USAID
FROM THE AMERICAN PEOPLE

BLACK SEA CYBERSECURITY STRATEGY DEVELOPMENT GUIDE

December 2017
This publication was produced for review by the United States Agency for International Development (USAID). It was prepared by the National Association of Regulatory Utility Commissioners (NARUC).

BLACK SEA CYBERSECURITY STRATEGY DEVELOPMENT GUIDE

Project Title:	Energy Sector Cybersecurity
Sponsoring USAID Office:	USAID/ Europe and Eurasia Bureau
Cooperative Agreement #:	USAID CA # AID-OAA-A-16-00049
Date of Publication:	December 2017
Authors:	Miles Keogh, Paul Stack, Ben Morano (NARUC)

National Association of Regulatory Utility Commissioners

This publication is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of the National Association of Regulatory Utility Commissioners (NARUC) and do not necessarily reflect the views of USAID or the United States Government.

Table of Contents

Background and Acknowledgments

With the support of the United States Agency of International Development (USAID), the National Association of Regulatory Utility Commissioners (NARUC) has developed this document, the *Black Sea Cybersecurity Strategy Development Guide*, in order to provide information and lessons learned that will support Black Sea regulators in developing their own commissions' cybersecurity strategies. Drawing from experiences and best practices from U.S. state-level regulatory commissions and elsewhere, the document has been designed to cover the important issues and questions that regulators should address as they begin the process of developing their unique cybersecurity strategies.

The document's contents have been informed by the NARUC Research Lab's work with US state regulators on cybersecurity, as well as two USAID-supported workshops conducted with Black Sea regulators, which took place in Kyiv, Ukraine from November 30-December, 2016 and Tallinn, Estonia from March 30-31, 2017, respectively.

Introduction

Cybersecurity is in many ways a journey, with unknowns, challenges, and many different paths that one can take. Just as a map is foundational to any journey, developing a strategy is foundational for any commission that wants to take cybersecurity seriously. Whether in the US or the European Union, most regulatory commissions have begun their work on cybersecurity with the creation of a strategy.

In light of the above, this *Black Sea Cybersecurity Strategy Development Guide* sets clear steps for regulators to follow as they develop their own cybersecurity strategies. The Guide includes key questions that regulators must address in structuring their strategies and lists examples detailing how regulators at US commissions have approached each of the given questions**.** Just as one would be lost on any journey without a map, commissions initiating their work on cybersecurity without a strategy in place will not be as effective.

It must be stressed that this Guide is not meant to tell regulators what to do or what their strategies should look like. Each commission faces different realities and has different priorities and resources at their disposal. As such, each commission will have different responses and develop different strategies according to their needs and priorities. While the end results will vary, taking the time to think about the issues and questions outlined in this Guide is by far the most important step. At the end of this process, each commission will have the basic structure and answers in place to develop their unique cybersecurity strategy.

While this process may seem daunting, it does not need to be. By following the steps and answering the questions outlined in this Guide, a commission should have the basic structure and direction to create a simple and effective strategy that can grow and develop as the commission and utilities move toward greater collaboration and effectiveness in improving the cybersecurity of the power sector.

1. The First Step – Defining Mission and Goals

At its core, any cybersecurity strategy contains an articulation of why a commission values cybersecurity, what the commission's goals are, and how those goals will be addressed. Prior to developing a cybersecurity strategy, each commission should first articulate their values and goals – that is, why cybersecurity is important to them and what they want to achieve in addressing it.

This first step sets the tone for the entire process of drafting the strategy and sends a message to utilities that cybersecurity is important. By setting regulatory expectations, a commission can articulate to utilities that prudently incurred expenses are acceptable and, by sending that message, motivate them to take cybersecurity seriously. This process does not need to be complicated. Many US commissions have started with a few sentences or paragraphs in the form of a policy statement.

