability gaps and areas for improvement before a cybersecurity incident occurs. The RC3 TTX Toolkit team selected a vendor, Delta Risk, LLC, and worked with three cooperatives to create a TTX Toolkit that included 12 different cybersecurity scenarios appropriate for three different levels of cybersecurity maturity, 4 scenarios for each maturity level. The RC3 TTX Toolkit has been downloaded more than 750 times by 216 cooperatives and includes:

- Planning Checklist
- Delivery Day Checklist
- After-Action Checklist
- TTX Sample Invitation
- Facilitator's Tips
- Participant Worksheet
- After-Action Report Template
- Facilitator's Guide & Slides

In addition to the RC3 SANS Voucher Program and the RC3 TTX Toolkit, other training courses and resources created under Task 2 included:

- Creation of a new cybersecurity course, *Who Do You Let In: Procuring and Managing Cybersecurity Vulnerability Assessment Providers*, initially offered as part of NRECA's Cooperative University in October 2017. The course was originally attended by 7 cooperative staff and received good reviews. Modifications were made to the course and it was offered four more times as a pre-Summit course held the day before one of the RC3 Cybersecurity Summits: 14 November 2018, 12 December 2018, 29 January 2019, and 5 June 2019. A total of 64 staff representing 59 cooperatives attended the course. It was very well received, with an average score of 4.6 out of 5, where 5 = strongly agree, in response to "Overall this course met my needs," and 4.76 out of 5 in response to "I would recommend this course to a colleague."
- Creation of a new cybersecurity course, *Managing Cybersecurity Risks in Purchasing Decisions*, offered as part of NRECA's Cooperative University in October 2017. The course was attended by 13 cooperative staff and received medium reviews. The RC3 Program did not offer the course again.

- Creation of a *Managed Security Service Providers (MSSP) for Electric Utilities* catalogue. To help cooperatives understand the wide range of cybersecurity services available, including vulnerability assessment providers, the RC3 Program team worked with the American Public Power Association (Public Power) to develop a catalogue of security service providers that would be appropriate for small and mid-sized utilities. The first version of the catalogue, released in October 2017, included descriptions of 46 MSSPs identified by the vendor who created the report, PreScouter. An additional 15 MSSPs that were part of NRECA's Service Members or Associate Members Programs were added to the catalogue and published in an NRECA Service & Association Members Addendum released in April 2018. This resource has been downloaded 212 times since its release in October 2017.

Task 3: Extend and Integrate Technologies

> *The Recipient will engage with members to support adoption of promising technologies, develop case studies based on the emerging technologies, and share the information with appropriate stakeholders to meet emerging needs and create a more resilient energy delivery system. This includes extending, integrating, designing, and developing tools, technologies, and techniques that have the key properties of resiliency, real-time availability, integrity, authentication, and confidentiality.*

The objective of Task 3 was to drive adoption of promising technologies. Cybersecurity technology is advancing rapidly, but technical advancement is of minor value if it is not accepted and used knowledgeably by the utilities. The RC3 Program started this task with an examination of available and emerging technologies and came to the conclusion that it would be possible to develop a technology that was substantially superior to what was available. This shortcoming stems from the commercial focus of cyber technology providers. The vast share of the cyber market is the protection of business systems with particular emphasis on Internet-based systems. The RC3 Task 3 team's prime interest was protection of the ICS and OT systems that operate the grid. Utilities are concerned with the protection of business systems and the privacy of employee and member data, but those aspects of utility operations are essentially the same as equivalent operations in general business. The RC3 team recognized that the grid is unique and vital and requires and merits special consideration, so the RC3 Task 3 team undertook development of a utility-focused high-performance cyber anomaly detection technology called Cybersecurity-Collect-Communicate-Collaborate (C4), developed by BlackByte Cyber Security, LLC (BlackByte).

The C4 technology provides a near instantaneous picture of network operations related to the control and monitoring of electric utility operations. C4 looks at the origins and destinations of messages flowing into, out of, and within the industrial control system, performing deep packet inspection to provide a nuanced picture of operations allowing rapid detection of any anomalous behavior. C4 was conceived as a partner piece to NRECA's GridState technology, which provides a near instantaneous picture of the state of the grid as expressed in voltage and other physical parameters, and the setting of switches and other devices with discrete states.

Together, C4 and GridState are included in the term "Essence 2.0," which refers to a product resulting from the integration of the two technologies. The combination of the two technologies is very powerful and is unique in the industry. Individually, the two technologies can identify any anomalous operation in either the ICS or the grid and provide extensive information on both to support root-cause analysis leading to remediation.

Work on C4 began in late 2017 and culminated in a stand-alone pre-commercial release C4 platform with completed components for discovery, storage, evaluation, and visualization and a reporting capability for the utility to have dynamic asset management.

In addition to advancing the C4 technology, other efforts under Task 3 included:

- Completion of a technology assessment evaluating the extent to which NRECA's initial Essence technology could be integrated with the Applied Resiliency for More Trustworthy Grid Operation (ARMORE) technology developed by the Grid Protection Alliance in partnership with the University of Illinois at Urbana-Champaign (UIUC). The analysis was completed by BlackByte and identified opportunities for the integration of data capture methods, merging protocol metrics, merging rule-based engines, and presenting data to the Analysis Layer within the Essence framework.
- Development and validation of a MultiSpeak® V3.x/V4.x online testing harness tool and associated technical reports documenting the verification and validation process. Existing interoperability testing for MultiSpeak® V3.x and V4.x was manually performed, pair-wise (two vendors were required to test), time consuming, and lacked comprehensive testing requirements of the business processes or operations, which potentially created "loopholes or gaps" that undermined cybersecurity. The effort resulted in an online comprehensive interoperability testing tool to identify gaps and improve cybersecurity.
- Completion of a *Vulnerability Scanning Runbook* for IT staff that have moderate to advanced IT skills. This *Runbook* sets forth guidelines and recommendations on the performance of vulnerability scanning and how to classify vulnerabilities to computer networks based on risk. The intent of the *Runbook* was to empower electric cooperative IT professionals to understand what a vulnerability scan is, how to perform a vulnerability scan, what tools an IT professional might utilize, and how to interpret the results of the scan.

Task 4: Information Sharing

The Recipient will enable and encourage its members to participate in programs to develop and evaluate technologies needed to better share cyber threat information with other entities as well as the government. The Recipient will leverage its members for a broad range evaluation and integration of cyber risk information sharing platforms. The Recipient will develop case studies to inform its membership on devices, tactics, and techniques best suited for their unique business model. To promote information sharing, the Recipient may utilize a platform to efficiently and securely communicate resiliency

and security risks to and among electric cooperative utilities and appropriate stakeholders.

Information sharing is an essential but difficult activity that contributes to the success of a stronger cybersecurity program and to building a resiliency mindset into how a cooperative approaches cybersecurity. The RC3 Program team interpreted this task very broadly. Leveraging insights gained from the RC3 Summits and the IAG on the skill level and cybersecurity maturity of the target audience, small and medium-sized distribution cooperatives, the primary goals in this task were to enable and encourage members to participate in programs to share threat information, utilize case studies and other communications to increase awareness of security risks, deploy the C4 technology, and to develop and promote other platforms members could use to expand their awareness of security issues.

The RC3 Cybersecurity Summit Series was a significant and effective mechanism for the RC3 Team to have discussions with cooperatives about the importance of cybersecurity information sharing and to introduce staff to the Electricity Information Sharing and Analysis Center (E-ISAC). Many distribution cooperatives had not interacted with the E-ISAC prior to an RC3 Cybersecurity Summit. The E-ISAC had a dedicated time on every Summit agenda and attended in person to share threat briefings and information on their purpose and how to join.

In addition to encouraging members to join the E-ISAC, the RC3 Program also encouraged members to utilize or create their own networks. NRECA hosts a number of platforms to share information, including professional communities. And many of the cooperative statewide associations host member meetings, including IT associations, security task forces and associations, and other topic-based networks. The peer-to-peer sessions in each Summit provided members an opportunity to improve and expand their internal sharing networks. The Summits introduced members to existing networks, exposed them to other formats for creating their own networks, and helped existing networks connect with each other.

The C4 work also extended into Task 4. The C4 technology roadmap envisioned utilizing the C4 platform for secure communications under a federated model, where information could be shared across a federation of C4 sensors. The deployment of C4 sensors and work related to building a platform for sharing information was under Task 4. Unfortunately, the COVID-19 pandemic occurred at the height of the deployment effort. While the C4 team was able to adapt and develop a learning management system to facilitate remote deployments, and successfully completed one remote deployment, the travel restrictions severely limited the deployment effort. By the conclusion of the period of performance, the C4 technology had been successfully deployed and extensively tested in 10 different cooperatives, including a G&T that extended use of the technology to its 5 distribution cooperatives.

A third major effort under Task 4 was the development of case studies and educational resources to expand an understanding of cybersecurity risks and threats and to increase awareness of the RC3 Program and its resources. The contract partner was University of Illinois at Urbana-Champaign (UIUC), who partnered with the RC3 team to develop of a series of six RC3

Cybersecurity Guidebooks. Each RC3 Guidebook targeted a different job role in the cooperative to help all of the staff recognize their unique responsibilities and opportunities to protect their cooperative.

- *Co-op Cybersecurity and You: Understanding Cyber-Incidents, Incident Prevention, and Incident Response*
- *Cybersecurity Guidebook for Electric Co-op Human Resources Staff and Benefits Administrators*
- *Cybersecurity Guidebook for Electric Co-op CEOs and General Managers.*
- *Cybersecurity Guidebook for Electric Co-op Board Members*
- *Co-op Cybersecurity for Financial and Office Managers*
- *Co-op Cybersecurity for Engineers, Operators and Staff with IT Responsibilities*

Other efforts under Task 4 included the development and dissemination of RC3 Program materials. Appendix F: RC3 Outreach and Recruitment provides a list of resources, articles, and publications created by the RC3 Program or by others to describe RC3 Program successes.

Measuring Success: RC3 Program Impacts

The RC3 Program team had some very specific goals in mind to determine whether the RC3 Program was 'successful' including:

- Changes made by cooperatives to harden their cooperative's systems as a result of their participation in the RC3 Program.
- Increases in the technical skill level of cooperative staff.
- Increased participation of non-IT staff in securing their cooperative.
- Increased awareness and focus on cybersecurity by senior leadership.
- Members find value in what the RC3 Program offered measured by high levels of member engagement with RC3 Program resources, tools, and offerings.
- Strengthening existing relationships and building new relationships critical to supporting shared resource models and cybersecurity information sharing.
- Changes in the cybersecurity ecosystem available to cooperatives, such as engaging new participants or increasing engagement of existing participants.
- Scaling up the RC3 Program's impact by the creation of cybersecurity initiatives internally within the cooperative community that were enabled by the RC3 Program but no longer dependent on the RC3 Program, and that would last beyond the RC3 Program period of performance, such as the creation of new entities, infrastructures, service models, and program efforts.

This section highlights some general examples of the RC3 Program's success. Additional examples are provided in the Appendices associated with some of the major RC3 Program efforts.

Did Cooperatives Use what the RC3 Program Created?

Critical to any assessment of program impact is determining whether the resources, products, and opportunities that were created in the RC3 Program were actually used. The RC3 Program measured this using:

- data on the number of participants at events, like Summits or training opportunities;
- comments made by participants on formal evaluation forms completed after attending an RC3 Program event or participating in an RC3 Program;
- data on the number of website visits to the resources available through the RC3 Program website;
- data on the number of downloads of resources available through the RC3 Program website;
- comments made anecdotally through emails and interactions with the RC3 Program team; and,
- examples of cooperatives describing how they benefited from the RC3 Program in articles and other publications.

In terms of member engagements, more than 1,800 cooperative staff have engaged in at least one of the five major RC3 Program offerings:

- participating in the RC3 Online Self-Assessment Program
- participating in the RC3 Cybersecurity Summit series
- participating in the RC3 SANS Voucher Program
- downloading the hardcopy RC3 Cybersecurity Self-Assessment Toolkit
- downloading the RC3 TTX Toolkit.

These staff represent more than 750 of NRECA's member utilities. This means approximately 82% of NRECA's members utilized at least one of the five major offerings of the RC3 Program. About one third of the 750 cooperatives, 37 percent, participated in at least three of the five major RC3 Program offerings, illustrating the relevance and value of the Program's deliverables. Roughly one third, 29 percent, participated in two major Program offerings, and the final third, 34 percent, directly participated in one of the five offerings. However, these members may have also utilized the RC3 Program website or downloaded other RC3 Program resources and these actions would not be reflected in the data the RC3 Program collected.

In addition, the RC3 team was invited to speak at more than 65 cooperative meetings and conferences about the RC3 Program, including 22 meetings and conferences specifically for CEOs, General Managers (GMs), and Board of Directors members. These speaking engagements have enabled the RC3 Program to have direct contact with an additional 2,000 cooperative staff or cooperative Board Members to better understand their needs, promote cybersecurity practices and the RC3 Program offerings, and to advance efforts to build the trust relationships needed to increase cybersecurity information sharing. The frequency and consistency of invitations to speak also reflected the value cooperatives found in the RC3 Program's products and offerings.

The products and resources the RC3 Program created were very well received. NRECA's member utilities have initiated more than 2,600 interactions with RC3 Program opportunities and resources. The RC3 Program created 19 different written products that have been downloaded more than 3,200 times, averaging 169 downloads per product, in addition to the RC3 Self-Assessment and RC3 TTX Toolkits. Six different articles have been written about the RC3 Program for NRECA's *RE Magazine*, and each article has received on average 450 page views. The interest and momentum initially created by the Program has been sustained. The RC3 Program website has had 7,158 visits since it was launched, and averaged 500 visits per quarter in calendar year 2020. Of specific note, the website landing page for the RC3 Self-Assessment has received 3,827 visitors since it launched in December 2018, and the landing page for the RC3 TTX Toolkit has received 2,390 visitors since it launched in August 2019. The landing page for the most recent offering, the RC3 Online Self-Assessment training videos, received 678 visits between July and December 2020.

Did the RC3 Program's Efforts Result in More Secure Systems?

Feedback through formal evaluations and voluntary disclosures confirmed that participants made structural changes to improve their cyber resiliency, increased their skill levels, and built stronger relationships conducing to cybersecurity information sharing as a result of participating in the RC3 Program. For example, the RC3 team frequently heard anecdotal stories from participants in the RC3 SANS Voucher Program who were having a hard time keeping up with the class because they would learn something and then spend time implementing what they learned before returning the course. Data collected from the RC3 SANS Voucher participants documented system hardening changes as a direct result of their participation in the Program. Approximately 45 percent of the staff returning evaluations said they had already completed changes to harden their cooperative's systems as a result of the training they received in the RC3 SANS Voucher Program, 19 percent had changes in progress, and 25 percent had changes planned. The RC3 SANS Voucher Program was one of the most successful RC3 Program offerings that resulted in specific concrete changes made by participants to harden their systems.

