Technology Advisory

Opportunity to Participate in NRECA's RC3 SANS Voucher Program for FREE Cybersecurity Online Courses

APPLICATION DEADLINE: MARCH 31, 2018

Program Overview

NRECA's Rural Cooperative Cybersecurity Capabilities (RC3) Program is dedicated to promoting a culture of cybersecurity and resiliency within the electric cooperative community. In these times of increasing cybersecurity threats in all market segments, it is important for cooperatives to be knowledgeable about how to improve their cybersecurity posture. The RC3 SANS Voucher Program works to connect cooperatives with leading cybersecurity experts, and to facilitate peer-to-peer learning for the benefit of both individual co-ops and the cooperative network.

The RC3 Program has recently secured an opportunity for cooperatives to participate in a SANS Voucher Program. SANS is a world-renowned cybersecurity training, certification and research company (https://www.sans.org/). The RC3 SANS Voucher Program allows participating cooperatives to attend up to three online training classes provided by SANS, and to build a strong network with other cooperatives while completing the training. These courses typically cost $2,000 to $6,000 each. Through the RC3 SANS Voucher Program, co-ops have a unique opportunity to access this leading cybersecurity organization's training courses for free.

The RC3 program is funded by the Department of Energy National Energy Technology Laboratory under Award Number(s) DE-OE0000807.

How will Cooperatives Benefit from Participating?

Are you having trouble understanding the basics of cybersecurity? Do you want to know how to develop a cybersecurity training plan? Do you know the "right" cybersecurity questions you should be asking partner organizations? Do you need to know how to securely segment your network from cyberattacks? Do you want to take specialized cybersecurity classes related to Industrial Control Systems? **The RC3 SANS Voucher Program was designed to help cooperatives develop the skills to address these questions and more.**

U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

NRECA America's Electric Cooperatives

There are a variety of SANS online courses available, for cooperatives to tailor their learning to their specific needs. Courses are also available at a variety of technical levels to accommodate staff who are beginners as well as those more experienced in cybersecurity. The RC3 SANS Voucher Program has defined a 'Training Roadmap' to help participants select courses that will be most advantageous.

Any cooperative, regardless of its size or its staff's cybersecurity capabilities, can greatly benefit from these courses.

Application Process

This opportunity is limited in the number of SANS vouchers NRECA has available and the timeframe in which courses must be completed. Interested cooperatives need to submit an application to NRECA for consideration. **Details on how to apply and the benefits and responsibilities of participants may be found in the accompanying Program FAQ.**

Below is the timeline for the RC3 SANS Voucher Program:

IMPORTANT DATES	
Application process opened	March 5
Deadline for co-op applications to NRECA	March 31
Announcement of selected co-op participants	April 6
SANS Voucher Program starts	April 9
Final SANS courses must be initiated by participants	October 12

Additional Resources

- RC3 Program Overview
- RC3 Program Website
- NRECA Cybersecurity Website

Contacts for Questions

- Andre Joseph, Principal, Cybersecurity: Andre.Joseph@nreca.coop
- RC3 Team Email: CyberSecurityRC3@nreca.coop

U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

NRECA America's Electric Cooperatives

RC3 SANS VOUCHER PROGRAM FAQ

Program Overview

NRECA has secured an opportunity for member cooperatives to take SANS online cybersecurity courses for free. These courses typically cost between $2,000 and $6,000 each. The RC3 Program strives to assist cooperatives in improving their cybersecurity posture and fostering a culture of cybersecurity. Toward this goal, the RC3 SANS Voucher Program will facilitate access for cooperatives to take cybersecurity courses from this leading training organization.

This Program is designed for cooperatives to increase their cybersecurity resilience and knowledge base. Participants will also have an opportunity to consistently network with RC3 staff and other cooperatives to learn about the ever-changing cybersecurity threat landscape.

Who Can Apply?

The RC3 SANS Voucher Program is open to any NRECA voting member U.S. electric cooperative for use by employees of the cooperative. To ensure NRECA's RC3 Program assists as many member cooperatives as possible, those participating in other funded/subsidized training through NRECA's RC3 Program, such as the RC3 Self-Assessment Research Program, will only be considered if there is not sufficient interest in the vouchers expressed by other cooperatives.