At the end of this first step, however, a commission should be able to clearly articulate their goals, how they will address cybersecurity, what the commission's role will be, and their level of engagement with utilities and other stakeholders. This policy statement, regardless of length, will provide a sense of purpose, identity, and long-term direction to the commission and will serve to communicate internally and externally what exactly the commission values with respect to cybersecurity.

1.1 Mission Statement

A **mission statement** allows a commission to define "who they are" in the realm of cybersecurity. A mission statement should highlight a commission's priorities and the issues they consider important, and it should also determine what the commission's threshold of progress for cybersecurity will be. While mission statements can vary significantly, each one should clearly and succinctly explain what is important to the commission in language that is clear to both commission staff and external stakeholders. This is extremely important, as it will set expectations both internally within the commission and externally with stakeholders. If utilities or other stakeholders are not able to determine the commission's priorities, it will be difficult for them to act accordingly.

The mission statement should also identify the strategy's **goals**. These goals or objectives provide a picture of where the commission wants to go. The goals of any commission should be realistic and attainable, combining what the commission values with the realities they face. A goal of being "100% fully cyber secure," for example, would be unrealistic for any commission. While some might think such a goal would show how seriously a commission is taking the issue of cybersecurity, the goal would in fact be counterproductive as both the commission and utilities would be unable to actually achieve it.

Instead, a commission might choose to define their goals as having the capability to improve cyber investments by utilities, having good communication with companies, and developing more transparent and useful reporting. These goals make it clear what the commission is attempting to do, and they are also achievable.

Washington Utilities and Transportation Commission (UTC) Case Study

As an example, regulators at the Washington UTC developed the following mission statement:

Our Mission is to protect the people of our state by ensuring that investor-owned utility and transportation services are safe, available, reliable and fairly priced. To assure our mission when considering cybersecurity, the objectives of this strategy are to facilitate risk based decision-making that weighs trade-offs and supports action that:

- *Prevents cyber-attacks against critical infrastructures;*
- *Reduces vulnerability to cyber attacks; and*
- *Minimizes damage and recovery time from cyber-attacks that do occur.*

To an outside observer, this mission statement may seem general, but to a utility, government agency, or the Commission as a whole, the language and message are quite clear. The words "safe, available, reliable, and fairly priced" stress that the Commission's objectives with regard to cybersecurity align with the overall mission of the UTC to provide safe, reliable, and affordable utility services to consumers. In other words, cybersecurity will not affect the core mission of the Commission. Furthermore, the language underscores the Commission will use a similar approach in balancing interests using risk-based decision making.

As discussed at the second USAID-NARUC workshop in Tallinn, Estonia, utility regulators are not cyber or security experts. Instead, they are "before" and "after" people, whether that is for the construction of new generation or emergency preparedness. The Washington UTC's mission statement underscores this point by focusing on the before and after components of cybersecurity, noting that the Commission will work with utilities to reduce vulnerability and "prevent cyber-attacks against critical infrastructures" (the before part) and to minimize damage and recovery time after cyberattacks have already taken place (the after part).

The language of "facilitation" and "support" also stress another key point about the Commission's approach to cybersecurity. The language implies that the primary group tasked with cybersecurity will not be regulators, but utilities. The UTC will not be micro-managing and working on the finer details of constructing a cybersecurity defense, but playing a facilitative and oversight role. A useful analogy was made by speakers at the Tallinn workshop – regulators are not castle-builders, but they need to be able to analyze and know what constitutes a strong, well-built castle. As such, a commission does not have to have the engineering and carpentry skills to build a proverbial castle, but they should be able to guide and oversee the process.

The last three bullet points are also important in that they are goals that are *achievable*. By casting the goals as reducing vulnerability and minimizing damage, the Washington UTC is recognizing that cyberattacks cannot be entirely eliminated. Indeed, there can be no 100% cyber secure system, and the Commission will not expect this from their utilities. Instead, the UTC will focus on accepting the fact that there is no perfect cybersecurity and work to mitigate and manage the associated risks.