In addition, there were numerous individual stories of cooperatives using the RC3 Self-Assessment to improve their systems. Below are a few examples and more details are provided in the Appendices specific to each RC3 Program effort.

- One GM/CEO from a cooperative that completed the RC3 Self-Assessment described how answering the questions in the RC3 Self-Assessment helped his cooperative understand that third party relationships and oversight are critical, and how working with vendors and getting information from vendors is important to securing his cooperative.
- Another CEO from a cooperative working the RC3 Self-Assessment explained how it was worthwhile to bring the entire team of senior managers to the table to discuss cybersecurity. You find things you did not know existed once you start the conversations with your managers, said the CEO. "We realized as a company that everyone needs to be on the same page with cybersecurity."
- After completing the RC3 Self-Assessment, another CEO explained how they immediately went and got all of their computers set up for automatic lock outs, they forced password changes, and got all their operating systems and patches caught up. They found they had huge gaps. And then they went through and started methodically getting their hardware in place. They found out that their firewall wasn't being kept current, that was key. And they initiated monthly phishing training and tests for their employees.
- Probably the most important thing, another CEO/GM who's cooperative completed an RC3 Self-Assessment stated, "other than identifying those holes and gaps and developing policies, we realized that this isn't an IT dept function. This is a top to bottom co-op function. And we were really able to build awareness of this."

Did the Cooperative Community Innovate and Take RC3 Beyond what was Initiated?

The RC3 Program did not have the resources to connect with every one of NRECA's members. From the beginning, the RC3 team knew it had to build and encourage an infrastructure, an ecosystem, that would enable the RC3 Program to scale beyond the cooperatives that were directly participating. A number of initiatives were begun by cooperatives to build on the RC3 Program's success utilizing the resources and tools the RC3 Program created. Below are some the examples of how the cooperative community is innovating and using RC3 Program resources. The work these cooperatives do will ensure the RC3 Program's impact extends well beyond the period of performance and benefits a much larger audience than the RC3 Program could reach on its own.

- The Iowa Association of Electric Cooperatives (IAEC) is the statewide association established to support the interests of its 37 distribution and eight G&T member electric cooperatives. In 2019 the IAEC secured ~$250,000 in state funding to hire a consultant to help all of their member cooperatives complete the RC3 Online Self-Assessment. In addition, the statewide association is contributing the time for one of its staff to facilitate an RC3 TTX for all of its member cooperatives.
- The Electric Cooperatives of South Carolina, Inc., (ECSC) is the statewide service and trade association for 19 consumer-owned electric cooperatives in South Carolina. In 2017 ECSC created a Cyber Security Task Force, and in 2018 they launched the Rural Electric Cybersecurity Advancement Program (RECAP). ECSC is using a peer-to-peer model where a staff member from ECSC pairs with an IT staff member from one of the South Carolina cooperatives, and together they facilitate an RC3 Self-Assessment for another member cooperative within the state. So far, the Task Force has completed two facilitated assessments in the RECAP Program. Their efforts slowed down dramatically due to the COVID-19 pandemic. They made the decision not to attempt RECAP virtually since they believed the process would not work as well as when it is done in person. The Task Force is planning to do all of the ECSC member cooperatives as time and travel restrictions permit. They are experiencing growing interest in RECAP.
    - The Colorado Rural Electric Association, the statewide association for Colorado cooperatives, began discussions with the ECSC Task Force at the end of 2020 to explore creating a similar RECAP offering to the cooperatives in Colorado.
    - Recently they were approached to make a similar presentation to the cooperatives in Ohio who are interested in RECAP.
- The Association of Illinois Electric Cooperatives (AIEC) is the service organization for 24-member electric distribution cooperatives and five G&T cooperatives in the state of Illinois. AIEC's Chief Technology Officer (CTO) has been using both the RC3 Self-Assessment and RC3 Tabletop Exercise (TTX) Toolkits to provide a facilitated Self-Assessment and TTX to any member cooperative that requests assistance. The CTO originally offered just the Self-Assessment, but after the RC3 Program released the TTX Toolkit he realized that participants had a much more comprehensive understanding of

cybersecurity if they completed a TTX on the first day, and then an RC3 Self-Assessment on the second day.

The RC3 Program team was thrilled to see these efforts growing within the cooperative community on their own initiative. The work the RC3 Program did to leverage cooperative principles and infrastructure, and to be responsive to cooperative challenges resulted in products and relationships that help enable these innovations. These examples of cooperatives helping other cooperatives use the RC3 Self-Assessment and TTX Toolkit are a testament to the value of the tools that were created with the DOE's financial support.

Recommendations for Future Work

Over the course of the RC3 Program's period of performance, many additional efforts were identified that were not included in the Program's initial focus. Below is a summary of some of the top issues that were identified by the RC3 Program team that could be addressed in future work.

Training

Top among the critical needs is training. Cooperative staff need access to affordable, appropriately scoped and scaled, and accessible cybersecurity training. This training needs to cover non-technical staff responsibilities in cybersecurity and technical training for staff with IT and cybersecurity backgrounds but limited skills. The RC3 SANS Voucher Program was extremely effective and oversubscribed, less than half of the applicants were accepted into the Program. The other training programs offered through the RC3 Program were also very well received but more is needed.

In particular, training is needed for engineers and operators on cybersecurity, and for IT staff on ICS cybersecurity. And more purple team training is needed, where red team professionals work side by side with the utility staff to train them on how to respond to a red team attack.

There is also a dearth of technical resources to help cooperatives scale down cybersecurity solutions designed for larger utilities to a series of steps that can be taken by a smaller utility with fewer staff. Before staff can understand what aspects of a cybersecurity solution are a 'must' and what aspects can be modified without impacting security, they need a stronger fundamental understanding of cybersecurity concepts and technical details.

Exercises and Incident Response

An ongoing request was for better resources and opportunities to improve incident response capabilities. The RC3 Program created the RC3 TTX Toolkit and that has provided a great starting point for many cooperatives. But a real incident response capability will extend beyond the cooperative to the broader emergency response community. Distributed play and simulation exercises that include a wider range of the response community are needed.

Third Party Security Risks and Vendor Management

For many cooperatives answering the RC3 Self-Assessment questions addressing cybersecurity risks associated with their third-party partners was a first introduction to this issue. The RC3 Self-Assessment required senior leaders to give detailed attention to risks associated with vendor management. Additional work is needed in this topic covering people, process, and technology approaches. New resources and tools are needed, and better training and enforcement mechanisms are needed.

Asset Identification and Asset Management

One of the most challenging sections of the RC3 Self-Assessment is the Identify section. Distribution cooperatives do not have adequate tools and training to fully enumerate what's in their systems and the existing communication architecture. Better tools are needed that can be implemented by an audience with a range of technical skills. A better understanding of their networks can help cooperative staff understand where the security risks are highest. In addition, a strong fundamental understanding of their existing assets and networks can help cooperatives create the opportunity to implement more advanced controls, from network segmentation to threat hunting.

Building Stronger Information Sharing Networks and Capabilities

When the RC3 Cybersecurity Summits started, most of the distribution cooperatives in the audience did not know about the E-ISAC or appreciate the value of joining the E-ISAC. Similarly, very few distribution cooperatives, especially those without dedicated IT staff, utilized threat feeds or other external cybersecurity information sharing resources. More work is needed to help cooperatives become familiar with information sharing resources, but also to raise their skill levels so they are better able to utilize the information provided by security announcements and threat feeds.

A Stronger Ecosystem of Shared Services

Most small cooperatives and many mid-sized cooperatives will never fund a full-time position entirely dedicated to cybersecurity, and those staff that are responsible for cybersecurity will generally have many other responsibilities. One of the significant challenges in rural areas is the lack of service providers willing to do on-site visits because of the hours needed to travel to where the cooperatives are located. The extreme cybersecurity workforce shortage exacerbates these issues. More work is needed to identify and support the development of effective shared service models that will enable cooperatives to have access to affordable cybersecurity professionals and technical assistance.

Methods to effectively communicate with senior leadership

Falling squarely in the 'process' category, many cooperatives expressed a need for resources to help them convey the seriousness and urgency of cybersecurity investments to their leadership. IT and engineering staff struggled with the challenge of defining a return on investment, to practical challenges non-technical staff face estimating an effective scope of work and budget based on the cybersecurity gaps identified. A multifaceted approach will be needed to address this challenge that includes specific targeted efforts to educate and inform senior leaders, and more practical efforts to help staff assess their needs and translate their concerns into a framework that senior leaders can understand.

Conclusions

The RC3 Program developed resources and offered opportunities that provided a great starting point for distribution cooperatives to create and strengthen their cyber resiliency. When the RC3 Program began, a reporter called NRECA to ask: “Will the DOE funding make a dent?” The answer is emphatically “YES!” The DOE funding allowed NRECA to contribute in a significant way to helping its member cooperatives advance their cybersecurity posture.

More than 750 cooperatives participated and directly benefited from the RC3 Program but the impacts of the Program will not stop there. Cooperatives made long-lasting improvements to the security of their systems, polices, procedures, and improved their cybersecurity knowledge, skills, and abilities as a result of their participation in the RC3 Program. In addition, many aspects of the RC3 Program design helped to build stronger relationships and infrastructures that the cooperative community is just beginning to use in innovative ways to continue on the path of constantly improving their cybersecurity posture and resiliency. In the true spirit of Cooperation Among Cooperatives, cooperatives are picking up the resources developed by the RC3 Program and creating their own programs to help each other.

Appendix A: RC3 Cybersecurity Summits: Addressing Cybersecurity Risks

The RC3 Cybersecurity Summits formed a foundational bedrock of insights and outreach that shaped the entire RC3 Program over the course of the period of performance. The target audience for the Summits was any staff member who had a responsibility for IT and/or cybersecurity, including the non-technical staff who were responsible for managing a third-party IT or security service provider. No cybersecurity expertise was expected. More than 380 staff from 290 cooperatives attended an RC3 Cybersecurity Summit.

The first Summit was held in January 2017 to test the waters and see what kind of reception it would receive. Based on the feedback, the format was slightly modified, and followed by 10 more Summits hosted at locations across the country to facilitate geographically diverse attendees and to reduce travel expenses for cooperatives as much as possible (Figure 3 and Table 1). Each Summit had a partner co-host and the agenda provided one full day of programming. Included on the agenda was a session highlighting the E-ISAC and information sharing, two breakout sessions for peer-to-peer interactions, brainwriting exercises[4], technical talks, an update on the RC3 Program, and, depending on the host location, a walking tour of the host facility providing participants with a chance to see ground-breaking research on security and energy technologies relevant to distribution utilities.

Figure 3: RC3 Cybersecurity Summit Announcements

[4] "Brainwriting" is an exercise where a group of attendees around a table are given individual pads of paper, each with a specific topic defined at the top. Each attendee writes his/her thoughts on that topic for a defined amount of time (typically a couple of minutes). Then, the pads are passed to the next person around the table, who may write their own thoughts on the topic and/or comment or add to the thoughts previously written. This method gives all attendees a chance to contribute to the input gathered, including those that are reluctant to talk. Typically, at the end of a full rotation of the pads, an open table discussion is facilitated for a defined amount of time to encourage the participants to build on what they wrote and read, and to have direct conversation on the information shared. This enables those participants who prefer to talk instead of write to also provide input.

Table 1: RC3 Cybersecurity Summit Co-Hosts, Locations, and Attendance

Date	Summit Co-host	Location	No. Cooperative Staff	No. Total participants (NRECA staff, host staff, Public Power staff, speakers, etc.)	No. of Co-ops
18 Jan 2017	National Renewable Energy Laboratory (NREL)	Golden, CO	45	58	37
26 April 2017	Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)	Fayetteville, AR	39	57	27
31 May 2017	Information Trust Institute (ITI)	Urbana-Champaign, IL	32	46	25
12 July 2017	Pacific Northwest National Laboratory (PNNL)	Richland, WA	28	46	25
11 Oct 2017	NRECA/Public Power	Arlington, VA	46	61	41
30 Nov 2017	Electric Power Research Institute (EPRI)	Knoxville, TN	36	45	26
1 Nov 2018	Alaska Power Association	Anchorage, AK	20	42	10
14 Nov 2018	Sandia National Laboratories (SNL)	Albuquerque, NM	33	47	22
12 Dec 2018	Great River Energy	Maple Grove, MN	46	53	34
29 Jan 2019	Idaho National Laboratory (INL)	Idaho Falls, ID	39	50	23
5 June 2019	Carnegie Mellon University (CMU)	Pittsburgh, PA	25	37	21
		TOTALS	389	542	291

The Summits served multiple purposes (see Table 2 for a summary of motivations and design principles and insights used to create the Summits). For many distribution cooperative staff the Summits were the first opportunity they had to meet someone from the E-ISAC. The RC3 Program modified products and opportunities based on member needs and challenges expressed during the Summits. The RC3 Program team used the Summits to get members thinking about concepts related to upcoming RC3 products and initiatives in advance of the start of those efforts. And, importantly, members loved the Summits. The last RC3 Summit was held in June 2019 and members continue to comment on how much they liked that training format.

Table 2: Motivations and Relevant Design Principles and Insights Used to Shape the RC3 Cybersecurity Summit Series

Motivations

Agenda Content

- Highlight cybersecurity information sharing and the E-ISAC.
- Provide cybersecurity training on concepts, issues, threats, and resources.
- Technical tours to introduce members to cutting edge scientific research.
- Mix of introductory and advanced material to ensure relevance for a wide audience.
- Market RC3 Program and other cybersecurity resources.

Agenda Structure

- Include 2 breakout sessions to encourage peer-to-peer interactions and break up interaction modes between listening and engaging directly.
- Use brainwriting exercises during breakout sessions to encourage deeper thought and ownership of RC3 Program direction.
- Include technical tours after lunch to create a second set of small groups for additional peer-to-peer interactions and keep energy levels up after eating.

Location

- Select hosts to build strategic partnerships or strengthen cooperative infrastructure.
- Locations near cooperatives to minimize travel costs.
- Based on building momentum within the state/region.
- Based on need to expand RC3 market awareness and engagement in state/region.

Advance RC3 Program

- Breakouts session topics to find out where they are, collect insights on cooperative challenges and issues.
- Content and breakout sessions topics to set stage for what was coming next, create a market for RC3 deliverables.
- Keep up the RC3 buzz, maintain a consistent high profile within the cooperative community.
- Identify potential champions for RC3 Program.
- Encourage feedback on RC3 Program direction, empower participants to 'own' the Program and request changes in Program direction as needed.