How Many Courses Can Each Participating Cooperative Take?

Cooperatives selected to participate in the RC3 SANS Voucher Program will be able to take up to three (3) **online** (i.e. OnDemand, vLive, Simulcast, etc.) SANS courses.

What Type of Courses Are Available?

SANS has a diverse portfolio of courses that range from highly specialized cybersecurity classes for Industrial Control Systems (ICS), to foundational cybersecurity classes that teach the basics. NRECA has developed a "Training Roadmap" to assist participating co-ops in selecting courses that focus on different roles of co-op staff:

1. Implementer
2. Administrator

Details about the Training Roadmap and related courses are available in Appendix A.

What are the Categories for Participation?

There are two different categories for participation in the RC3 SANS Voucher Program:

- **Category A** for distribution cooperatives with limited information technology and cybersecurity staff, who are early in their cybersecurity program development, and interested in taking courses; and
- **Category B** for larger distribution cooperatives and G&T cooperatives who are more advanced in their cybersecurity program development and interested in taking courses.

Category A participants will participate in courses defined in a Training Roadmap (explained in Appendix A); Category B participants will be able to select courses from the SANS catalog that would best augment their existing cybersecurity knowledge.

Cooperatives may apply for consideration in both categories, but must submit two separate applications, one under each category.

What are the Participant Benefits and Responsibilities?

The goal of the RC3 SANS Voucher Program is to assist cooperatives with their individual cybersecurity knowledge and capabilities and, in the process, also benefit the broader cooperative network.

This is a valuable opportunity and one through which NRECA can only accommodate a limited number of interested cooperatives. Selected participants are expected to make good use of the available vouchers and to support peer-to-peer learning.

It is important that the RC3 SANS Voucher Program benefits the broader cooperative network, not just the individual cooperatives that participate. As such, it will be expected that participating cooperatives be active ambassadors of the RC3 SANS Voucher Program, and be willing to share the knowledge and skills they gain by participating in this Program with other cooperatives.

The following provides further details on the benefits and responsibilities for participants:

Benefits

- Access to the world-renowned SANS cybersecurity training organization
- Free cybersecurity courses
- Advancement of your co-op's cybersecurity knowledge
- Improvement to your cooperative's cybersecurity posture

- Gain a basis for developing your own cybersecurity training programs for your cooperative
- Opportunity to share experiences and insights with other co-op participants

Responsibilities

- Initiation of courses in a timely manner* (Note: Delays in using the vouchers will result in forfeit, so that another co-op may benefit from participation)
- Completion of courses within the allotted time of 12 weeks per course*
- Consistent staff participation in weekly conference calls with NRECA RC3 staff and other cooperatives taking the same course for peer-to-peer learning. These meetings will serve as opportunities to forge stronger relationships with other cooperatives in the group, and to enhance information sharing initiatives related to cybersecurity.
- Sharing of experience through:
    - Submitting a course evaluation after completing each course
    - Availability to be interviewed by NRECA RC3 team members for the gathering of insights and feedback
    - Interactions with other co-ops during your normal business activities
    - Voluntary presentations at conferences, webinars, or workshops as feasible to share skills and lessons learned with other co-ops (travel and hotel expenses to be covered by the participating cooperative)
- Listserv Participation: All Category A participants are expected to participate in listservs which will be dedicated to each course. This is an opportunity for peer-to-peer learning, allowing you to ask and answer questions about course material and help ensure your understanding and success in the course. For each listserv, a Category B participant will be assigned, who will be responsible for monitoring the listserv activity daily and using their more advanced cybersecurity knowledge to provide answers to Category A participants' questions.

*The Importance of Completing Selected Courses

NRECA's RC3 team will be monitoring the SANS training portal to ensure participants are able to complete the courses before their vouchers expire, and before the 12-week period per course expires. NRECA is not able to extend the SANS deadlines.