2. Developing a Cybersecurity Strategy – Questions to Ask

Once a commission knows who they are (mission statement) and where they want to go (goals), they are then able to develop a cybersecurity strategy to determine how they plan to achieve those goals, the level of engagement they will have with utilities, and what their role will be. This can, and in many cases does, begin at a very small scale before developing over time. The Connecticut and Washington Commissions have two of the most sophisticated cybersecurity strategies of any US regulators, but they both began

from a much more simple starting point. When the Washington UTC began to focus on cybersecurity, they started with a two-page memo stating that cybersecurity is an issue that they will prioritize. From that memo, the UTC formed a working group, which in turn collaborated with other stakeholders to produce a more sophisticated cybersecurity strategy outlining the Commission's priorities, scope, and manner of engagement. By starting simple, the Commission indicated that cybersecurity would be a priority for them, and this helped set expectations, both within the Commission and externally, and build momentum to bring them to where they are today.

The following section was developed in order to provide a starting point for regulators. These questions do not have one correct answer, but should be used to see what each commission wants to get out of this process as they develop their strategies.

As Arthur House, former Chairman of the Connecticut regulator PURA, noted in his presentation to Black Sea regulators in Kyiv, Ukraine in December 2016, it is absolutely essential for regulators to at least take the first step. That first step will establish the goals and path forward for each commission and will serve as a basis to initiate a conversation with utilities that will lead to improved cybersecurity of the energy sector.

2.1 Scope of Strategy

What scope do you want your strategy to cover? What sectors should it cover and what level of focus should it have?

The question of scope refers to the **breadth** and **depth** of a commission's focus and attention to cybersecurity. This question is fundamental to the development of a cybersecurity strategy. Each commission will have to match their scope to the realities they face – e.g., resources, priorities, relationships with utilities – in order to determine what scope makes the most sense for them. From there, the scope can be expanded as realities or circumstances change. As mentioned in the introduction, successful strategies have been developed with different responses to the above question, so there is no "one size fits all" template.

As for breadth, a scope should cover which sectors the regulator would like to address. For example, Connecticut initially decided to cover its electric distribution companies, natural gas, water, and telecommunications.

Conversely, depth refers to the degree and regularity of engagement a commission expects to have with their utilities. For some Black Sea countries, where there are relatively few distribution and transmission companies, the question of scope may be relatively straightforward, whereas for Ukraine, with over 40 distribution companies or "oblenergos," NEURC may want to consider some of the approaches of larger US states.

While there are myriad US state examples, the Washington UTC and the Kentucky Public Service Commission (PSC) serve as helpful contrasts to approaches Black Sea regulators can take:

- The Washington UTC determined that they would be best to begin with a very narrow and shallow scope in order to get the process started rather than waiting. In other words, they wanted to simplify the process and operate successfully with limited resources. The Commission started

with 12 questions, and they decided that they would only ask these questions to their investor-owned utilities. Over time, the strategy was built to be more comprehensive and involve additional stakeholders. The Washington UTC said they learned that beginning with a narrow scope requires less time and resources, and can help to make progress and build momentum in order to further develop the Commission's cybersecurity capabilities.

- The Kentucky PSC started with a much wider and deeper scope, including all of its companies in the process. While this approach can be more comprehensive, it requires much more time and resources, as well as cooperative companies, in order to take this approach and be effective.

A helpful starting point for determining a commission's scope is the NARUC Research Lab's Cybersecurity 2017 Primer, which provides an introductory explanation of key issues and includes over 100 questions to ask utilities. While not every question may be relevant to commissions, picking out a set of questions that a commission wants to ask their utilities can be an easy and effective place to begin.

2.2 Commission Preparation

How should a commission prepare?

At its core, effectively managing cybersecurity is about **process** and **mediation** for commissions. While technical knowledge is important, the approach and focus should be cross-cutting and involve many departments within a commission. One of the biggest mistakes a commission can make is sequestering cybersecurity as strictly a technical problem.