Relevant Design Principles and Insights

- Ensure the Summits emphasize all three pillars: people, process, and technology.
- Stick to the three A's. Design the Summits so they are affordable. Meet them where they are by creating appropriately scaled content that can be useful to a cooperative whether it has no inhouse IT staff, dedicated IT staff with limited cybersecurity skills, or an already existing strong internal cybersecurity program. Make sure the Summits are accessible to all and minimize the time and travel burden.
- Leverage the cooperative principles and the cooperative infrastructure and, if possible, reinforce both.
- Encourage senior leadership engagement at some level.
- Select topics and content that will advance the knowledge, skills and abilities of the participants and increase their exposure to threat information and cutting-edge cybersecurity practices and techniques.
- Ensure the Summits emphasize that cybersecurity is relevant to all job roles that impact cybersecurity, including staff responsible for interacting and contracting with third-party vendors.
- Increase awareness of the need to define cybersecurity responsibilities clearly within the organization and with third parties.
- Integrate peer-to-peer options.

2017 Summit Insights

Of the cooperative participants who attended the 2017 RC3 Summits, approximately 34 percent of the attendees were in a non-IT related job function. One goal of the RC3 Program was to promote a culture of security where everyone in the cooperative sees cybersecurity as part of their job function. The RC3 Cybersecurity Summits provide a new avenue for non-IT cooperative staff to learn about cybersecurity best practices and lessons learned from Summit presenters and from fellow cooperatives.

During the 2017 Summits, there were two sessions of brainwriting. One focused on 8-10 specific challenges around cybersecurity, such as Labor, CEO/Board Support, Documentation, etc. The other focused on elements and challenges associated with cybersecurity information sharing. An analysis of the 2,199 comments collected during the brainwriting exercises revealed the following insights:

- The complexity and inflexibility of many compliance documents was high on the list. These guidance documents were viewed as very difficult to dig through because of their length and their use of "government-speak" or legalese. Just the amount of time required to decipher the contents made it difficult for many participants wearing the multiple hats common for cooperative employees to decipher the material. A need for more simplified documents and guidance was a reoccurring theme.
- Participants shared their view that existing cybersecurity resources and documents all seem to apply to large utilities and organizations with little information or direction on how to change it to match the needs of a smaller operation. The issue was "scalability." The concern among participants was that scaling cybersecurity recommendations to meet their situation and constraints might affect the effectiveness of the solution in unforeseen ways negatively impacting the desired results.
- Access existing resources and documents was another concern voiced during the Summits. Many agencies and organizations are producing cybersecurity guidance documents. These are generally housed on each individual source organization's website, meaning a staff person at the cooperative must first know how to access each organization's electronic resources and then must know what information to gather. It is a very time-consuming process for staff who aren't dedicated to IT or cybersecurity to develop and maintain a list of where various documents and resources are located.
- Knowing where to start was listed as a need. Documents overlap, requirements may be for industries other than electric utilities, content was viewed as theoretical, and little specific information was available that could be acted on immediately in terms of hardware and software to implement an effective cybersecurity solution.
- Limited human resources serving in IT/cybersecurity roles was a common theme driving the call for simplicity, actionable guidance, and automated tools to handle reporting, configuration management, documentation, etc.
- There is a need for education and training on cybersecurity and IT in general.
- There is a need for meaningful metrics to convey the value of intangible results.

The comments from the brainwriting session focused on cybersecurity challenges were further categorized into the five NIST CSF functions that were used to structure the RC3 Cybersecurity Self-Assessment. Most of the challenges participants wrote down were issues associated with the Identify function. The challenges identified by Summit participants were distributed across the NIST functions as follows:

- Identify 51.9 %
- Protect 14.4 %
- Detect 1.8 %
- Respond 27.3 %
- Recover 4.6 %

All Summit participants were asked to complete anonymous evaluations. The major take-away themes from an analysis of the evaluations were:

1. **High Value of Peer-to-Peer Interaction:** One of the most highly ranked aspects of the Summits was the opportunity for cooperatives to come together and discuss with each other the challenges of cybersecurity.
2. **Need for Awareness about Cybersecurity Threats:** Attendees particularly enjoyed hearing real-world examples about cybersecurity risks, such as overview of the Ukraine attack and information shared by the U.S. Department of Homeland Security.
3. **Interest in Resources:** The Summits increased the cooperatives' awareness of the wealth of resources and tools available for cybersecurity, especially the free resources that would be very helpful for small cooperatives. Many expressed appreciations for the contacts and indicated an intention to use the resources in the future.
4. **Looking for Guidance:** Attendees expressed a strong interest in specific guidance on what to do to prevent, mitigate, respond, and recover from cybersecurity threats.
5. **Desire for Additional Summits:** The attendees emphasized the value in NRECA presenting information about cybersecurity at future sessions, including Summits, and cooperative state and regional meetings.

Another goal of the 2017 Summits was to build stronger partnerships with the Co-Host organizations. In an analysis of interviews with some of the Co-Host organizations, the benefits expected and received fell into one of the following categories:

1. Wider recognition and awareness of the capabilities, products, and services of the host organization.
2. Exposure to different vertical markets to expand the opportunity for the hosts to apply their expertise.
3. Providing the opportunity for newer, less experienced employees/students to hear about real world utility needs.
4. Using the input to refine research and development efforts to better match field needs and situations.
5. For NRECA, broader recognition of NRECA's demonstration of attention to the critical aspects of their members' operations.

Some of the lessons learned from the 2017 Summits included:

- The diverse audience resulted in some participants wanting more technical depth and others needing more introductory material.
- While the brainwriting was effective, participants were less engaged in the second brainwriting session.
- Using the Summits to seed interest in upcoming RC3 products and initiatives was effective.
- The participant feedback emphasized the need to increase attractiveness of Summits to non-IT audiences, including CEOs/GMs and other senior leaders, especially for those cooperatives with no inhouse IT staff.

2018-2019 Summit Insights

There was a significant shift in focus for the five Summits held in 2018 and 2019 based on lessons learned during the 2017 Summits and the RC3 Program roadmap. The agenda continued to include a breakout session and brainwriting exercise on issues associated with cybersecurity information sharing. Instead of a second brainwriting session, a more formal mini-workshop was used. The workshop was either on insider threats and presented by the Software Engineering Institute's Insider Threat Program, or was a CyberSecure My Business workshop presented by the National Cyber Security Alliance (NCSA). In addition, the RC3 Program introduced two pre-Summit classes held the day before the Summit for the last four Summits. Once class was designed for non-technical staff and the other class was designed for more technical staff. The goal of these pre-Summit classes was to provide more targeted information for the wide range of skills in the Summit audience in advance of the Summit so participants would also be able to gain more value from the Summit content.

In general, participants ranked the Summits as valuable. On a scale of 1-7, with 1 being not at all valuable and 7 being extremely valuable, the average rating across the five Summits held in 2018 and 2019 was 6.27. The participants in the 2018-2019 Summits came from a broad range of job roles, including CEOs/GMs, one of the audiences the RC3 Program specifically made an effort to attract to the Summits (Figure 4).

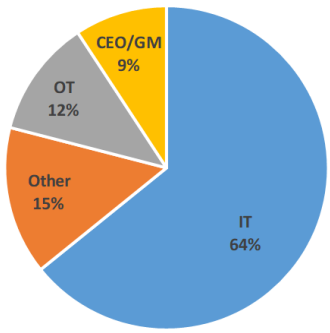

Figure 4: Distribution of 2018-2019 Summit Participants by Job Role

The addition of pre-Summit courses providing introductory and advanced training to enable participants to better understand the Summit content appeared to work. Summit participants were satisfied with the level of technical detail provided at the Summits (Table 3).

Table 3: No. of Summit Evaluation Responses Evaluating the Summit Technical Level

	Alaska	Sandia	GRE	INL	CMU	Total
Too basic	1	2	3	0	0	6
Too technical	1	0	0	2	0	3
Right level	13	19	37	19	15	103

Participants were asked to identify the "Most Valuable Takeaways" on their Summit evaluations. Their comments were organized into seven topics based on the nature of the comments: information sharing/resources, people/culture, process, technology, vendors, legal, and other. An approximate breakdown of the frequency of comments is provided in Figure 5 and examples of comments for each topic are provided in Table 4. The majority of participant comments indicated that discussion and resources associated with information sharing were the most valuable takeaway (24 percent).

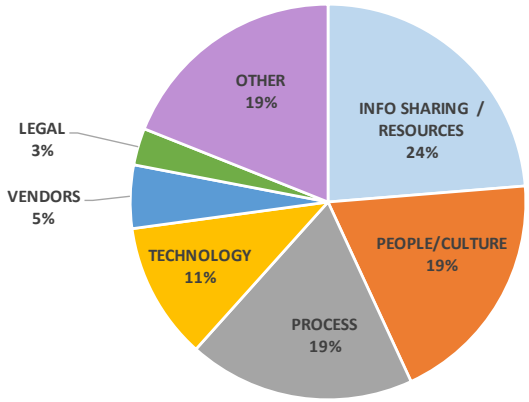

Figure 5: Distribution of "Most Valuable Takeaways" Comments on Participant Evaluations Organized by Topic

Table 4: Examples of "Most Valuable Takeaways" Listed on Summit Participant Evaluations

Info Sharing/Resources comments:

- "Networking with others. Finding out what other are doing with cybersecurity."
- "We have a long way to go but we are not alone. There are resources available to help us get where we need to be."
- "Resources - Many resources that are free for assistance."
- "I was not previously aware of Cyber Mutual Aid listing."
- "Opportunity to network in-person with experts not in my normal sphere."

People/Culture comments:

- "I believe the most valuable takeaways for me is that we are vulnerable due to all of the different access points and that it is not just strictly our IT dept's job. We all play a role."
- "Need to emphasize the value of budgeting for security measures to CEO and BOD."
- "Good info on how to make sure Management/Board/Legal need to be part of team."
- "Learned additional things we can do for insider threat."
- "Cultural shift that every employee is a part of cybersecurity."

Process Comments:

- "Co-ops need a cyber incident response plan similar to natural disaster, weather outages, and oil spill response."
- "Need to increase more internal controls - Administrator roles/passwords."
- "Planning to review, create and implement policies, controls, incident response plans."
- "Need for formal cyber security program."
- "How to continue or start cybersecurity plan."

Technology comments:

- "Segmenting."
- "Encrypting backups."
- "More focus on protecting OT systems."
- "Evaluate security with different systems to be sure employees have JUST the access they need to do their job function."
- "No co-op is too small to harden its system to ward off malicious cyber attacks."
- "Smart systems will be tied to cybersecurity."

Legal comments:

- "Legal Involvement - vendor contracts; Vendor Management"
- "Have knowledgeable corporate lawyer on cybersecurity, need to involve her more."

Vendor comments:

- "Vetting a Pen testing company"
- "Tools and questions to ask vendors when looking to do an assessment."
- "Better (more informed) RFP writing for IT services."

Other comments:

- "Learned valuable information about current cyber threat landscape."
- "More can always be done."
- "Cybersecurity will always be an ongoing process that takes TIME!!!"
- "Ukraine review"
- "NRECA is trying to supply good information to utilities."

Responses to the evaluation question "Where do you have the greatest need for more cybersecurity information or increased capabilities?" were organized into nine topics: people/training, people/staffing, process, technology, OT specific, information sharing/resources,

vendors, unsure, all areas. Summit participants indicated that more information related to People/Training was the greatest need (31 percent of comments) (Figure 6).

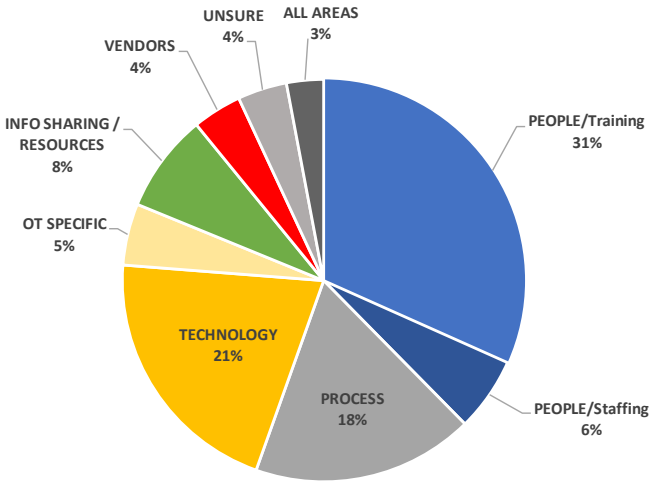

Figure 6: Distribution of "Greatest Need for More Information" Comments on Participant Evaluations Organized by Topic

Using the RC3 Cybersecurity Summits to Shape RC3 Program Design and Goals

Figure 7 provides a time series illustration of activities associated with the RC3 Cybersecurity Summits. Items in purple represent programmatic activities and items in green represent outreach and website activity. Many of the insights gained from the RC3 Summits were instrumental in focusing and shaping the RC3 Program roadmap, including what was created and when it was released.

For example, the RC3 Program used the analyses from the 2017 Summits to prioritize what cybersecurity controls would be emphasized in the RC3 Self-Assessment tool. Issues associated with the NIST CSF Identify function were a particular challenge for distribution cooperatives and the RC3 Self-Assessment focused on addressing these issues in the Identify section of the Self-Assessment tool. The 2017 Summits also revealed how challenging existing cybersecurity resources were for distribution cooperative staff to utilize. RC3 Program materials were designed to minimize these barriers. People and process challenges were repeatedly ranked higher than technology challenges, and the RC3 Program prioritized creating solutions that addressed people and process issues.

The need for general and technical training was a priority. This drove the creation of the RC3 SANS Voucher Program and developing new cybersecurity courses with content that was more

appropriately scaled to the needs of distribution cooperatives. Another issue that was raised repeatedly was the urgent need for higher levels of engagement from cooperative CEOs/GMs and increased understanding and awareness of cybersecurity risks by the Board of Directors. This prompted the RC3 team to increase the number of speaking engagements to CEO/GM audiences and Board of Director audiences to build the knowledge base needed to support leadership decisions on resource allocations for cybersecurity.

The very high number of cooperative staff without cybersecurity training that were responsible for cybersecurity at their cooperatives was revealed during the Summits. This prompted the focus on creating the RC3 Cybersecurity Guidebook series to create introductory cybersecurity training and awareness materials for non-IT staff.