It is essential that cooperatives participating in this program are dedicated to completing the courses they choose. The opportunity for these vouchers is limited and it is expected that not all interested cooperatives will be able to be accommodated. If you are selected, please realize that there are likely others not afforded this same opportunity. Your timely initiation and completion of the courses, and your active

participation in peer-to-peer learning, is expected for your cooperative's benefit and the benefit of the membership as a whole. **Any cooperative not completing a course will automatically forfeit any remaining vouchers.**

Will I Need To Travel?

Travel is not required to participate in this Program or to complete one of the SANS courses. All of the courses available to participants through the RC3 SANS Voucher Program are the **online** SANS courses. The weekly meetings for peer-to-peer learning will be conducted by conference calls. In addition, the requirement for participants to share their gained knowledge with other cooperatives is expected to be fulfilled through the co-op's normal business activities.

How Much Time Will I Need to Commit to this Program?

Participants are under no obligation to take their courses at a specific time in the day, but each course within the Training Roadmap for Category A participants must be completed in a 12-week period from course initiation. Category B participants must complete each selected course within the timeframe defined by SANS at the time of course sign-up. As indicated in the Timeline of Important Dates, all final vouchers must be used to select courses by October 12, 2018.

The table below provides a breakdown of the estimated minimum number of hours a week staff will need to commit to this Program to successfully complete each course in the training roadmap, in a 12-week period. The hours per week in the table **include** time required for weekly group meetings with RC3 Staff and other Program participants.

Course	Training Roadmap Branch	Average Hours Per Week
SEC301	Implementer/Administrator	4 ½
SEC401	Implementer	5
SEC503	Implementer	5
MGT512	Administrator	4 ½
MGT514	Administrator	4 ½

With these estimates, a participant who worked a 40-hour, 5-day work week would need to dedicate up to 1 hour a day on average to participate in the Program.

Listservs for Groups

Category A participants will be grouped according to the courses they are taking and will be provided with a dedicated listserv per group that can be used to field questions they may have during the course. These will be private listservs, whereby only group participants will be able to see questions posted and participate in the discussions. Each Category B participant will be assigned to a listserv, to monitor and answer questions and to support the Category A participants' learning.

What Is the Application Process and Selection Criteria?

The application consists of three parts:

- **General Information Questions**

  The answers to these questions will provide information about the applicant and will not be used for scoring the application.

- **Technical Assessment Questions**

  Answers to the technical questions will be evaluated along with the essay to arrive at the final application score.

  As noted earlier, in order to support the greatest advancement for co-ops through the Voucher Program, selection preference for Category A will be to cooperatives that:

  - do not have dedicated cybersecurity staff;
  - have 3 or fewer staff in information technology; and
  - are in the early-stages of developing a cybersecurity program.

- **Essay**

  The application requires a potential participant to describe how the cooperative will share its experiences to benefit colleagues at other cooperatives. The description of what actions your cooperative will take to support the efforts of other cooperatives to improve their cybersecurity posture will be a critical component of the application. Essays will be anonymized prior to review by a team of panelists at NRECA. The cumulative essay score will be combined with the technical assessment score to arrive at the applicant's composite score.

As mentioned earlier, cooperatives who are already participating in other aspects of NRECA's RC3 Program through funded/subsidized training events or activities, like the RC3 Self-Assessment Research Program, will only be eligible for the RC3 SANS Voucher Program if there is not adequate interest expressed by other cooperatives.

How Many Cooperatives Will Be Able to Participate?

With the allotted vouchers from SANS, we anticipate being able to accommodate at most 30 cooperatives to participate in Category A and at most 10 cooperatives to participate in Category B.

What is the Timeframe for the Program?

IMPORTANT DATES	
Application process opened	March 5
Deadline for co-op applications to NRECA	March 31
Announcement of selected co-op participants	April 6
SANS Voucher Program starts	April 9
Final SANS courses must be initiated by participants	October 12

What are the Next Steps for Those Interested?

Cooperatives interested in participating should first determine which application category best applies, Category A or B. As noted earlier, an electric distribution cooperative may apply for consideration for both categories, but must submit two separate applications.