Instead, commissions should develop a working group with people who can bridge interest groups and who know how to manage processes and competing interests. Identifying a champion within leadership who can help to drive the process, as well as a few staff in different areas of a commission, has proven effective for many US commissions. While this is an effective approach, the specific organization and structure of working groups have varied widely, and commissions should choose a structure that best fits their priorities and organizational makeup. US commissions have found that groups with both technical and policy expertise, as well as one Commissioner to drive the process, have been very successful.

In light of the above, the strategy should clearly articulate: 1) which staff at the commission will work on cybersecurity – this also means determining whether there should be a specific cybersecurity position or if staff should work on cybersecurity in addition to other responsibilities; and 2) how the commission initially plans to approach cybersecurity.

2.3 Cybersecurity Staff and Policies

Who will be responsible internally? What policies are needed internally?

In order for cybersecurity to be taken seriously, it needs to be **staffed** and **funded** at a commission. While the levels of staff participation and funding may vary widely by commission, those two elements are crucial in order for it to be successful. In the US, for example, the Texas, New York, and Ohio commissions all have dedicated staff assigned to working on cybersecurity, whereas the Washington UTC

hired two additional staff, one with a background in policy and the other in regulatory services, to work on cybersecurity. In 2017, the Illinois Commerce Commission (ICC) decided to create a Cybersecurity Director position, a more senior level position. Instead of hiring new staff, regulators can also choose to build the capacity of existing staff members to work on cybersecurity on top of their current responsibilities. This role may not even be a full position - it may only be a portion of the time that existing staff spend on it, but that time needs to be identified and assigned.

Commissions should also be realistic in assessing their relationships with utilities and how able they are to get information from them. Information exchange and information management is key to success. The most successful US commissions have found that regulators and utilities must engage differently when it comes to cybersecurity than they might on other issues.

This not only covers how regulators engage with utilities, but also who is leading that engagement. Are the people that currently interact with utilities regarding other issues going to be the right people for cybersecurity? Communication and sharing of information are key, and commissions should ensure that they select people who are able to build relationships and work effectively with their counterparts at utilities.

Cybersecurity has technical aspects that can make for an easy conversation among computer experts. However, in the domain of utility regulation, economic and regulatory specialists must also be able to understand the language of cybersecurity and corresponding issues in order to evaluate utilities. Commissions should ensure that those individuals at the utilities and among the regulators who are covering the technical and economic issues are talking to and understanding each other. While each side has competing interests, goals, and concerns, developing some level of communication and understanding between the two sides will allow for more comprehensive and effective planning.

In order to assure that the right personnel are involved and the mechanisms they use for communicating a cybersecurity strategy might outline:

- How many and which staff from the commission will engage in cybersecurity work on behalf of the commission.
  As mentioned above, US states have found value in cybersecurity working groups that have an inter-departmental makeup. Given that trust and collaboration are paramount on the subject of cybersecurity, it is important to assign the right staff or Commissioners to interact with their utility counterparts on sensitive issues, which is likely not going to be the same staff who engage with utilities in contexts that can be more adversarial and confrontational.
- The level of funding a commission will set aside for the purposes of addressing cybersecurity
- The policies for internal and external communication that commissions may have to change or adopt to effectuate their cybersecurity strategy and engage with utilities For example, a commission may have to consider if they need new policies to handle sensitive information they receive on cybersecurity. The strategy should thus consider if a commission needs to revisit and/or develop additional procedures or processes and how they will do so.

2.4 Performance Requirements and Reporting

What performance requirements do you want from the companies you regulate?

Commissions should determine what they expect from their utilities in terms of cybersecurity investment, so that those expectations can be incorporated into future planning and operations. In order to do this, commissions should determine what outcomes or events they absolutely want to guard against, such as data breaches and operational disruptions. By determining what is acceptable and what is not, all stakeholders can plan accordingly.