In addition to driving RC3 Program direction, the Summits provided an ongoing pressure within the cooperative community to elevate cybersecurity discussions and awareness over the three years when the Summits were held. Across the country the RC3 team seeded conversations about cybersecurity, introduced resources to different regions of the country, and kept an ongoing stream of cybersecurity events and opportunities in front of the cooperative community so spur discussion and interest. The Summits provided the RC3 Program with a two-way megaphone – insights and guidance came into the RC3 Program from the Summits and RC3 Program opportunities and training went into the cooperative community through the Summits.

The Summits were also used to seed a market and increase awareness on key topics prior to the RC3 Program releasing those products. Two specific examples were the use of the brainwriting exercises to get cooperatives to start thinking about cybersecurity challenges before the RC3 Self-Assessment was released. By the time the RC3 Self-Assessment was released in December 2018, cooperatives were already eagerly looking forward to the tool to help them address the challenges they had already identified by participating in the Summits. Within the first three months after the RC3 Self-Assessment Toolkit was announced it was downloaded 330 times by 253 cooperatives.

The RC3 Program used the same tactic to prime the cooperative community for the release of the RC3 TTX Toolkit. The 2018 and 2019 Summits included discussions centered around incident response and insider threats. These discussions raised awareness and attention to the use of cybersecurity exercises to improve incident response capabilities. By the time the first set of cybersecurity TTX scenarios were released in the RC3 TTX Toolkit in August 2019, the cooperative community was ready and waiting for it. The RC3 TTX Toolkit was downloaded 249 times within the first few months of its release. The Summits provided an ideal format for advance marketing and getting cooperative buy-in to help shape the two toolkits and to anticipate them.

RC3 PROGRAM TIMELINE	2016		2017				2018				2019				2020			
	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec
2017 RC3 Cybersecurity Summits																		
Evaluate cybersecurity training options, create training format accessible to and appropriate for cooperatives. Identify host partnerships for Summits.																		
Develop and implement roll-out plan for RC3 Cybersecurity Summits																		
1st Summit - hosted at NREL, CO; # co-op attendees (# total attendees)			45 (58)															
2nd Summit - hosted at the University of Arkansas/SEEDS, AR; # co-op attendees (# total attendees)				39 (57)														
3rd Summit - hosted at the University of Illinois/ITI, IL; # co-op attendees (# total attendees)				32 (46)														
4th Summit - hosted at PNNL, WA; # co-op attendees (# total attendees)					28 (46)													
5th Summit - hosted with APPA at NRECA, VA; # co-op attendees (# total attendees)						46 (61)												
6th Summit - hosted at EPRI, TN; # co-op attendees (# total attendees)						36 (45)												
2017 Analysis of Summit data																		
Analyzed data from Summits and used results to inform RC3 Self-Assessment Program and RC3 TTX Toolkit efforts. Identified cybersecurity incident response as a breakout session topic for the 2018-2019 Summits. Identified need for pre-Summit training classes.																		
2018 RC3 Cybersecurity Summits																		
Identify host partnerships for Summits																		
7th Summit - hosted at Alaska Power Association, AK (including The CyberSecure My Business™ workshop); # co-op attendees (# total attendees)										20 (42)								
8th Summit - hosted at SNL, NM (including the CMU SEI Insider Threat Mitigation training session); # co-op attendees (# total attendees)										33 (47)								
9th Summit - hosted at Great River Energy, MN (including the CMU SEI Insider Threat Mitigation training session); # co-op attendees (# total attendees)										46 (53)								
10th Summit - hosted at INL, ID; # co-op attendees (# total attendees)											39 (50)							
11th Summit - hosted at Carnegie Mellon University, PA (including the CMU SEI Insider Threat Mitigation training session); # co-op attendees (# total attendees)												25 (37)						
NRECA Summits Are Catalyst for Co-op Discussions about Cybersecurity Risks; release																		
RC3 Cybersecurity Summits and Classes; landing page views									260	353	135	328	51	55	23	12	8	8

Figure 7: Timeline of RC3 Cybersecurity Summit Planning and Activities

Appendix B: RC3 Cybersecurity Self-Assessment

The RC3 Cybersecurity Self-Assessment tool was created in two phases. The first phase, completed under the RC3 Self-Assessment Research Program, focused on creating a research program that engaged cooperatives to help create, test, and refine the Self-Assessment questions, and improve the process used to facilitate completion of the Self-Assessment. The second phase, completed under the RC3 Online Self-Assessment License Program, created an online version of the tool hosted on the Axio360 platform operated by Axio Global, Inc. After the start of the Online Self-Assessment License Program, the RC3 team, in partnership with Axio, offered 7 training webinars, five of which were recorded, on how to use the online version of the RC3 Self-Assessment. Additional details on the structure and implementation of the Programs can be found in the final case study, "NRECA's RC3 Cybersecurity Self-Assessment Program", submitted to the DOE with the RC3 Program's final quarterly progress report on January 30, 2021. See Table 5 for a summary of motivations, and design principles and insights used to create the RC3 Self-Assessment Programs. The target audience for the RC3 Self-Assessment Programs was all small and mid-sized cooperatives.

RC3 Self-Assessment Research Program

The RC3 Self-Assessment Research Program was structured to allow cooperatives to apply under one of three categories but required each individual cooperative to submit a separate application whether the cooperative was applying as an individual cooperative or as part of a group/cluster. These categories were created after considerable discussions with the IAG, other cooperative staff, and within NRECA, to provide the widest flexibility for the RC3 Program to work with the largest number of members during the beta-testing effort.

- Category A – for distribution cooperatives to apply as an individual cooperative.
- Category B – for distribution cooperatives that applied as a group that would work together. This option leveraged and reinforced the Cooperation Among Cooperatives principle.
- Category C – for G&T cooperatives that provided direct cybersecurity services to their distribution cooperatives to apply as a group that included the G&T and a subset of their distribution cooperatives. This option leveraged and reinforced the existing cooperative infrastructure between G&Ts and their member cooperatives.

The application process was designed to be competitive so only those cooperatives that were highly motivated would be involved. It was important that this group of cooperatives be interested in helping other cooperative as this beta-group were intended to become champions for the Program. After a competitive application process, 36 cooperatives were selected to participate in the RC3 Self-Assessment Research Program as beta-testing cooperatives. All participants in the Program had to agree to have active participation by their CEO/GM, participate in 3 separate site visits from the RC3 Program team, attend a Lessons Learned workshop, and actively work to help the RC3 team improve the tool and, once completed,

promote the tool. These cooperatives worked with the RC3 Program team over the next 2 years to build the self-assessment tool.

The first site visit focused on completing a draft version of the RC3 Self-Assessment and providing feedback. The entire leadership team of the cooperative was required to participate in this site visit and the process was facilitated by the RC3 team and completed over a 2-day period. During the nine months that it took to complete the first site visits with the 36 cooperatives, the Self-Assessment tool was modified three times based on feedback from the participants. A final version of the RC3 Self-Assessment Toolkit was released in December 2018. Figure 8 and Figure 9 show examples of the results from an RC3 Self-Assessment. The final Toolkit consisted of three documents:

1. 2018 Reducing Risk in Cybersecurity: An RC3 Guide for Electric Cooperatives - Version 1.0 (Guide). The Guide is a Microsoft Word document and is the longest of the three documents. It provides detailed background information about the Self-Assessment questions (Figure 8).
2. 2018 RC3 Cybersecurity Self-Assessment Template - Version 1.0 (Template). The Template is a Microsoft Word document. It is an interactive document that contains all of the Self-Assessment questions and embedded drop-down menus to answer each question. There are a total of 133 cybersecurity control practices in the Template (Figure 9).
3. 2018 RC3 Cybersecurity Self-Assessment Scoring Worksheet - Version 1.0 (Scoring Worksheet). The Scoring Worksheet is a Microsoft Excel document. It is linked to the Template. Once the Template is completed, the answers are transferred to the Scoring Worksheet where the final results are calculated and illustrated in a series of graphics that help the user understand the results.

In the first three months after its release there were 330 downloads of the RC3 Self-Assessment Toolkit from the RC3 website by 253 cooperatives. This rapid success was a testament to the efforts made to create a 'market'. The RC3 Summits helped develop a broad awareness within the cooperative community of the value of the RC3 Program, and the RC3 Self-Assessment was one of the first major products released to benefit from all of the groundwork done in the previous years. As of the end of the RC3 Program's period of performance, there were 672 downloads of the RC3 Self-Assessment Toolkit by 391 cooperatives. The rate of downloads of the hardcopy RC3 Self-Assessment Toolkit slowed considerably after the release of the online version of the RC3 Self-Assessment in December 2019.

The second site visit focused on reviewing a Technical Assessment of each of the participating cooperative's Self-Assessment results from the first visit. The Technical Assessment was created by the RC3 team and Synopsis, Inc., the primary contractor helping the RC3 team with this effort. The third and final site visit involved completing the entire Self-Assessment a second time with the RC3 team there to help facilitate. This visit did not require the full participation of the leadership team though some of the cooperatives did chose to include their full teams.

Table 5: Motivations and Relevant Design Principles and Insights Used to Shape the RC3 Self-Assessment Programs

Motivations

RC3 Self-Assessment Research Program

- Leverage the insights from the RC3 Summits to create a tool that would address cooperative challenges.
- Design questions that were granular and specific so if a cooperative answered 'no' it would be clear what actions would need to be taken to get to a 'yes'.
- Structure the questions so it would be feasible to address some of the gaps within a 3-4 month timeframe.
- Create graphics that would be sensitive to progress so that even small steps forward would be visually apparent in the results.
- Use a competitive application process to identify champions that would help create the tool and promote its use.
- Structure the program to strengthen relationships between the participating cooperatives and their G&Ts, statewide association, or neighboring cooperatives.
- Utilize the Program as a platform to encourage, nurture, and facilitate spin-off actions within the cooperative community that would persist beyond the RC3 period of performance.

RC3 Online Self-Assessment License Program

- Utilize the lessons learned in the Self-Assessment Research Program to create improved training resources that would last beyond the RC3 period of performance.
- Structure the program to strengthen relationships between the participating cooperatives and their G&Ts and statewide associations.
- Create a user-friendly interface accessible to all staff.
- Create an online version that could transition to a commercial product that would last beyond the RC3 period of performance.
- Utilize the Program as a platform to encourage, nurture, and facilitate spin-off actions within the cooperative community that would persist beyond the RC3 period of performance.

Advance RC3 Program

- Nurture a pool of champions who would promote the RC3 Self-Assessment and the RC3 Program generally.

Relevant Design Principles and Insights

- Ensure the Self-Assessment questions emphasize all three pillars: people, process, and technology.
- Stick to the three A's. Design the program so it is affordable. Meet them where they are by creating an appropriately scaled Self-Assessment that can be completed and useful to a cooperative whether it has no inhouse IT staff, dedicated IT staff with limited cybersecurity skills, or an already existing strong internal cybersecurity program and can be used by staff without a high level of skill or large amounts of time. Host the Self-Assessment on cooperative.com so it is accessible to all cooperatives.
- Leverage the cooperative principles and the cooperative infrastructure and, if possible, reinforce both.
- Require senior leadership engagement at some level.
- Advance the knowledge, skills, and abilities of the participants and increase their exposure to threat information and cutting-edge cybersecurity practices and techniques.
- Ensure the self-assessment is relevant to all job roles that impact cybersecurity, including staff responsible for interacting and contracting with third-party vendors.
- Create solutions and program designs that can persist beyond the RC3 Program's period of performance.
- Integrate peer-to-peer options.

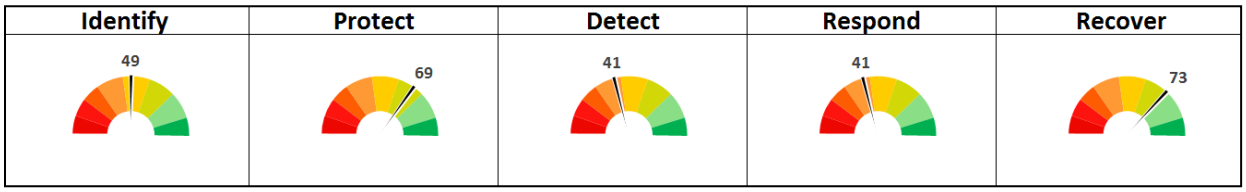

Figure 8: Example of Summary Results from an RC3 Self-Assessment

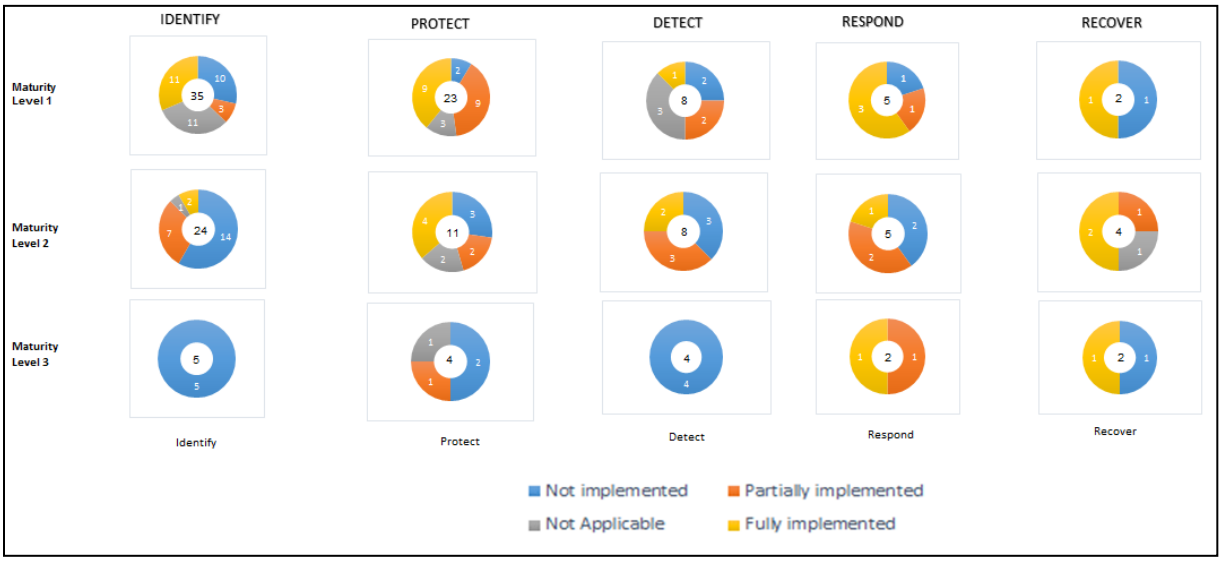

Figure 9: Examples of Summary and Detailed Results from an RC3 Self-Assessment

RC3 Online Self-Assessment License Program

The RC3 Program purchased 100 licenses from Axio to use their Axio360 platform and began working with Axio in late 2018 to create the online version of the RC3 Self-Assessment. The online version provided superior features including:

1) An interactive dashboard with visualizations summarizing the *RC3 Self-Assessment* results;
2) Tools to improve collaboration with a cooperative's internal team members to ensure everyone is working on the same version;
3) Unlimited access for all team members within a cooperative;
4) A capability to record action items linked directly to each cybersecurity question, set target dates for actions, and create summary lists of what's due. These features will enable a cooperative to track progress on tasks assigned to individual staff;

5) An ability to develop a "target goal" for each *RC3 Self-Assessment* question, and a dashboard to visualize comparisons between current responses and target goals to monitor progress;
6) Tools to improve version control and make updates over time;
7) Visual tracking of results and progress over time; and,
8) A printed summary report that includes a wider variety of results graphics than currently available in the hardcopy version.