To be considered, applicants must submit their applications using an on-line application form. The on-line application may require a combination of management, legal counsel, and technical staff input to complete the questions. We recommend that you have all of the answers for the application prepared before you begin the on-line application process. You will not be able to save a partially completed application and return to the on-line system to complete the application at a later time. To help you prepare your responses before you begin the on-line application process, a complete list of the application questions is provided in Appendix B.

The deadline for applications is March 31, 2018.

Click here when you are ready to begin the on-line application process:

APPLICATION to PARTICIPATE in the RC3 SANS Voucher Program

Other Opportunities to Participate in RC3

Beyond this RC3 SANS Voucher Program, there are a variety of ways cooperatives may participate in NRECA's RC3 program, including:

- attending a RC3 Cybersecurity Summit
- participating in other training events
- becoming a Working Group member to help create new cybersecurity tools and resources

In addition to the RC3 SANS Voucher Program, the RC3 Program is in the process of developing new training courses, cybersecurity guidance books and educational resources, case studies, and technical articles that will be available to all members.

For more information:

- Visit our RC3 website
- Sign up for NRECA's TechUpdate newsletter
- Contact our RC3 Team at: CyberSecurityRC3@nreca.coop

Contacts for Questions

- Andre Joseph, Principal, Cybersecurity: Andre.Joseph@nreca.coop
- RC3 Team Email: CyberSecurityRC3@nreca.coop

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

APPENDIX A

Training Roadmap for Category A Participants

NRECA's RC3 Program team has developed a Training Roadmap to assist participants in developing the target skills that are a goal of the RC3 SANS Voucher Program. This Roadmap was developed to closely align with one offered by SANS, recognizing the benefit of taking certain courses sequentially. The RC3 Training Roadmap can also be used as a basis for the development of training programs that participants may want to develop for implementation within their own cooperatives.

Category A Participants are **required** to take at least two (2) courses in this Roadmap. After successfully completing participation in the Program with these 2 courses, Category A participants may choose any SANS course for their third voucher.

Category B Participants are not required to follow the Roadmap. It is expected that Category B participants are more advanced in their cybersecurity expertise, so they will be able to select other SANS courses that will help further improve their cybersecurity skills and training.

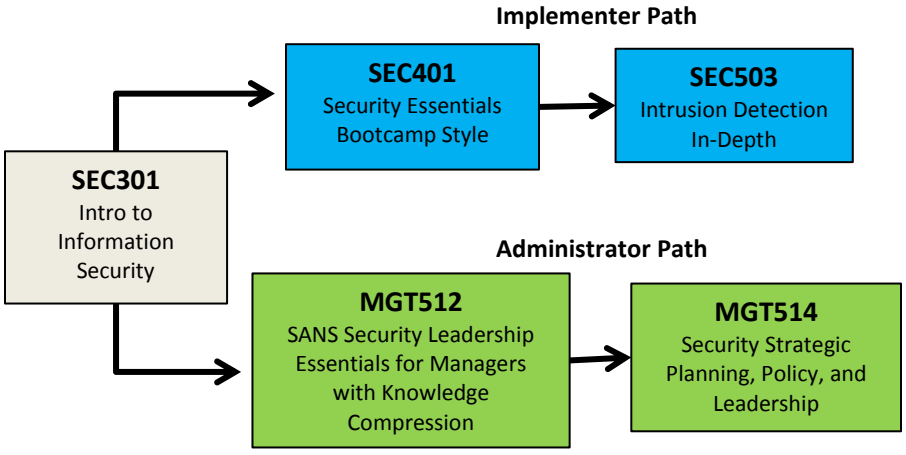
Training Roadmap Paths

The RC3 SANS Voucher Program Training Roadmap has five classes that separate into two paths:

1. **Implementer:** targeted towards participants who will be responsible for implementing information technology (IT) and operational technology (OT) security controls (e.g. segmenting a computer network, administering antivirus updates, implementing network intrusion detection, etc.).

2. **Administrator:** targeted towards participants who are responsible for overseeing individuals who implement IT and OT security controls.