It is also important for commissions to determine how they will interact with their utilities. How will utilities brief regulators and what kind of communication will work best? Who will be part of reviews and how will incidents be reported? These processes should be developed during the planning process with input from utilities. This will ensure buy-in and lead to a more efficient process.

US State Examples

Action Plan - Connecticut regulators worked with utilities and decided to move forward with creating an action plan, which utilities would present to regulators on an annual basis.

Briefings – Michigan, Iowa, and Indiana – these states use informal briefings at the company. These briefings are scheduled on a regular basis (at least annually).

Audits – Pennsylvania.

Note: It should be noted that regulators should be careful with cybersecurity audits because audits are on some levels adversarial by nature and may not be in line with the trust and confidence-building that collaborative work on cybersecurity requires.

Breach Reporting Requirements – New Jersey sets breach reporting requirements for its utilities in order to set expectations for how they will interact and what information must be communicated.

Risk Management Program – the Kentucky PSC opted in favor of a risk management program, which was a full multi-stakeholder collaborative process that led to a structure for risk-based security action, including a mechanism for ongoing communication about issues, threats, and best practices.

Reporting - What reporting do you want, before, during, after events?

US commissions have consistently found informal communications and reporting practices to be the most effective approach, as they allow for a more open and frank discussion and more useful information sharing. The reporting process also needs to be risk-compatible. Formal audit reporting, for example, does not properly capture all of the elements involved. Instead, scheduling semi-regular in-person reviews allows for a more free-flowing discussion and sharing of information.

During a cybersecurity event, communication should focus on the estimated time to restoration from attacks. Determining a containment date for each data breach not only helps to manage expectations for stakeholders, but it also sets a baseline from which lessons can be learned and performance can be evaluated afterwards.

After an event, a process should be developed for utilities to complete an "after-action" report with remedial steps and lessons learned. This report should provide both the commission and their utilities with useful information regarding how the event happened, what steps or actions could have been taken to prevent it from taking place, and what steps the utility and commission will take next.

Connecticut Case Study:

Connecticut regulators agreed that confidentiality was of high importance to them, and so, in collaboration with utilities, they decided to conduct annual meetings to review cybersecurity defense with no records and no notes allowed. In fact, PURA required all attendees at the annual meeting to enter into non-disclosure agreements. At his presentation at the Tallinn workshop, Art House noted that Connecticut PURA's strategy details how their reporting and communications should take place, which he broadly summarized in the bullet points below:

- All reporting takes place at an annual meeting;
- An outline of each utility's presentation, key points, and charts is shared with regulators before the meeting;
- Given that no notes and records are kept (in addition to the non-disclosure agreements), regulators and utilities agreed that there would be significant disclosure during the meeting;
- Regulators and utilities will come to an agreement on a summary report of the annual meeting afterwards. The summary report will not cite results or sensitive information for any individual utility;
- The summary report will then be submitted as a final report to the Governor, legislature, and public outlining the high-level results of the annual meeting.

For more detail, PURA's strategy provides an overview of the discussions on reporting that took place after regulators' first-ever meeting with electric and gas utilities on cybersecurity in 2015:

> Regarding cybersecurity reporting standards, [certain utilities] prefer to use the ES-C2M2. They said they are already following the ES-C2M2 for their respective cybersecurity programs and believe it would be more meaningful and easier to use than state reporting requirements. They also suggested that the ES-C2M2 concept of MILs [Maturity Level Indicators] might be useful for reporting to satisfy the PURA reporting requirements. However, they cautioned that numerical indicators may be misinterpreted by uninformed audiences. They also suggested using "heat maps" of their cybersecurity posture as an annual reporting mechanism to convey a general sense of the areas requiring the most attention.
>
> The electric and gas companies opined that ES-C2M2 provides a good structure to frame the cybersecurity discussion, whereas an MIL rating model would be too subjective. Additionally, they were concerned that each company might apply the rating model differently. They do not want the process to be comparative in nature. Moreover, they were uncomfortable with a quantitative rating system for the ES-C2M2 detailed scorings, but would accept reporting maturity levels. They indicated it might be possible and expected that not all security domains would be at the highest level of maturity. Each company would balance the risk and value from moving to a higher level, while explaining their rationale for maintaining a certain maturity level in each category.
>
> PURA acknowledged that many factors contribute to a company's maturity level for a specific set of controls and assured the companies that they would be allowed to justify their reporting.