The online version debuted in March 2019 and was tested by a group of cooperatives as part of a pre-conference workshop the day before NRECA's TechAdvantage conference. Feedback from workshop participants was integrated into the online version before the RC3 Online Self-Assessment License Program launched.

The RC3 Online Self-Assessment License Program was structured very differently from the Research Program. Only "*Group Licenses*" were awarded. Each Group License had to consist of at least five (5) cooperatives, and no more than thirty (30) cooperatives.[5] All members of the Group License had to be an owner/operator electric cooperative or a Statewide Association. If an individual cooperative wanted to participate in the RC3 Online Self-Assessment License Program, the cooperative must be part of a Group License application. All the members of the Group License must agree on and designate one member as the "*License Lead.*" All License Lead organizations were required be voting members of NRECA.

There were three ways cooperatives could assemble into a Group:

- Category A: Individual distribution and G&T cooperatives can form a Group and designate one member of the Group, either a distribution or G&T cooperative, as the License Lead.
- Category B: A G&T cooperative can assemble its member distribution cooperatives into a Group with the G&T as the License Lead;
- Category C: A Statewide Association can assemble its member distribution and G&T cooperatives into a Group with the Statewide as the License Lead.

This structure was intentional to leverage the existing cooperative infrastructure with a longer-term goal of building a relationship structure and encouraging the cooperative community to innovate and create solutions that would survive beyond the RC3 Program's period of performance.

The first opportunity to apply to the RC3 Online Self-Assessment License Program for a license, Round 1, opened in October 2019 and closed in December 2019. The RC3 team anticipated that this Round would include applications from all of the members who had been tracking the RC3 Program closely and were aware that an online version would be released soon. There were 326 cooperatives accepted into the Program in Round 1 that used fewer than 30 licenses to cover them. The second opportunity, Round 2, opened in February 2020 and closed May 15, 2020.

[5] Exceptions to this were made on a case-by-case basis under unique circumstances.

Another 165 cooperatives joined the Program in Round 2 and used another 30 licenses leaving 40 licenses for Round 3. The third and final round for applications, Round 3, was announced in August 2020 and closed in October 2020 with 42 additional cooperatives joining the Program.

During this time the COVID-19 pandemic hit, accompanied by travel restrictions, and the online version of the RC3 Self-Assessment provided a level of flexibility that was well suited for a work-from-home reality.

RC3 Self-Assessment Training Webinars

To keep the momentum up similar to the energy created by the RC3 Summits, the RC3 Program held its first training webinar to introduce members to the online platform and how to use it in February 2020. This webinar had more than 240 participants. An additional five training webinars, each focused on a different part of the RC3 Self-Assessment, were offered in May, June, and July 2020 and were recorded and made available to cooperatives on the RC3 webpage on cooperative.com. These training webinars were 90 minutes long and included question and answer opportunities throughout the webinar and at the end. More than 500 cooperatives attended at least one of the first six webinars. The final webinar was jointly hosted by Seven States Power Corporation, a cooperative serving utilities in the Tennessee Valley Authority service territory. This webinar was 3 hours long and included a vendor, NRECA, Public Power, and Axio and was limited to Seven States' membership. (Table 6Table 1)

Table 6: Training Webinars for the RC3 Online Self-Assessment

Date	Webinar Topic	Registered	Attended
10 Feb 2020	RC3 Self-Assessment Webinar Series: Introduction to the RC3 Self-Assessment on the Axio Platform	294	248
20 May 2020	RC3 Self-Assessment Webinar Series: Introduction to the RC3 Self-Assessment on the Axio Platform (second opportunity)	284	240
26 May 2020	RC3 Self-Assessment Webinar Series: Introduction to the Identify Section of the RC3 Self-Assessment – Part I	216	183
9 Jun 2020	RC3 Self-Assessment Webinar Series: Introduction to the Identify Section of the RC3 Self-Assessment – Part II	266	212
23 Jun 2020	RC3 Self-Assessment Webinar Series: Introduction to the Protect Section of the RC3 Self-Assessment	260	213
14 July 2020	RC3 Self-Assessment Webinar Series: Introduction to the Detect, Response, and Recover Sections of the RC3 Self-Assessment	332	255
1 Sept 2020	CyberSecure: A Virtual Cybersecurity Workshop for Electric Utilities (In partnership with Seven States Power Corporation, TN. Participation in this webinar was limited to Seven States' member utilities.)	46	39

Impact and Lessons Learned from the RC3 Self-Assessment Programs

> "It wasn't so much that I didn't think it was important, or that there would be no value, I just didn't have any sense of what the value would be. And when I sat through that interview process, that Q&A period, I really saw the value of it. I really saw the value of it then."
>
> Comment from a General Manager
> of a ~3,400 meter cooperative after completing
> the RC3 Self-Assessment with the cooperative's leadership team

The RC3 Self-Assessment Programs have been a great success. There are 656 cooperatives that have either downloaded the RC3 Self-Assessment Toolkit or applied to the RC3 Online Self-Assessment License program. This represents 73 percent of NRECA's member utilities. Of the 533 cooperatives that completed an application to participate in the RC3 Online License Program, 206 have started an online self-assessment and 89 have completed at least one self-assessment on the Axio platform. Figure 10 provides a time series illustration of activities associated with the RC3 Self-Assessment Programs to illustrate the flow of events over the period of performance. Items in blue represent programmatic activities and items in green represent outreach and website activity.

While originally developed for a target audience of small and mid-sized distribution utilities, the RC3 Program has received consistent feedback from larger distribution utilities and G&Ts who have found the RC3 Self-Assessment useful. One of the larger distribution cooperatives explained, "We find the RC3 right-sized and more manageable for an organization of our size," and one of the G&T cooperatives said, "We used the RC3 self-assessment method and have found it to be an effective method of quickly identifying areas of strength and weakness in a security program."

The RC3 Self-Assessment was intentionally designed to require participation from many of the other staff roles in a cooperative. Another CEO from a distribution cooperative with ~6,700 meters that participated in the RC3 Self-Assessment Research Program explained:

> "After you [the RC3 Team] came out for our site visit, and we went through that exercise, we actually thought we were pretty good before you came, but there were about 4-5 things discovered while you were here as we talked with the senior group that our IT guys didn't have a clue were going on. We realized as a company everyone needs to be on the same page with cybersecurity. We've taken some steps to try and correct that problem."

Similar comments were made by other participants. Once the leadership went through the process as a team, the first seeds of a cultural shift were planted. Staff realized why they were there, and that a lot of cybersecurity practices and controls were not technical and not the responsibility of an IT job role.

A survey was sent to the 209 staff members who participated in the beta-testing self-assessments and 113 responses were sent back from 33 of the 36 participating cooperatives. Below are a few of the comments made to some of the questions and the job role of the person responding.

Question: At the outset, did you understand the rationale and value of your co-op participating in a cybersecurity self-assessment?

- After our discussion I was able to realize how important all the departments are in supporting and bringing to light potential issues we will face. – Finance/Accounting

Question: Did your opinion of the value of the self-assessment process change from the start of the process to the conclusion -- after you discussed the final results?

- I felt the process would be valuable but was pleasantly surprised with the amount of discussion with the staff and the value we received. – CEO/GM
- The survey became more valuable than I expected it to be – CEO/GM
- Discovered a few weaknesses. – GM/CEO
- I had more value in the process as we went through the day – GM/CEO
- We have more issues than I might have thought. – Finance/Accounting/Admin/GM/CEO
- There were some interdepartment issues I was not aware of – IT
- Helped us see the holes in our system by department. – IT
- It emphasized how cybersecurity is everybody's job, not just the IT folks. _ IT
- I figured some members on our staff would resist getting involved. I was happy to see everyone contribute to the discussions and to see the value of the self-assessment. – IT
- It helped me understand how important it is – Operations/Safety
- I can appreciate that there is a need for more security. – Operations/Engineering
- Changed for the better; There is a lot of stuff our contract IT takes care of that we had no clue about – Engineering/Safety
- Through examples and suggestions shared in the workshop we were led to think more thoroughly about just how far cyber security extends in our work. – Member Services/Admin/Media & Communications
- It makes you think about your processes and being more protective of your everyday tasks – Member Services/Operations/Media & Communications
- We have not gotten our final results yet. But, the questions brought up things we would not have thought about. – Member Services/Media & Communications
- Realized even moreso the importance of the self-assessment. – Administration
- Saw the value in each department contributing because of how cyber security affects all of us – Administration

Question: Did you learn anything new (or anything that surprised you) about cybersecurity or about your cooperative's cybersecurity efforts during the self-assessment?

- Learned more ways we are vulnerable – CEO/GM
- I learned many things new with cybersecurity. We need to take steps to inventory our equipment, create better passwords, and know who has access to our members information. I also know that all hacks can not be prevented but we can definitely make it harder for the thieves to enter. – GM/CEO

- we are lacking – GM/CEO
- I learned that management needs to communicate better. – GM/CEO
- overall importance of it, and the fact that it will be forever in our strategic plans going forward – GM/CEO
- We have allocated resources but we are still not getting the bases covered – GM/CEO
- How much we have to depend on people, not just technology for Cyber Security - IT
- It had more value than I realized – IT
- I do not work with any of the outside vendors, and had no idea how much of our sensitive information was out there. – IT
- Absolutely....I just realized how much the protection against cyber threats is an ever-changing process. It really made me think hard about where our weaknesses are. – Finance/Accounting
- The amount of time cyber attacks were inside your system before being detected – Administration
- How easy it is for hackers to get into networks – Operations
- The knowledge of the people and the eye opening information that came from assessment alone. – Engineering
- How little documentation we had on devices connected to the system. – Engineering

One of the main lessons learned from the RC3 Self-Assessment Programs was the process of delivering and completing the RC3 Self-Assessment was as important of a product as the self-assessment tool itself. The availability of an online version of the Self-Assessment was fortuitous in timing, given the shift to a work-from-home reality during the COVID-19 pandemic, but the work-from-home situation made it more difficult for the cooperatives to assemble and build a 'team' within their leadership to complete the Self-Assessment. Many took a one-on-one approach to work with the relevant staff members and this diminished some of the power of everyone realizing cybersecurity is a whole-of-organization effort. When all the leadership are able to assemble at the same time and grapple with the questions together there is a deeper exploration and discovery of the potential gaps.

The incredibly strong response to the training webinars also made us realize that many of the cooperatives are ready to take this step but need more of an ongoing support infrastructure to continue to make progress.

Last we were encouraged by the initiative shown by the cooperative community to take the RC3 Self-Assessment and start to create their own program efforts around it. This was a primary goal of the RC3 Program from the beginning, to intentional design the RC3 Program products and efforts so they would encourage and support spin-off efforts. The lesson here is that there are benefits to intentionally structuring the RC3 Program and actively encouraging members to 'own' the products. The RC3 team strongly believe the design of the RC3 Program helped contribute to the independent innovation efforts cooperatives are now demonstrating to improve their cybersecurity resilience.