The diagram below shows a flowchart for this Training Roadmap:



Beginning the Training Roadmap

The first class in the training roadmap for all Category A participants, SEC301, is geared towards participants who wish to understand the basics of cybersecurity, and is perfect for participants who:

- need an introduction to the fundamentals of security,
- feel bombarded with complex technical security terms they don't understand but want to understand,
- are non-IT security managers who deal with technical issues and understand them and who worry their company will be the next mega-breach headline story on the 6 o'clock news,
- are professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don't need "deep in the weeds" detail.

Implementer Path Courses

The first class in the **Implementer** path, SEC401, is for participants who:

- want to know what steps to take to securely segment a network with a combination of VLANs and firewall rules,
- want to learn about tools and techniques that can be used to verify their network is hardened against attacks,
- want to understand what cybersecurity questions they should ask partner organizations.

The second class in the **Implementer** path, SEC503, is for participants who:

- want to take a deep dive into intrusion detection,
- want to learn about tools and techniques that can be used to determine how good their IDS systems are.

Administrator Path Courses

The first class in the **Administrator** path, MGT512, is for participants who:

- need tools and strategies to understand the information IT security providers give to them,
- need to understand what cybersecurity questions they should ask partner organizations,
- need to communicate tactical and strategic decisions to a cooperative's board members, or others who are not "deep in the weeds."

The second class in the **Administrator** path, MGT514, is for participants who:

- need to ascertain the validity of IT security controls potential partners are pitching to them,
- would like to learn about tools and strategies that can be employed to validate cost and implementation time estimates for cybersecurity initiatives.

Full course descriptions may be found at: https://www.sans.org/courses/all/

Courses for Category B Participants

A comprehensive list of all SANS online courses can be viewed at https://www.sans.org/courses/all/.

APPENDIX B

RC3 SANS Voucher Program Application Questions

The following are the questions which are contained in the technical assessment and essay portions of the online application. **Applicants should review these questions prior to starting the online application, as you will not be able to save and return to a partially completed application.**

TECHNICAL ASSESSMENT PORTION OF ONLINE APPLICATION:

Cybersecurity Capabilities – People

1. How many of your employees provide Information Technology (IT) services to your staff?
    a. 0
    b. 1
    c. 2
    d. 3 or more
2. What is your role/job-title at your electric cooperative?
3. How many hours a week can you commit to this Program?
4. How many of your employees provide Cybersecurity services to your staff?
    a. 0
    b. 1
    c. 2
    d. 3 or more
5. Is there a staff member in a senior leadership position who is responsible for managing cybersecurity efforts at your cooperative?
    a. Yes/No
6. If yes, what is the current title of that staff member?
7. How often does your Board of Directors receive briefings on cybersecurity?
    a. Every meeting
    b. At least once a quarter
    c. At least once a year
    d. Other (please specify when the Board is briefed on cybersecurity)
8. How would you rank the cybersecurity skills and expertise of your staff? Where:
    a. None = staff have no training in cybersecurity practices
    b. Moderate = staff have a moderate level of cybersecurity training and skills
    c. Advanced = staff are highly trained and use advanced cybersecurity techniques

Cybersecurity Capabilities – Process

1. Does your cooperative have a dedicated cybersecurity budget?
    a. Yes
    b. No
    c. Other (If your cybersecurity funding is not in a dedicated cybersecurity budget but is included in another budget category, please specify how you fund your cybersecurity efforts.)
2. Does your cooperative assess cybersecurity risks associated with major capital investment projects?
    a. Yes
    b. No
3. Does your cooperative have a policy or procedure that: (Select all that apply)
    a. governs information access and security?
    b. governs network access for Mobile Devices?
    c. governs patch updates and patch management?
    d. prohibits password sharing?
    e. None of the above apply
4. How often is your cooperative's physical security policy or guideline reviewed and/or updated?
    a. At least once a year
    b. At least every two (2) years
    c. Every three (3) years or longer
    d. I don't know
    e. Other (Please describe your cooperative's review process for your physical security policy or guideline.)
5. Does your cooperative's physical security policy or guideline integrate cybersecurity risks?
    a. Yes/No
    b. I don't know
6. Is cybersecurity addressed in any of your emergency plans? (Select all that apply)
    a. Not included in any plan
    b. Disaster Recovery Plan
    c. Business Continuity Plan
    d. Emergency Response Plan
    e. Continuity of Operations Plan
    f. Other (please specify)

