Fact Sheet

January 2019

NRECA
America's Electric Cooperatives

RC3 Cybersecurity Self-Assessment Do-It-Yourself Toolkit

Key Findings

- Cybersecurity threats are an unfortunate reality for all business sectors, including utility companies. It is important for cooperatives to understand their cybersecurity posture and continually work toward improvements.
- NRECA now offers a Cybersecurity Self-Assessment DIY **Toolkit** to help member co-ops identify cyber threats and vulnerabilities. NRECA's Rural Cooperative Cybersecurity Capabilities Program (RC3) staff designed the Toolkit to provide a starting point for small- and medium-sized co-ops in the early stages of developing a cybersecurity program. Completing a Self-Assessment can help your cooperative gain valuable insights to use in developing an action plan.
- The Toolkit has an overview of the Self-Assessment process, a template, and a scoring worksheet. The RC3 team expects to update the Toolkit and launch it on an on-line platform later this year.

What is the RC3 Cybersecurity Self-Assessment Do-It-Yourself Toolkit?

The RC3 Cybersecurity Self-Assessment DIY Toolkit (Toolkit) is a set of documents that your cooperative can use to evaluate your current cybersecurity capabilities, and to help you prioritize investments to improve your cybersecurity posture. The Toolkit includes 123 questions that cover cybersecurity controls that can be implemented at your cooperative. For example, some of the questions can help you discover vulnerabilities in your cooperative and understand mitigation options to address those vulnerabilities, some questions focus on ways to improve security controls when working with vendors, and others address ways to train staff. In addition, the Toolkit contains background information to understand the questions, and a way to calculate and summarize your results.

RC3

What is the purpose of the RC3 Cybersecurity Self-Assessment Toolkit?

The goal of the Toolkit is to help your cooperative assess your current cybersecurity controls, identify areas for improvement, and use those insights to develop and implement a cybersecurity action plan. It is specifically designed for cooperatives with few, or no, information technology (IT) staff. The target audience for the Self-Assessment Toolkit is your cooperative's leadership team. The majority of questions in the Self-Assessment cannot be answered by IT staff alone.

What is included in the RC3 Cybersecurity Self-Assessment Toolkit?

There are three documents currently available in the Toolkit:

1. *2018 Reducing Risk in Cybersecurity: An RC3 Guide for Electric Cooperatives* - Version 1.0. 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.
2. *2018 RC3 Cybersecurity Self-Assessment Template* - Version 1.0. The *Template* is also a Microsoft Word document. It is an interactive document that contains all of the Self-Assessment questions and drop-down boxes to answer each question.
3. *2018 RC3 Cybersecurity Self-Assessment Scoring Worksheet* - Version 1.0. 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 can help you understand your results.

A fourth document, a *Train the Trainer Manual*, is scheduled to be released in mid-2019. The *Trainer Manual* will provide guidance on how to facilitate the Self-Assessment process.

Who can access and use the RC3 Self-Assessment Toolkit?

All NRECA members.

How much does the RC3 Self-Assessment Toolkit cost?

The RC3 Cybersecurity Self-Assessment Toolkit is **FREE** for NRECA members.

How do I get a copy of the RC3 Cybersecurity Self-Assessment Toolkit?

You can download the Toolkit from cooperative.com at: https://www.cooperative.com/programs-services/bts/Pages/Assessing-Your-Cybersecurity-Posture.aspx

Who should complete an RC3 Cybersecurity Self-Assessment?

NRECA recommends you involve your entire leadership team in a discussion to address each question and decide what is the most appropriate answer for your cooperative. Many of the questions cannot be answered accurately without some discussion among your leadership team members. In addition, your leadership team will decide how your cooperative wants to use the Self-Assessment Tool. For example, in cases where a question pertains to a security practice that your co-op can fully implement relatively quickly, your leadership team may decide to answer a question as 'no' or 'partially complete' to demonstrate progress over time, or your leadership team may decide to answer the question 'yes' to demonstrate a stronger initial assessment. These are strategic decisions based on how your cooperative wants to use the Self-Assessment Tool.