RC3 PROGRAM TIMELINE	2016		2017				2018				2019				2020			
	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec
RC3 Self-Assessment																		
Create hard-copy of RC3 Self-Assessment Toolkit																		
Review resources, define requirements with input from IAG, create draft RC3 Self-Assessment.																		
Develop criteria for the RC3 Self-Assessment Research Program to select cooperatives to deploy, test and refine the RC3 Self-Assessment.																		
Complete 3 alpha-field tests of the draft RC3 Self-Assessment, modify Self-Assessment based on field testing.																		
Release Program Opportunity Announcement and select Cohort #1 cooperatives for beta-testing the RC3 Self-Assessment; # selected (# applications received)				16 (43)														
Conduct first of three site visits with the Cohort #1 beta-test cooperatives. Modify Self-Assessment based on field testing.																		
Develop methodology for analyzing RC3 Self-Assessment results and creating a Technical Assessment report for the Cohort #1 beta-cooperatives																		
Lessons Learned Workshop with RC3 Self-Assessment Cohort #1 cooperatives to provide peer-to-peer support and networking between the Cohort #1 beta-cooperatives.																		
Complete Technical Assessments, schedule and complete 2nd site visits with Cohort #1 beta-cooperatives to review results.																		
Make final revisions to RC3 Self-Assessment and associated materials and release Toolkit to cooperative community December 2018.										Release								
RC3 Self-Assessment Toolkit; downloads.										18	312	75	57	80	27	54	31	18
Schedule and complete 3rd and final site visits for Cohort #1 beta-cooperatives to redo their RC3 Self-Assessment and evaluate progress.																		
Create an Online Version of RC3 Self-Assessment																		
Work with IAG to develop specifications for a graphical user interface/online version of the RC3 Self-Assessment. Integrate lessons learned from the RC3 Self-Assessment field tests.																		
Issue RFP and select vendor partner to host an online version of the RC3 Self-Assessment																		
Develop and implement roll-out plan for RC3 Online Self-Assessment Program																		
Create an online version of RC3 Self-Assessment and release it at NRECA's TechAdvantage conference March 2019											Release							
Create an application process for the RC3 Online Self-Assessment Program, Cohort #2																		
Opportunity Announcement: *RC3 Online Cybersecurity Self-Assessment License Program (Round 1);* downloads														107	25			
Collect RC3 Online Self-Assessment Program applications for Round 1 and implement Program; # accepted (#applications														326 (392)				
Opportunity Announcement: *RC3 Online Cybersecurity Self-Assessment License Program (Round 2);* downloads															37	3		
Update Opportunity Announcement: *RC3 Online Cybersecurity Self-Assessment License Program (Round 2 extended);* downloads																50	19	
Collect RC3 Online Self-Assessment Program applications for Round 2 and implement Program; # accepted (# applications																165 (253)		
Opportunity Announcement: *RC3 Online Cybersecurity Self-Assessment License Program (Round 3)* downloads																	19	23
Collect RC3 Online Self-Assessment Program applications for Round 3 and implement Program; # accepted (# applications																		42 (44)
Provide Training for the Online RC3 Self Assessment: Webinar Series																		
Webinar: *Introduction to the RC3 Self-Assessment on the Axio Platform;* attendees															248			
Repeat Webinar: *Introduction to the RC3 Self-Assessment on the Axio Platform;* attendees																240		
Introduction to the RC3 Self-Assessment on the Axio Platform; website pageviews and slide downloads																112	87	37
Webinar: *Introduction to the Identify Section of the RC3 Self-Assessment – Part I;* attendees																183		
Introduction to the Identify Section of the RC3 Self-Assessment – Part I; website pageviews and slide downloads																52	63	18
Webinar: *Introduction to the Identify Section of the RC3 Self-Assessment – Part II;* attendees																212		
Introduction to the Identify Section of the RC3 Self-Assessment – Part II; website pageviews and slide downloads																17	41	11
Webinar: *Introduction to the Protect Section of the RC3 Self-Assessment;* attendees																213		
Introduction to the Protect Section of the RC3 Self-Assessment; website pageviews and slide downloads																	29	6
Webinar: *Introduction to the Detect, Response, and Recover Sections of the RC3 Self-Assessment;* attendees																	255	
Introduction to the Detect, Response, and Recover Sections of the RC3 Self-Assessment; website pageviews and slide downloads																	21	11
Webinar: *CyberSecure - A Virtual Cybersecurity Workshop for Electric Utilities;* attendees limited to Seven States' member																	39	
Complete RC3 Self-Assessment Case Study Final Report																		
Promote RC3 Self-Assessment and build a user community																		
Develop and implement roll-out plan for RC3 Self-Assessment																		
Develop and host a series RC3 Cybersecurity Summits to collect information on cybersecurity and to promote the RC3 Self-Assessment and the RC3 Program; # cooperatives (total #			37 (58)	52 (103)	25 (46)	67 (106)				66 (158)	23 (57)	21 (43)						
Integrate insights and lessons learned from cooperatives during the RC3 Summits into the RC3 Self-Assessment.																		
RC3 Program Overview - TechAdvantage conference session presentation																		
Value of a Cybersecurity Self-Assessment - TechAdvantage conference session presentation																		
RC3 Cybersecurity Self-Assessment DIY Toolkit - TechAdvantage one-day training session																		
RC3 Self-Assessment Toolkit; landing pageviews.										29	1026	309	255	520	365	629	340	354
RC3 Self-Assessment Program: What the CEOs and GMs Have to Say About Cybersecurity; website pageviews and article								63	57	50	21	19	10	23	1	32	1	0
RC3 Self-Assessment Program – Lessons Learned; landing pageviews									34	133	46	36	0	60	27	32	19	14
RC3 Self-Assessment Program – Lessons Learned: CEO Leadership is Critical to a Strong Culture of Cybersecurity; article downloads									12	32	9	7	0	7	1	4	1	3
RC3 Self-Assessment Program – Lessons Learned: Engaged Employees are a Cooperative's First Line of Defense Against Cyberattacks; article downloads										34	8	3	1	9	2	3	0	0
Co-ops Can Gauge Vulnerabilities With New Cybersecurity Self-Assessment Tool; article pageviews											421	26	1	5	1	1	3	1
RC3 Self-Assessment Toolkit Factsheet; downloads											234	117	60	118	42	39	21	18

Figure 10: Timeline of RC3 Self-Assessment Program Planning and Activities

Appendix C: RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit

Electric cooperatives are familiar with incident planning exercises, designed to sharpen capabilities in handling electric service outages, thanks to requirements from the Federal Emergency Management Administration (FEMA) and the U.S. Department of Agriculture's Rural Utilities Service (RUS). Such exercises test a utility's response to a hypothetical – but realistic – physical disaster that severely disrupts service, such as a hurricane or ice storm.

But, while electric cooperatives have been responding to physical outages since electric lines were first energized, cyberattacks are relatively new and ever-changing. Cooperative staff may lack experience in detecting or resolving cyber incidents, and roles and responsibilities may be poorly or insufficiently defined or understood.

The idea of a tabletop exercise on cybersecurity designed for cooperatives emerged during development of the RC3 Program, and specifically from a question asked by Andrea Christoffer, manager of marketing and communications at Federated Rural Electric Association of Jackson, Minnesota. Christoffer attended a cybersecurity presentation at NRECA's 2016 CONNECT conference on the cybersecurity threat facing electric cooperatives. "That talk left me feeling a little freaked out," she says. "I realized that we'd be in a world of hurt if we were hit." Christoffer approached the RC3 Program team after the presentation to discuss the value of developing cybersecurity tabletop exercises (TTX) appropriate for smaller cooperatives. The initial efforts were put on hold after staffing changes at the DOE and the RC3 Program's primary contact on the effort moved to another agency.

In 2017, Federated REA applied to participate in the RC3 Self-Assessment Research Program. Working through the RC3 Self-Assessment gave Christoffer and her colleagues confidence that they could build stronger cyber defenses. But she wanted to know what more could be done to reinforce the right habits and continue to change attitudes at the cooperative, and the initial discussions around creating a cybersecurity TTX were revisited.

Recognizing the need for more resources to help cooperatives with response and recovery, based on the insights gained from the RC3 Summits, the RC3 Program set out to build an RC3 Cybersecurity TTX Toolkit that could be used by cooperatives to create a structured opportunity for cooperatives to test their staff's ability to assess and respond to a potentially damaging cyber incident. Each tabletop exercise was designed as a cross-functional team project, with representatives of different departments of the cooperative working together on a solution. Table 7 provides a summary of motivations and design principles and insights used to create the RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit. The target audience for the RC3 TTX Toolkit was all distribution cooperatives.

The RC3 Program hired Delta Risk, LLC, to work with the RC3 team to help build the toolkit and assembled a research cohort of three electric cooperatives to help design and test the exercise scenarios and the do-it-yourself (DIY) toolkit materials. The test cooperatives selected represented three levels of in-house staff skill: cooperatives with no IT staff, cooperatives with IT staff but limited cybersecurity expertise, and cooperatives with staff that had cybersecurity training. The TTX team visited the three representative cooperatives to gather data that was then used to formulate incident scenarios tailored to these three levels of skill and resources.

Table 7: Motivations and Relevant Design Principles and Insights Used to Shape the RC3 Cybersecurity Tabletop Exercise Toolkit

Motivations	**Relevant Design Principles and Insights**
• Build stronger incident response skills, and policies and procedures. • Facilitate creation of cybersecurity incident response teams. • Elevate awareness of the important of every staff member in cyber incident response. <u>Advance RC3 Program</u> • Nurture a pool of champions who would promote the RC3 Program generally.	• Ensure the TTX scenarios emphasize all three pillars: people, process, and technology. • Stick to the three A's. Design the TTX Toolkit so it is affordable and minimizes the need to hire external support. Meet them where they are by creating three categories of exercise scenarios appropriate for different levels of maturity, and developing all the associated materials to enable any cooperative, regardless of their internal skills, to complete the exercise. Host the Toolkit on cooperative.com so it is easily accessible to all cooperatives. • Leverage the cooperative principles and the cooperative infrastructure and, if possible, reinforce both. • Strongly encourage senior leadership participation. • Advance the knowledge, skills and abilities of the participants. • Ensure the exercises are relevant to all job roles that impact cybersecurity, including staff responsible for interacting and contracting with third-party vendors. • Increase awareness of the need to define cybersecurity responsibilities clearly within the organization and with third parties. • Create solutions and program designs that can persist beyond the RC3 Program's period of performance. • Integrate peer-to-peer options.

Twelve difference cybersecurity scenarios were created, 4 for each of the three skill levels. After considerable discussion, the RC3 team decided not to release all of the scenarios at once, but to aim for a new release every quarter. The goal was to extend the shelf-life of the scenarios and to maintain a high level of engagement with the members over a longer period of time. The final

version of the Toolkit complete with the first set of 3 scenarios was released in August 2019. Figure 11 shows the timeline of the four released and the download and website activity metrics associated with the RC3 TTX Toolkit. Items in gold represent programmatic activities and items in green represent outreach and website activity. Since its initial release, the RC3 TTX Toolkit has been downloaded more than 750 times by 216 cooperatives.

RC3 PROGRAM TIMELINE	2016		2017				2018				2019				2020			
	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec
RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit																		
Create a hard-copy do-it-yourself (DIY) RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit																		
Analyze input from the IAG, cooperatives, and the RC3 Cybersecurity Summit series to identify core needs for a cybersecurity tabletop exercise (TTX)																		
Issue RFP and select vendor partner to create an RC3 Cybersecurity TTX Toolkit																		
Develop criteria and select beta-testing cooperatives to help design and test the TTX Toolkit																		
Conduct initial site visits to develop the TTX scenarios																		
Draft 12 TTX scenarios appropriate for 3 different cybersecurity maturity levels																		
Conduct field tests using the draft TTX scenarios and Toolkit documents																		
Integrate lessons learned from field tests and complete drafts of RC3 TTX Toolkit documents																		
Promote RC3 TTX Toolkit and create a user community																		
Develop and implement roll-out plan for RC3 TTX Toolkit																		
Utilize the RC3 Cybersecurity Summits to build awareness on how to use cybersecurity exercises, and to promote the RC3 TTX Toolkit and the RC3 Program, # attendees (#										66 (158)	23 (57)	21 (43)						
Cybersecurity Tabletop Exercises – Lessons Learned from Co-ops - TechAdvantage conference session presentation																		
Tabletop Exercises in Cybersecurity Help Cooperatives Prepare for "the Real Thing"; article pageviews											16	15	51	17	11	44	43	56
RC3 Cybersecurity TTX Toolkit - Factsheet; downloads												23	48	34	5	71	49	63
RC3 Cybersecurity TTX Toolkit - FAQ; downloads												13	31	19	2	36	21	35
RC3 Cybersecurity TTX Toolkit; landing pageviews													745	315	211	397	374	349
New NRECA Toolkit for Distribution Co-ops Geared to Close Cybersecurity Gaps; article pageviews													96	46	21	46	33	44
Release RC3 Cybersecurity TTX Toolkit																		
Complete final edits and released first set of 3 TTX scenarios													Release					
Complete final edits and released second set of 3 TTX scenarios																Release		
Complete final edits and released third set of 3 TTX scenarios																	Release	
Complete final edits and released fourth and final set of 3 TTX scenarios																		Release
RC3 Cybersecurity TTX Toolkit; downloads													372	110	42	113	81	62
Complete RC3 Cybersecurity TTX Summary Report																		

Figure 11: Timeline of RC3 TTX Toolkit Planning and Activities

Impact and Lessons Learned from the Three Cooperatives

As part of the Toolkit development process, the RC3 team returned to the three cooperatives to observe as the cooperative staff used the Toolkit. Each cooperative selected a facilitator from its staff to lead the exercise and spent an average of one and one-half hours working through their tabletop exercise using the TTX materials. After the exercise, the RC3 team interview the three cooperatives. All of the cooperatives reported that the exercise was productive in terms of raising awareness and pushing the staff a little out of its comfort zone to confront its readiness to respond to a cyber emergency.

One of the cooperatives said that the RC3 TTX scenario – in which a malicious attachment led to a cybercriminal taking over the cooperative's network and demanding a ransom – was more challenging than one that the cooperative would have created on its own. "NRECA's work on the tabletop exercise was amazing," explained the staff member. "The scenario was both realistic and it scared us half to death – which is a good thing." He said that the exercise underscored the need to do a better job of testing system back-ups and disaster recovery plans. The response of the staff to the exercise was seen as pay-off for its investment in making cybersecurity a positive part of the cooperative culture.

"While we were stressing cybersecurity, and I had support from senior management, I think many employees looked at it as something they just had to do – that cybersecurity simply meant they could not have access to things. I was concerned that employees were not taking the threat seriously enough," explained the second cooperative. "So, I was delighted when we were recommended for participation in the RC3 tabletop exercise project."

The tabletop exercise "accomplished just what I had hoped for" explained the staff member. The scenario involved the discovery of a USB device that no one recognized that had been inserted into a human resources computer. As the team discussed the possible ramifications of an intruder using the USB to collect payroll information or member data, "it dawned on everyone just how serious this could be," said the staff member. "The possibility of someone messing with people's money – that gets everyone's attention."

The third cooperative, Federated REA who initiated the effort, selected a member of the marketing team to serve as the exercise facilitator. "The people who prepared the exercise did it with the characteristics of a small cooperative in mind. Thanks to the prepared slides and the talking points, you don't have to be an IT expert to talk through technical topics in a productive way," said one of the staff members.

The tabletop team included the general manager, communications, office and operations managers, the accountant and two linemen, and "everyone participated very well, not one person held back," says Christoffer. "The NRECA folks observing us commented that we have a good dynamic. I think that's the trait of a small co-op – we have good teamwork."

But, not every member of the team had bought in to the importance of cybersecurity before the exercise. One staff member noted that during the discovery process with Delta Risk in the first visit, "what one of the linemen said was an eye opener. He said that as linemen, they didn't care about cybersecurity. But after the tabletop, his view had changed. He said, 'Oh, I can see that we do need to know about cybersecurity. It's not just an inside problem.' So, there has been a little bit of a culture shift because of this project," explained the staff member.

Appendix D: RC3 SANS Voucher Program

A stark reality today is that every organization, no matter how big or small, is exposed to cyber risks that are continually changing. This shifting threat landscape is coupled with a severe domestic and global workforce shortage in cybersecurity professionals, especially those trained in ICS or OT cybersecurity. For utilities in rural areas, this workforce shortage is particularly acute as many of the existing cybersecurity professionals are unwilling to relocate to rural communities. These challenges require tailored solutions. Rather than focusing on how to recruit from a limited pool of cybersecurity professionals, the RC3 Program focused on helping existing utility staff gain access to training and education that would help them assess vulnerabilities in their systems and implement controls to counter the evolving threats. The RC3 SANS Voucher Program was one of the training programs created to help address cybersecurity skills gaps within the cooperative community. The target audience for the RC3 SANS Voucher Program was staff from distribution cooperatives with a limited number of IT and/or cybersecurity staff and that were early in their cybersecurity program development. A second audience was staff from larger distribution cooperatives and/or G&T cooperatives that were more advanced in their cybersecurity program development and were interested in helping other cooperative staff improve their cybersecurity skills.

SANS Institute is a world-renowned for-profit cybersecurity training, certification, and research company (https://www.sans.org/). At the time the RC3 SANS Voucher Program was created, a 5-day in-person SANS course cost more than $6,000 per student, which was out-of-reach for many electric cooperatives. In addition, it was difficult for cooperative staff to leave their utility for a week to take a 5-day in-person course.