> [Certain utilities] indicated that they would adopt and follow ES-C2M2 in support of the PURA process. They claim to have been mapping their own programs against ES-C2M2 during development of the model and have noticed no gaps in either direction between their current programs and the emerging maturity model. However, the extent of coverage for each topic may differ. The companies noted that the ESC2M2 model provides the framework through which the utilities communicate with DHS and DOE at the federal level. [PURA's consultant] suggested that the companies' reports should describe their operational cybersecurity status over the prior year. Further details should also include discussion of the changing threat environment, level of attacks and number of attacks detected and thwarted. The companies saw this request as already covered by the ES-C2M2 reporting domain.

2.5 Encouraging Activity

Does your commission want to encourage activity and investments?

Commissions must determine whether they are worried about deficiencies enough to say that investments in cybersecurity are expected. While such encouragement might be seen by utilities as an opportunity to spend at will, such an approach has been used for other issues in the US such as renewable energy and low-income assistance. Some type of indication is often necessary, as utilities usually think that any issues regulators do not overtly encourage will not be allowed. Finding the right balance, however, is important so that utilities do not see this as an invitation for profligate spending. As in just about every decision regulators must make, encouraging prudent investment and prudent cybersecurity measures is the best approach.

Connecticut Case Study:

In Connecticut's strategy, the Commission outlined the activity that it broadly sought to encourage:

- Basic change: from cybersecurity as confidential company matter to information shared with regulators
- Attitude of utilities: recognize seriousness of cyber threat and need for new policies and actions
- Corporate culture: awareness and obligation to change security habits throughout the company
- Acceptance of need for education, constant communication
- Recognition that cybersecurity is a public issue

2.6 Relationships with Other Stakeholders

Who else will you work with (law enforcement, information technology, etc.)? How will you work with them?

The cybersecurity strategy should probably have a section that identifies the other stakeholders working on cybersecurity and outlines what the relationships and collaboration will be between the commission and all the different stakeholders and governmental agencies involved. This will help address and minimize any uncertainty, areas of overlap, and gaps in regulatory jurisdiction, as well as reinforce what the role of the regulator will be with respect to cybersecurity.

This section is important because many different stakeholders have a role to play in cybersecurity. Effective collaboration with all involved stakeholders allows for more informed decision-making. Law enforcement agencies, information technology management, vendors, the intelligence community, and neighboring utilities are all involved in cybersecurity. While the levels of engagement with different stakeholders may vary, commissions should determine what entities are most connected to their work and how they should best collaborate and communicate with them.

In the US Mid-Atlantic region, commissions convene a stakeholder group on a quarterly basis. Although the meetings are open and noticed, no official minutes are kept, and they are driven by the intent of informal context-producing conversations, rather than a formal joint investigation (which would be more administratively burdensome.)

It must be stressed that this section is going to be very specific to each regulatory commission based on country-specific circumstances. In the US, the federal and state jurisdictional issues mean that collaboration and coordination between stakeholders and governmental agencies can be tricky and complicated. Black Sea regulators are likely to encounter different and unique challenges specific to their respective countries.

In drafting this section, Black Sea regulators should consider the case of the Connecticut regulator PURA. PURA was in close collaboration with the Governor's office and shared drafts with stakeholders to review this section in particular. This helped ensure that everyone was on the same page about the role of the regulator and the relationship they would have with all other parties.