How long does it take to complete an RC3 Cybersecurity Self-Assessment?

This depends on what your co-op wants to accomplish. The NRECA RC3 Team recommends that your leadership team take at least 8-10 full hours to complete the Self-Assessment questions.

Your cooperative can use the Self-Assessment questions to increase your leadership team's awareness of who is responsible for what cybersecurity controls across your cooperative, and to build a stronger cybersecurity culture within your cooperative. If possible, schedule the process to occur over 2 days, which will give everyone on your team at least one night to absorb the first day's discussion. On the second day, review your progress and have time to discuss any new observations among your team members, and then complete the Self-Assessment.

It has been the NRECA RC3 Team's experience that trying to complete the process in one full day can be overwhelming for staff members who are new to cybersecurity issues. If you rush the process, you may be less likely to uncover how the different members of your leadership team have work flows and responsibilities that directly affect your cooperative's cybersecurity.

What if our cooperative has few or no information technology (IT) staff and we outsource our IT functions? Will we be able to complete the RC3 Cybersecurity Self-Assessment?

The Self-Assessment was specifically developed for cooperatives with few or no IT staff. Your leadership team will be able to answer most of the questions, even if no one on the team has expertise in IT or cybersecurity. Questions in the Self-Assessment are organized into 5 sections: Identify, Protect, Detect, Respond, and Recover. Most of the questions in the Identify, Respond, and Recover sections will not require input from someone with IT experience. Questions in the Protect and Detect sections will require input from your third-party provider and/or partner who is responsible for helping your cooperative manage your IT services.

You may want to divide up the time your team takes to complete the Self-Assessment and invite your third-party provider/partner to participate in helping your cooperative answer the questions in the Protect and Detect sections. You can work with your third-party provider/partner remotely, by phone, or in-person depending on what arrangement would work best for your cooperative. In some cases, you will need to contact more than one of your third-party providers/partners to answer all of the Self-Assessment questions.

What's the difference between the 2018 RC3 Cybersecurity Self-Assessment and NRECA's 2014 Risk Mitigation Guide (RMG)?

The goal of the 2018 RC3 Cybersecurity Self-Assessment is to meet the unique needs of small- to mid-sized cooperatives that are just starting, or are in the early stages of developing a cybersecurity program. The 2014 Risk Mitigation Guide was developed to provide cooperatives with guidance to improve their general security posture, as well as specific guidance to implement cybersecurity controls to meet the unique security challenges introduced by smart grid technologies and devices.

The 2018 Self-Assessment and the 2014 RMG are not mutually exclusive. **Both can be used to help you improve your cooperative's cybersecurity capabilities**. If your cooperative is just starting a cybersecurity program, then NRECA recommends that you start with the 2018 RC3 Self-Assessment. If your cooperative is further down the path of implementing a cybersecurity program, then you may find it more productive to complete the 2014 Risk Mitigation Guide.

Who should I contact if I have questions?

If you have any questions about either the 2018 RC3 Cybersecurity Self-Assessment or the 2014 Risk Mitigation Guide, please contact NRECA's RC3 Team at CybersecurityRC3@nreca.coop. If you are interested in learning more about the RC3 Program, please see the RC3 webpage on cooperative.com at: https://www.cooperative.com/programs-services/bts/rc3/Pages/default.aspx.

How do I stay informed of updates to the RC3 Cybersecurity Self-Assessment Toolkit and other cybersecurity resources available from NRECA?

We encourage you and your colleagues and staff to sign-up for our twice-monthly newsletter, *Business and Technology Update*. A simple sign-up form is available at: https://www.cooperative.com/programs-services/bts/Pages/Technology-Update.aspx. Also, visit www.cooperative.com to find more resources about cybersecurity and a wide variety of other topics affecting cooperatives today.