SANS, in partnership with the Center for Internet Security (CIS), offers an Aggregate Buy program that enables eligible organizations to purchase groups of vouchers for OnDemand and Live Online classes at approximately 50% of standard prices. The RC3 Program purchased 183 vouchers through this program in 2017 and 2018, and created a training program using the vouchers and built on cooperative principles. See Table 8 for a summary of motivations and design principles and insights used to create the RC3 SANS Voucher Program.

In addition to offering cooperative employees opportunities to learn from leading cybersecurity experts, the Program was structured to foster peer-to-peer information sharing. Participants were required to join small-group discussion conference calls while taking courses, and to use their newly acquired knowledge to benefit not just their own cooperative, but also other cooperatives around the country. This kind of collaboration supports Cooperative Principal #6: Cooperation Among Cooperatives. Based on comments in the evaluation forms and numerous anecdotes, the discussion groups were one of the most beneficial elements of the program.

Using a competitive application process, the RC3 Program made course vouchers available at no charge to employees of NRECA-member electric cooperatives. On average NRECA's distribution cooperatives have approximately 24,300 consumer-members. More than 75% of the

Program participants were from cooperatives serving less than 50,000 consumer members, and more than 50% were from cooperatives serving less than 24,300 consumer members.

The Program was administered in three phases, each lasting five to six months, to provide multiple participation opportunities. Participants of each phase were referred to as a Cohort. The RC3 Program opened the application process for Cohort #1 in the first quarter (Q1) of calendar year (CY) 2018, the Cohort #2 application process opened in CY 2018 Q3, and the final cohort, Cohort #3, applications opened in CY 2019 Q2. Cohort #1 participants started in late April 2018 and met in their groups through October of 2018. Cohort #2 started in late January 2019 and met through July 2019, and Cohort #3 started in late August 2019 and ran through January 2020. The RC3 SANS Voucher Program ended in January 2020 when participants in the final cohort completed their courses.

Figure 12 provides a time series illustration of activities associated with the RC3 SANS Voucher Program to illustrate the flow of events over the period of performance. Items in pink represent programmatic activities and items in green represent outreach and website activity.

Across the three cohorts the RC3 SANS Voucher Program provided training to 122 cooperative employees at 114 cooperatives located across 40 states.

RC3 PROGRAM TIMELINE	2016		2017				2018				2019				2020			
	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec	Jan - March	April - June	July - Sept	Oct - Dec
RC3 SANS Voucher Program																		
Create a cooperative cybersecurity training program around SANS course vouchers																		
Analyzed results from Cybersecurity Summits and input from IAG to identify training needs that were not currently met by existing cybersecurity courses																		
Evaluated options and purchase vouchers for online SANS cybersecurity training courses																		
Identified Program goals and developed a training roadmap based on available SANS courses																		
Created selection criteria and application materials																		
Opportunity Announcement: RC3 *SANS Voucher Program - Q&A;* downloads							320		7	13	1	8	0	11				
Collect RC3 SANS Voucher Program applications for Cohort 1; # accepted (# applications received)								42 (140)										
Work with Cohort 1 until completion of program																		
Purchased a second set of SANS vouchers for cohorts 2 and 3																		
Evaluated lessons learned from Cohort #1, make program improvements																		
Opportunity Announcement: RC3 *SANS Voucher Program Cohort #2;* downloads										101	10	6						
Collect RC3 SANS Voucher Program applications for Cohort #2; # accepted (# applications received)										36 (75)								
Work with Cohort 2 until completion of program																		
Evaluated lessons learned from Cohort #2, make program improvements																		
Opportunity Announcement: RC3 *SANS Voucher Program Cohort #3;* downloads												139	19	11	11	7	4	4
Collect RC3 SANS Voucher Program applications for Cohort 1, # accepted (# applications received)													36 (127)					
Work with Cohort 3 until completion of program																		
Promote RC3 SANS Voucher Program and create a user community																		
Develop and implement roll-out plan for RC3 SANS Voucher Program																		
Cooperatives Are Gaining Cybersecurity Skills with RC3 SANS Voucher Program ; article downloads											7	36	12	9	4	2	2	1
Beyond Passwords and Firewalls: Cybersecurity Tactics for Today's Co-op - TechAdvantage conference session																		
Complete RC3 SANS Voucher Program Final Report																		

Figure 12: Timeline of RC3 SANS Voucher Program Planning and Activities

Table 8: Motivations and Relevant Design Principles and Insights Used to Shape the RC3 SANS Voucher Program

Motivations	**Relevant Design Principles and Insights**
• Advance the level of cybersecurity skills for cooperative staff who had limited cybersecurity training, especially staff from small and mid-sized cooperatives. • Incentivize and train cooperative staff to take actions to identify and address vulnerabilities in their systems. • Build a stronger trusted peer-to-peer network between cooperative staff that they could utilize after the Program ended. • Elevate awareness of the value of investing in technical cybersecurity training within the cooperative community. <u>Advance RC3 Program</u> • Nurture a pool of champions who would promote the RC3 Program generally.	• Ensure the Program emphasizes all three pillars: people, process, and technology. • Stick to the three A's. Design the program so it is affordable. Meet them where they are by creating program eligibility criteria that are appropriately defined for the audience that will benefit from the courses. Make sure the participants have access to a structure that will facilitate their success. • Leverage the cooperative principles. • Advance the knowledge, skills and abilities of the participants and increase their exposure to threat information and cutting-edge cybersecurity practices and techniques. • Create solutions and program designs that can persist beyond the RC3 Program's period of performance. • Increase awareness of the need to define cybersecurity responsibilities clearly within the organization and with third parties. • Integrate peer-to-peer options.

Impact and Lessons Learned from the RC3 SANS Voucher Program

All participants in the SANS Voucher Program were asked to complete a Program Evaluation after their cohort had concluded. The same online evaluation tool was used for each cohort. Out of the 114 participants, 75 completed evaluation forms. The RC3 Team used the evaluation feedback to make improvements to the RC3 SANS Voucher Program between Cohorts, and to better understand the cybersecurity training needs of cooperatives. The RC3 Program also used responses on the evaluations to assess whether the RC3 SANS Voucher Program met its stated goals.

The first question on the evaluation form was: "Did any part of the SANS course you took trigger you to review your cooperative's cybersecurity practices, procedures, and/or policies? If so, which class were you taking and what sections in the class inspired you to review your

current practices, procedures, and/or policies?" Nearly all respondents who took SANS courses SEC 301 and/or SEC 401 indicated that the course(s) had caused them to review some aspect of the "practices, procedures, and/or policies" at their cooperatives (see Table 9).

Table 9: Reviews Triggered by Taking SANS Courses SEC 301 and SEC 401

	Cohort #1	**Cohort #2**	**Cohort #3**
# of Respondents Who Took SEC 301 or SEC 401	21	17	12
# of Respondents who Stated SEC 301 and/or SEC 401 Triggered Reviews	19	16	11
% of Respondents who Stated SEC 301 and/or SEC 401 Triggered Reviews	90%	94%	92%

Below are some representative samples of responses to Question 1 categorized as "yes":

- "It made me go over all of my policies, and I presented them to all of the employees at an all employee meeting and sign that they understood."
- "Yes, while taking SEC 401 there was discussion about managing access controls and reviewing that access from time to time. This prompted a review of our procedures for monitoring and maintaining user access based on job role."
- "Yes. SEC301, Principle of least privilege, authentication & authorization, among others. SEC401 end point security, firewall rule review and firewall, windows security, analysis of open ports, more password reviews. Review of the real business critical data and processes to help focus the plan. Too many improvements identified to answer."
- "Enhanced GPO policies talked about in 401.5. In 401.4 adjusted VPN settings to make them more secure. Enhanced Virtualization security from 401.1"
- "Honestly, just about every part of the course inspired me to look closer at security in my coop. It also had me realize that we have done some things well, we have a long way to go to fully be secure."
- "Yes, 401.1, 401.2, 401.5. These sections all provided an overview of information that led me to make changes to our IDR system and also prompted me to change some graphs in SolarWinds to watch for outgoing connections."
- "Yes, the SANS course did trigger me to review many of our cybersecurity practices, procedures, and policies. …the 401 Security Essentials class … inspired me to review our internet usage policy, disaster recovery policy, firewall rules, wireless encryption configuration, and asset inventory."
- "Yes, this course in its entirety triggered a review of our policies, procedures, and a review of what our contracted vendors were providing. … Specifically, the sections of security technologies, and hands on lab experiences triggered those questions."

The most commonly mentioned review areas were: password complexity; access control/least privilege; Microsoft Windows patching and security features; network awareness and security measures; encryption; and, logging and monitoring. There were also several general comments stating that all or many policies would be reviewed, but no additional specificity was provided. To learn more, the RC3 team broke down comments by specific policy areas mentioned (N=87 distinct comments) and cross referenced these comments to one of the five functions used in the RC3 Self-Assessment: Identify, Protect, Detect, Respond, and Recover. About half of the review areas fell under the Protect function, and about a quarter more were general comments that spanned many functions. Policies or practices aligned with Detect and Identify were mentioned about equally, with Respond/Recover measures mentioned the least often. Figure 13 shows a rough distribution of the results.

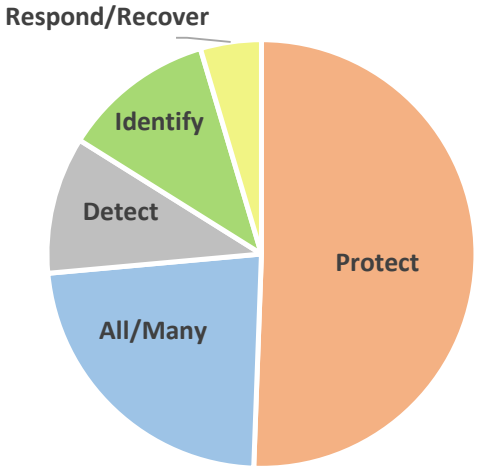

Figure 13: Areas Identified for Review Categorized by NIST Function Areas

Question 2 was designed to document actual changes that participants made as a result of participating in the Program. This question asked: "Did you make any changes to your cooperative's cybersecurity practices, procedures, and/or policies based on what you learned in the SANS class? If so, what did you change?"

Of the 75 total responses from all Cohorts:

- 45% (or 34 participants) indicated that at least one concrete change at their cooperative was "Complete", or fully enacted, as a result of something they learned during their time in the Program. Many described several completed changes.
- Fourteen (14) participants, or 19%, who hadn't fully completed a change stated that there were one or more changes "In Progress" at their cooperatives.
- Nineteen (19) participants, or 25% of the total, stated that they had changes "Planned", but none were "In Progress" or "Complete" at the time of the survey.
- 8 participants, or 11% of respondents, did not indicate that they had planned or initiated any changes at the time of the survey.

The most frequently mentioned individual measures, not including general policy updates across the organization, had to do with access control/least privilege, improving password complexity, creating or revising incident response plans, enhancing employee cybersecurity training, and increasing frequency of logging and monitoring. The RC3 team sorted individual measures by organizational element, i.e. People, Process or Technology. Technology and Process measures were referenced about equally. People measures, such as employee awareness programs, were the least often mentioned (seeFigure 14). Based on this analysis it appears that the RC3 SANS Voucher Program spurred wholistic changes across organizations rather than simply treating cybersecurity like an IT problem with an IT solution.

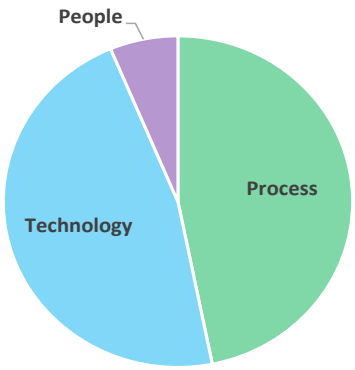

Figure 14: Changes Categorized by NIST Functions

The most common overall comment on the evaluations was to provide more time to complete the courses. The second most frequent comment as to provide positive feedback on the Program and/or courses taken. And the third most frequency comment was a request to continue the Program. For example:

- "If NRECA could do like an umbrella over us smaller cooperatives then maybe SANS would be willing to give discounts to classes cooperatives participated in. Maybe decrease the cost by half would be nice. I learned so much more from SANS then I did at the university course I took. Would love the opportunity to take additional classes in the next group offered if possible."
- "[B]eing able to take a course like this for free was amazing, but I'd love it if a discount could be negotiated by NRECA so they could be taken at will. I know my co-op would happily pay for someone to take a course every couple years, but full retail price plus a certification attempt is a tough sell"
- "I thought the program was great, the instructor was excellent, and I felt I had good support."
- "I don't see any need for it to be changed. The whole experience was excellent."

Some of the key lessons learned and recommendations at the end of the Program:

- Be more intentional in marketing to the target population to ensure all eligible candidates are aware of the Program;

- hold kick-off calls prior the start of the classes to set expectations;
  optimize the discussion groups so they are required and organized so people taking a similar class are grouped; and
- structure the discussion groups so someone in the cooperative community is responsible for organizing meetings rather than an RC3 Program staff so the discussions groups are more likely to continue after the RC3 Program staff no longer have time to continue to schedule meetings.

Appendix E: Cybersecurity-Collect-Communicate-Collaborate (C4) Technology R&D

Work on C4, developed by BlackByte, began in late 2017. Figure 15 provides a time series illustration of activities associated with the C4 R&D & deployment effort to illustrate the flow of events over the period of performance. Items in green represent programmatic activities. The relevant design principles and insights guiding this effort include:

- Design a deployment strategy with an understanding that all three pillars are needed: people, process, and technology.
- Leverage the cooperative principles and the cooperative infrastructure and, if possible, reinforce both.
- Create resources to advance the knowledge, skills, and abilities of the staff assisting with the deployment and responsible for using the technology.
- Create a technology and deployment strategy that can persist beyond the RC3 Program's period of performance.
- Integrate peer-to-peer options for sharing lessons learned when possible.

The C4 technology can process both static and live data. First, any network capture in the form of a PCAP can be ingested through the C4 collector and presented to the C4 analysis graphical user interface. This provides historical analysis of captures, or certain captures that have network considerations that need to be studied for anomaly or even confirmation of network operations from time to time. Second, is the dynamic processing of live network data. The C4 collector can be attached to any single network interface, or any number or combination of multiple network interfaces. This ensures, for instance, that if a utility engineer would like to have a live view of both their IT and OT networks without combining them, they are simply connected to the C4 platform separately in a passive manner as to not introduce any potential vulnerability into the utility overall network architecture.

