SAFETY Act Electricity Sector Applications
September 2017

Introduction

The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate's Office of SAFETY Act Implementation (OSAI) provides the following information to electricity generators and distributors who are interested in seeking SAFETY Act protections for physical and cybersecurity measures designed, developed, or modified to prevent, detect, identify, or deter acts of terrorism or limit the harm such acts might otherwise cause.

This information is intended to provide potential applicants in this industry a thoughtful approach for beginning their SAFETY Act application. This is not intended to change how an applicant applies and this is not intended to be binding guidance. This is intended to provide insight into how OSAI is approaching the review of these types of applications and the types of information OSAI may request during the application review process.

OSAI believes it is important to emphasize that the SAFETY Act Program seeks to incentivize the development and widespread deployment of effective anti-terrorism technologies and capabilities. It is not a regulatory program that focuses on compliance with a set of requirements, but is one that seeks to encourage discretionary activities that strengthen anti-terrorism capability. Thus, as stated below under "Relationship to the NERC CIPs", our evaluation of a SAFETY Act application will look for aspects of cybersecurity and physical security programs that go "above and beyond" regulatory requirements. Applicants must clearly show this "above and beyond" or "forward leaning" aspect as part of a SAFETY Act application.

Identifying and gathering the information required to support this kind of application can be challenging. This discussion is intended to help you structure your application to make for a more efficient submission and evaluation process. OSAI may provide additional resources at a later date to help applicants in this sector begin preparing SAFETY Act applications. This discussion contains the following:

1. The three-pronged application approach that OSAI finds to be the most efficient way to evaluate these types of SAFETY Act applications.
2. Helpful hints for getting started with an application
3. Examples of documentation you should include for each kind of application
4. Information on the relationship between SAFETY Act applications, the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards (NERC CIPS), and the National Institute of Standards and Technology (NIST) Cybersecurity Framework

Three-Pronged Application Approach

Applicants are encouraged to consider the three-pronged application approach shown in Figure 1 for electricity sector SAFETY Act applications.

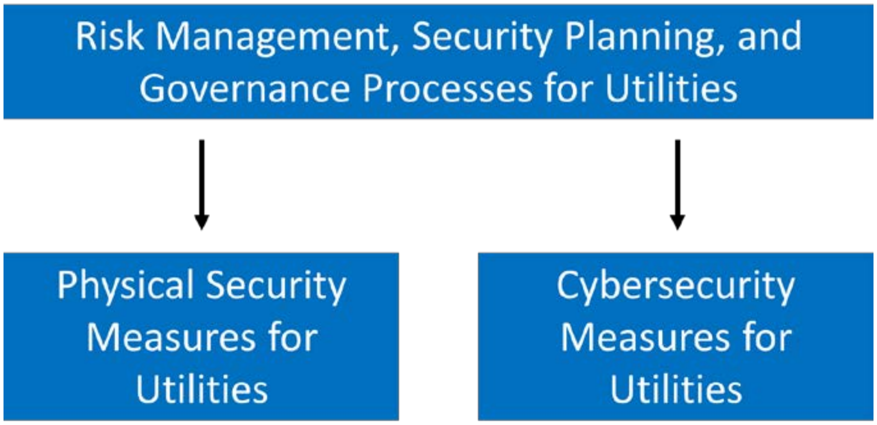
Risk Management, Security Planning, and Governance Processes for Utilities
Physical Security Measures for Utilities
Cybersecurity Measures for Utilities

Figure 1. Three-Pronged Application Approach

First application – focus on the Applicant's risk management, security planning, and governance processes for utilities. This application should provide information on the Applicant's top-level security practices, planning, risk management, and business continuity planning, as well as organizational elements that form the foundation of a security (cyber and physical) program. The application should be based on the development of policies, procedures, and planning for cyber and physical security, including the conduct of risk/vulnerability assessments, business continuity and disaster recovery planning, internal standards or security postures, and security strategies. Further, this application should address dissemination of internal, corporate physical security and cybersecurity practices. It should also include internal audit processes that show adherence to these corporate practices and regulatory requirements. Additional attention should be given to the overall corporate quality management system.

Second application –address physical security measures. This application provides a more detailed approach to the governance application, including physical security technical assessments. It should focus on operational implementation—for example, the method by which the utility puts into place specific physical security measures at individual locations such as sub-stations, distribution networks, and plant facilities. This application could be focused on the selection and maintenance of equipment, the quality of the service providers, and the repeatability of integration through use of qualified practitioners across all locations. An Applicant's compliance with applicable standards and regulations would be a factor (but not the focus). Inspections, audits, and documented physical security measures—including consistent anti-terrorism measures—would be useful.