7. How would you rank the maturity of your current cybersecurity policies and procedures? Where

a. None = policies and procedures not developed
b. Moderate = policies and procedures exist and are occasionally reviewed or exercised
c. Advanced = policies and procedures to prevent, detect, respond and recover from a cyber incident are regularly reviewed and exercised, and regularly updated based on the results of reviews and exercises

Cybersecurity Capabilities – Technology

1. Has your cooperative ever conducted a cybersecurity assessment or hired a 3rd party vendor to conduct a cybersecurity assessment?
   a. Yes/No
2. If your cooperative has had cybersecurity assessments, what kinds of assessments have you had? (Select all that apply)
   a. We have not had a cybersecurity assessment
   b. Cybersecurity Self-Assessment (e.g. RC3 Self-Assessment, NRECA Risk Mitigation Guide, C2M2, NIST, CSET, etc.)
   c. Cybersecurity Audit
   d. Vulnerability Assessment
   e. Penetration Testing – External Perimeter
   f. Penetration Testing – Internal and External (business systems only)
   g. Penetration Testing – Internal and External (SCADA and ICS systems)
   h. Payment Card Industry (PCI) Security Assessment
   i. Other (please specify)
3. If your cooperative has had cybersecurity assessments, how often have cybersecurity assessments been conducted?
   a. We have not had a cybersecurity assessment
   b. At least once a year
   c. At least every two (2) years
   d. Every three (3) years or longer
   e. Other (please specify)
4. How often do you inventory your IT (hardware and software) and network assets?
   a. We have not had an inventory of our IT and network assets
   b. At least once a year
   c. At least every two (2) years
   d. Every three (3) years or longer
   e. I don't know
   f. Other (please specify)
5. How do you monitor the traffic and systems on your network? (Select all that apply)
   a. Cooperative staff monitor the network using specialized tools

   b. We use a service provider to monitor our network
   c. We monitor our internal and external network demilitarized zone (DMS) using different cybersecurity techniques
   d. I don't know
   e. Other (please specify)

6. Is your internal network segmented with firewall rules?
   a. Yes
   b. No
   c. I don't know

7. If your cooperative allows employees and/or Board Members to have remote access, does your cooperative use a virtual private network (VPN) and/or two-factor authentication?
   a. Yes
   b. No
   c. I don't know
   d. Our cooperative does not allow remote access

8. Do any of your vendors, suppliers, and/or contractors have remote network access to your business systems?
   a. Yes
   b. No
   c. I don't know

9. Do any of your vendors, suppliers, and/or contractors have remote network access to your meter systems, SCADA systems, or other operational systems or devices?
   a. Yes
   b. No
   c. I don't know

10. How would you rank the cybersecurity technology capabilities of your cooperative? Where:
   a. None = no cybersecurity technology or tools used
   b. Moderate = cybersecurity technology and tools are used and integrated into some of the cooperative's operations
   c. Advanced = advanced cybersecurity technologies and tools are integrated into all levels of the cooperative's operations

ESSAY PORTION OF ONLINE APPLICATION:

Cooperation Among Cooperatives

1. Please describe your cooperative's current cybersecurity efforts and the cybersecurity goals for your cooperative. Please limit your response to 1,000 words.
2. Please describe how your cooperative would benefit from participating in the RC3 SANS Voucher Program. Please limit your response to 1,000 words.
3. Please describe how your cooperative would share any success or benefits gained from participating in the RC3 SANS Voucher Program with the larger cooperative community. Please limit your response to 1,000 words.

Contacts for Questions

If you have any questions about the application, please contact:

- Andre Joseph, Principal, Cybersecurity: Andre.Joseph@nreca.coop
- RC3 Team Email: CyberSecurityRC3@nreca.coop