The C4 tool has been tested in many different segments of the utility network. Testing the features and functions of the C4 tool was accomplished in both static and dynamic environments. The most valuable position for the utility today is to deploy within the OT network which is represented on the far right of the diagram. Determining what devices exist, their communications paths, and what protocols are used has proven to be an effective method for confirming existing engineering configurations as well as providing real-time situational awareness while deploying new devices in the field. By using the capability to listen on multiple networks, the C4 platform is able to monitor all traffic traversing different segments of the network. At a minimum this capability has been tested by monitoring both the OT network and the Business Network on the internal utility network fabric.

C4 Deployments and Lessons Learned

The first case study was a distribution utility with approximately 48,000 meters. There were a number of issues in the early month of operations. C4 collects a huge volume of data. While

much of this is redundant, reflecting normal operations, the systems retain as much as possible. The goal is to give an analyst all of the information they might want or need to analyze anomalies both in regular reports and reports generated from logs as the investigation proceeds. Until data retention was optimized the system halted operation when the volume of operation reached hardware limits. A manual restart was required. Methods were developed to allow continuous operation and C4 now operates reliably without intervention. The NRECA team tested the installation by writing special rules/filters defining normal operations of interest as potential anomalies. The systems were 100% successful in the application of rules/filters in numerous tests, and the capability has been demonstrated in real time to many organizations and individuals.

The second case study involves a deployment that was installed by the distribution utility in a virtual cluster and connected to their OT network to monitor substations and meter data from different feeds in their network.

The third case study is a distribution utility with 300+ downline devices and metering for extended data.

The fourth case study is a distribution utility that also has downline devices and metering for monitoring the downline devices and meters on the network.

The fifth case study is a G&T that does not serve its customers directly, but manages infrastructure including 100+ substations supporting it’s five member distribution cooperatives providing a very different architecture.

Regardless of the diversity in the utility electric systems and their network designs, C4 was able to achieve successful connectivity regardless of where the data resided in the utilities network, and to maintain persistent data processing during excessive network traffic from remote stations, and visualize network activity and protocol dynamics in real-time network contexts.

After installation the C4 technology was able to detect a number of issues at the partner utilities including: incorrectly configured ports or field devices; devices failing to report on normal frequency which was found to be caused by RF issues; a misconfigured VLAN allowing UDP connections on both VLANS; a new DNS server discovered that was giving outdated DNS lookups in the OT network and, a workstation in the OT network was duel-homed to an external file share with a persistent connection.

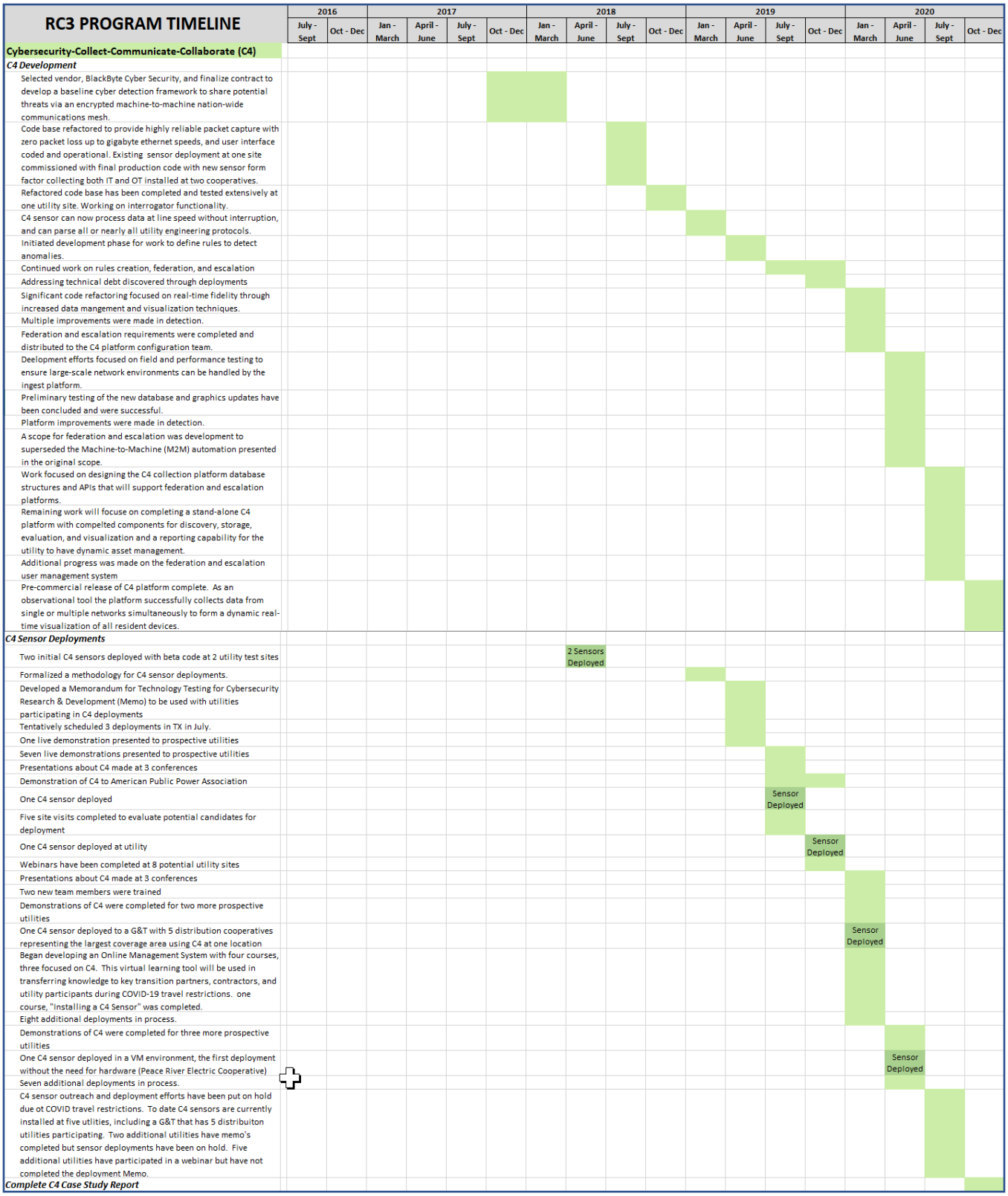

Figure 15: Timeline of C4 R&D and Deployment Planning and Activities

Appendix F: RC3 Outreach and Recruitment

The RC3 Program worked closely with NRECA's marketing and communications team to disseminate announcements of Program resources and opportunities. An analysis of the marketing materials demonstrated that the top 10 audiences engaged with the RC3 Program materials were:

- General Manager/CEO
- IT Manager
- Chief Financial Office
- Executive Assistant
- Directory of Regulatory Affairs
- Director of Member Services and Education
- Office Manager
- Chief Information Officer
- Attorney
- Information Security Program Manager

The second primary marketing method was announcements in NRECA's "Business and Technology Update" bi-weekly digital newsletter. Based on a similar analysis, the top 10 audiences engaged with the RC3 Program materials through this method were:

- General Manager/CEO
- Lineman
- Executive Assistant
- Engineering & Operations Staff
- Member Services Representative
- Line Superintendent
- Chief Operating Officer
- Office Manager

Below is a listing of the other products created by the RC3 Program and by other departments in NRECA that highlighted and celebrated the RC3 Progam.

The RC3 Program was highlighted every year for the past four years in NRECA's Annual Report:

- *2020 NRECA Annual Report*
- *2019 NRECA Annual Report: Safeguarding the Grid*
- *2018 NRECA Impact Report: Cybersecurity*
- *2017 NRECA Annual Report: Solving Business Challenges - Cybersecurity*

Twelve articles were published that highlighted the RC3 Program in *Rural Electric (RE) Magazine*, NRECA's flagship publication distributed to more than 20,000 subscribers.

1. *Co-op Tech: IT/OT Cyber: Increased use of smart devices elevates the need for operational security* (September 1, 2020)
2. *NRECA Designs Cybersecurity Guidebooks to Help Co-ops Define Roles, Risks* (December 2019)
3. *10 Key Technologies: Essential tools and devices for enabling the distributed energy grid* (November 30, 2019)
4. *Cyber TTX: A new RC3 tabletop exercise toolkit puts critical testing resources at co-ops' fingertips* (September 3, 2019)
5. *Supply Chain Cybersecurity: A new report advises co-ops on exposing and fixing procurement weak links* (September 18, 2018). Article highlighting supply chain issues that are key risks in cybersecurity.
6. *Outsourcing Cybersecurity: For some co-ops, thwarting hackers means leveraging third-party expertise* (June 25, 2018).
7. *Cyber Cooperation: Co-ops have a secret weapon in the war against network attacks* (July 20, 2017).
8. *HR's Role in Cybersecurity* (July 20, 2017)
9. *Taking Stock: A new tool to assess your co-op's cybersecurity posture* (July 20, 2017)
10. *Commentary: Electric Co-ops and Cybersecurity Partnerships: NRECA CEO Jim Matheson on Cybersecurity and Co-ops* (June 19, 2017)
11. *Ransomware: Electric Co-ops Fight the Latest Battle in an Increasingly Sophisticated Cyber War* (May 17, 2017) – Sidebar: *RC3: Help for Building a Cybersecurity Culture* (May 17, 2017)
12. *Ransomware: 'Your Personal Files are Encrypted'* (December 27, 2016)

Fifteen articles were published on cooperative.com, NRECA's primary website for member engagements, that highlighted the RC3 Program.

1. *NRECA Designs Cybersecurity Guidebooks to Help Co-ops Define Roles, Risks* (December 2, 2019)
2. *New NRECA Toolkit for Distribution Co-ops Geared to Close Cybersecurity Gaps* (May 31, 2019)
3. *Co-ops Can Now Apply for RUS Loans to Boost Their Cybersecurity* (May 29, 2019)
4. *Co-ops Can Gauge Vulnerabilities With New Cybersecurity Self-Assessment Tool* (February 5, 2019)
5. *RC3 Leverages 'Cooperation Among Co-ops' to Confront Cybersecurity Challenges* (October 2, 2018).
6. *How Would Your Co-op Handle a Cyberattack?* (September 19, 2018)
7. *GridEx Gives Co-ops Chance to Flex Cybersecurity Muscles: It's never too early to plan for an attack* (April 24, 2018)
8. *Why Even a Small Co-op Is a Big Target for Cyber Crooks* (April 5, 2018)
9. *Matheson: Co-ops Need More Cybersecurity R&D, Information-Sharing: NRECA CEO brings co-op message to Capitol Hill* (March 2018)

10. *Cybersecurity Responsibility Belongs to Every Co-op Employee* (March 2018)
11. *How the Federal Spending Bill Helps Electric Co-ops* (March 23, 2018)
12. *NRECA CEO to Promote Electric Co-op Cybersecurity Efforts in Senate Testimony* (February 2018)
13. *Building Cyber Resiliency Across America's Electric Cooperatives* (August 2017)
14. *Rural Cooperative Cybersecurity Capabilities Program (RC3): The facts about how NRECA is taking a lead role on cybersecurity* (May 2017)
15. *Perry Hails Co-ops for Energy Security: Energy Secretary recalls his co-op ties at annual NRECA Legislative Conference* (April 2017)

Thirteen NRECA *Technology Advisories* about the RC3 Program were published and posted online:

1. *Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – August 2020
2. *Update Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – April 2020
3. *Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – February 2020
4. *Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – October 2019
5. *Tabletop Exercises In Cybersecurity Help Cooperatives Prepare For "The Real Thing"* – February 2019
6. *Cooperatives Are Gaining Cybersecurity Skills with the RC3 SANS™ Voucher Program* – February 2019
7. *Opportunity to Receive FREE Cybersecurity Online Courses through NRECA's RC3 SANS™ Voucher Program: Cohort #2* – October 2018
8. *RC3 Self-Assessment Program – Lessons Learned: CEO Leadership is Critical to a Strong Culture of Cybersecurity* – September 2018
9. *RC3 Self-Assessment Program – Lessons Learned: Engaged Employees are a Cooperative's First Line of Defense Against Cyberattacks* – September 2018
10. *RC3 Self-Assessment Program: What the CEOs and GMs Have to Say About Cybersecurity* – May 2018
11. *Opportunity to Participate in NRECA's RC3 SANS Voucher Program for FREE Cybersecurity Online Courses* – March 2018
12. *NRECA Summits Are Catalyst for Co-op Discussions about Cybersecurity Risks* – February 2017
13. *RC3 Overview* – February 2017

Two Fact Sheets and six Frequently Asked Questions (FAQs) were published:

- FAQ: *Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – August 2020
- Update FAQ: *Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – April 2020
- Fact Sheet: *RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit* – April 2020

- FAQ: *RC3 Cybersecurity Tabletop Exercise (TTX) Toolkit* – April 2020
- FAQ: *Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – February 2020
- FAQ: *Opportunity Announcement: RC3 Online Cybersecurity Self-Assessment License Program* – October 2019
- FAQ: *NRECA's RC3 SANS Voucher Program Frequently Asked Questions (FAQ)* – May 2019
- Fact Sheet: *RC3 Cybersecurity Self-Assessment Do-It-Yourself Toolkit* – January 2019

Other RC3 Program publications included:

- *Cooperative Cybersecurity: Are you doing everything you can to keep your network safe?* (August 2017 v1, August 2018 v2) – A 12-page insert on cybersecurity originally published in the August 2017 issue of NRECA's *RE Magazine*. An additional 4,000 copies were printed for distribution at conferences and meetings. An updated and revised version was released in August 2018 for distribution at member conferences and meetings.
- *NRECA's Rural Cooperative Cybersecurity Program (RC3)* (December 2019 v2) – RC3 at a glance, a single page infographic highlighting some of the accomplishments and impacts of the RC3 Program in the past 3 years. The initial version, published August 2018 (v1), covered the first 2 years of the RC3 Program.
- *OPPORTUNITY ANNOUNCEMENTS:*
    - *Opportunity to Receive FREE Cybersecurity Online Courses through NRECA's RC3 SANS™ Voucher Program Cohort #3* (May 2019)
    - *Accepting Applications to Participate in NRECA's RC3 Self-Assessment Research Program* (February 2017) – a 12-page description of the RC3 Self-Assessment Research Program, information on how to apply to participate, and a copy of the application published on-line.

In 2019, NRECA's Cybersecurity Program Manager was highlighted as part of NRECA's *We Are NRECA* video series:

- *We Are NRECA: Cynthia Hsu on Cybersecurity* (September 2019) – a short video showcasing the RC3 Program's Principle Investigator, Cynthia Hsu at: https://www.youtube.com/watch?v=OuI9vCFV12s

The success of the RC3 Program team in engaging more than half of NRECA's members in the RC3 Online Self-Assessment Program was highlighted in NRECA's internal employee web-based newsletter, *NRECA Now!*.

- *BTS Celebrates Strong Co-op Response to New Cybersecurity Assessment* (June 23, 2020)