2.7 Standards

At the March 2017 workshop in Tallinn, Estonia, Black Sea regulators expressed an interest in potentially including the subject of standards in their strategies. Standards take time to develop and will likely evolve over time. Therefore, as regulators develop their cybersecurity strategy, they may want to consider explaining whether they intend to develop or adopt standards, rather than actually enumerating or developing the standards themselves.

Black Sea regulators interested in cybersecurity should certainly become familiar with what the NERC Critical Infrastructure Protection (CIP) standards require for the bulk power system. These mandatory standards and compliance-based structures oblige operators of the bulk power system to conform to specific cybersecurity practices. In addition to reviewing the NERC CIP standards, Black Sea regulators should also review the National Institute of Standards and Technology's Cybersecurity Framework (CSF). Taken together, the NERC CIP and NIST CSF stand as the current best practice for how a standard and risk-management-based approach complement each other to effect strong cybersecurity.

It is important for commissions to understand that there is a distinction between standards and best practices. This in many ways relates to the distinction between compliance-based and risk-based approaches to cybersecurity, which NARUC's 2017 Cybersecurity Primer for Regulators covers in great detail. Below is an excerpt from the Primer on this subject:

> The NERC standards have evolved over time, but fundamentally are a requirements-driven approach. Although these standards are robust and a strong improvement over what existed before, state regulators should bear in mind that the NERC CIP Standards are still evolving as they relate to the bulk electric system. Those interested in improving these standards argue that

distribution systems and other key areas where cybersecurity remains a concern to state regulators may not be covered entirely by the existing standards. Additionally, those who argue that the CIP standards are incomplete point out that compliance only proves compliance; utilities' cybersecurity should be based in risk assessment. Risk management includes assessment, mitigation, and continuous improvement, whereas compliance offers a view of cybersecurity at a fixed point in time, not a dynamic picture of it. Utilities may be compliant with the CIP standards and still not be secure. Utilities may also be secure but not be compliant with the CIP standards. One is not the guarantee of the other. As such, these standards provide an essential floor, whereas using other tools in complement to the standards may yield an even stronger risk-based outcome.[1]

This section of the Primer underscores that compliance and standards alone may be a great baseline, and they may contribute to good cybersecurity performance. However, regulators should not think that a simple checklist or a requirements-driven approach through specific standards will be enough.

In light of this, a regulator's strategy may want to underline that the commission understands the distinction between standards and best practices and will work with utilities and governmental agencies to establish appropriate country-specific standards and to utilize a risk-based approach to motivate good, effective cybersecurity performance. A strategy could also simply cover a commission's approach to developing rules. The NERC CIP Standards are a good resource to at least identify the topical areas where standards have been applied. Below are the CIP Standards Version 5[2]:

Number	Title/Summary	Enforcement Date
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	07/01/2016
CIP-003-6	Cyber Security - Security Management Controls	07/01/2016
CIP-004-6	Cyber Security - Personnel & Training	07/01/2016
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	07/01/2016
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	07/01/2016
CIP-007-6	Cyber Security - System Security Management	07/01/2016
CIP-008-5	Cyber Security - Incident Reporting and Response Planning	07/01/2016
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	07/01/2016
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments	07/01/2016
CIP-011-2	Cyber Security - Information Protection	07/01/2016

[1] NARUC Research Lab's Cybersecurity Primer for Regulators, 2017. Pg. 12

[2] http://www.nerc.net/standardsreports/standardssummary.aspx

CIP-014-2	Physical Security	10/02/2015

In contrast to the bulk power system, it should be noted that there are presently no mandatory, enforceable, or comprehensive standards in place at the distribution level in the US.

2.8 Other

What else does a commission need to learn to be ready?

Each commission will need to determine what level of readiness is acceptable for them and how much in terms of time, effort, and attention they want to invest in cybersecurity. What level of staff time and resources do they want to dedicate to learning about cybersecurity? Do they want any staff to become subject matter experts or at least fluent in the vernacular? Do they need any staff to get certifications or clearances? Answers to these questions will vary by commission depending on their priorities and goals.

How will a commission will evaluate itself and improve?

Regulators should also consider how they will measure their own success and engage in a cycle of continuous improvement.

3. Developing Internal and External Communication Strategies

As noted throughout this document, communication—both within a commission and between regulators and utilities—is absolutely essential to effective cybersecurity. As commissions develop their cybersecurity strategies, they must also determine internal and external communications strategies for cybersecurity that may include differences from their standard communications protocol.

Internally, commissions must develop a communication strategy that allows different departments representing different interests to talk and discuss their priorities and concerns regarding different issues related to cybersecurity and incorporate that process into the cybersecurity strategy development and execution. As with other issues, different departments within a commission will have different priorities for cybersecurity. As an example, Information Technology staff may be more disposed toward cybersecurity investments by utilities, while finance staff may look at the same investments more unfavorably due to the potential for the costs to be passed on to the consumer. It is important for groups with competing interests within a commission to talk to and understand each other in order to develop a more complete understanding of the risks posed by cybersecurity and the options available in developing a commission's strategy.

Externally, commissions should determine the means and methods for communication that are most effective for them given their relationships with utilities. As mentioned earlier, the most successful US commissions have found that a different approach is needed in communicating and engaging with utilities on cybersecurity. While relationships between commissions and utilities may at times be contentious when dealing with other issues, that contention should not carry over into the realm of cybersecurity.

Cooperation and engagement are keys to effective security, and they are crucial for the relationship between regulators and utilities in addressing cybersecurity. The most successful US commissions have found that it may be necessary, in order to develop an effective working relationship with utilities, to develop a communications strategy around staff that do not interact with utilities regarding other issues. Instead, designating staff that are involved in the cybersecurity working group, such as technical or policy staff, to communicate with their counterparts at utilities can help to begin a more collaborative discussion. Opening different channels for communication sends a message to utilities that regulators want to engage in a productive relationship that is separate from the other issues that may be more divisive.

4. Draft Structure of Cybersecurity Strategy

This section is intended to provide a template that commissions can customize and adapt based on their specific needs, priorities, and country-specific circumstances. This draft structure provides important topics and areas that might be useful for commissions to include or think about as they develop their strategies. However, each commission should ultimately determine the structure that is most useful for them.

Statement of Importance of Cybersecurity as a Commission Priority and Commitment to Act

- What are the commission's values and goals?

Scope of Engagement – Sectors Where Regulators Will Engage

- Defining scope and focus of a commission's strategy

Commission Internal Preparation

- Developing a working group with representation from across the commission

Performance Requirements for Commissions and Utilities

- Determining expectations of and interactions with utilities

Reporting

- Reporting practices before, during, and after events

Role and Relationship with Other Bodies (Public Sector, Law Enforcement, Utilities)

- With what other stakeholders will a commission work and how will they engage?

Internal and External Communication Strategies

- Developing effective communications strategies that may be outside the norm

Standards

- Outlining the approach a commission will take with regard to setting in place voluntary or mandatory rules
  Part I – Does the commission want to develop standards?
  Part II – If yes, what will the process be, what topical areas will be covered, and what documents and existing standards or frameworks might serve to provide guidance for the commission in the drafting process (NERC CIP, NIST, etc.)?

Cycle of Continuous Improvement

- How a commission will evaluate itself and improve

Direction of Growth

- Starting small and moving toward greater capability

For questions regarding this publication, please contact
Erin Hammel (ehammel@naruc.org).

National Association of Regulatory Utility Commissioners (NARUC)
1101 Vermont Ave, NW, Suite 200
Washington, DC 20005 USA
Tel: +1-202-898-2210
www.naruc.org