Third application – address the cybersecurity program. This application should focus on the technical controls of the cybersecurity program. Security controls that safeguard or provide countermeasures to avoid, detect, or minimize security risks to physical property, information, computer systems, or other assets should be included.

Each of these three applications will be considered independently. Therefore, Applicants can submit one or more in any sequence. However, OSAI does encourage Applicants to consider filing the overarching risk management, security planning, and governance processes application (what we call the “first” application) before either of the two operational applications. In addition, for physical and cyber controls, OSAI may request a site visit as part of the evaluation preparation or process. The visit is to help provide OSAI further supporting evidence and exposure to the program architecture and systems.

Before You Start the SAFETY Act Evaluation Process

Preparation is the key to successfully filing a SAFETY Act application, no matter the type. The following two helpful hints can minimize the need for multiple submissions and information requests from OSAI.

A. Clearly Describe/Define the Technology for Which You Are Seeking SAFETY Act Protection.

Defining your technology (that is, the program or set of technologies that you employ at your utility) earlier can help guide your submission process. This Technology Description is the “what” and the “how” of your technology, and tells us who you are and what you do. The SAFETY Act uses the word *Technology* to mean whatever it is that you provide or use internally that creates an anti-terrorism benefit. We suggest you start by defining your baseline anti-terrorism offering and those elements that are customizable or optional.

When describing your Technology, try to keep it as simple as possible and do not try to “sell” it to us. We are looking simply for the facts: what is your technology and what you are seeking SAFETY Act protections for? Do not use marketing language or descriptors that can not be supported by effectiveness data.

It is important to be clear and direct in describing your Technology. The Technology Description is what will be evaluated for SAFETY Act protections and what would eventually form the legal definition of your Technology and be protected under the SAFETY Act. When describing the services your company provides, use active voice to describe what you are doing.

Drafting a Technology Description is intended to be interactive—it is a collaborative process between you and DHS to determine the most complete definition that can be reasonably evaluated as part of our review and sufficiently supported by your submission. While this process is collaborative, you must approve the Technology Description as it is yours. Also, please remember—if you make changes in the future or update your Technology with more components, you are able to modify your Technology Description later via a Notice of Modification. So start with what you are doing today, not what you plan to do in the future, and focus your Technology Description on things that you can support now.

B. Carefully Consider the Documentation Needed to Support Your Application.

Thinking carefully about the information you need to provide will offset the possibility of incomplete applications and delays in evaluation. The program office can provide additional details on what you might need to prepare based on your specific application and business. This can be accomplished through a SAFETY Act pre-application process. For more information about this process, contact the SAFETY Act helpdesk.

Example Documentation

The following documentation should be collected to support each of the three application types.

A. Risk Management, Security Planning, and Governance Processes for Utilities

The core of this first application will be the clear definition of a set of responsibilities and practices exercised by those who are responsible for making sure that risks to a utility are managed appropriately and that an enterprise's resources are used responsibly. This will include a definition of your organizational structure, information on policies and procedures, a list of personnel and their responsibilities, a strategy for measuring performance, and information showing that policies are updated as needed.

Applications should include plans, policies, and internal standards for governing your physical and cybersecurity programs. A key part of a governance application is telling us how you conduct threat, vulnerability, and risk assessments. You should define your general methodology, include examples of such assessments, and supply information on how results from these assessments affect changes in the defined program. Applications should include information on the sources of information used to inform these assessments. Finally, Applicants should discuss the implementation (or not) of any recommendations.

Applicants should also supply information on the "who" of the governance structure. This information should include the commitment of management to physical and cyber security, as well as a discussion about the experience and qualifications of a core staff. Typically, Applicants supply:

- A sample organizational chart
- The base qualifications for key roles, including job descriptions and resumes
- Policies for recruiting, hiring, and screening personnel, including sample background checks
- Information on training supplied and training records
- Information on tabletop exercises that might be used to train employees

Applicants will also need to define how they measure the performance of their governance program.

B. Physical Security Measures for Utilities

Typically, this type of application will identify the physical footprint (that is, the locations affected) and the site components or assets that are considered critical and essential to each location. Documentation might include a methodology for determining the unique vulnerabilities and threats facing each site that identifies critical components or assets implemented based on the vulnerabilities facing a given location. The following aspects of physical security might also be considered during the review of a physical security application:

- Unique facility characteristics
- Threat history/documentation review
- Threat intelligence reporting

- Physical security and resiliency measures
    - Physical barriers and site hardening
    - Physical entry and access controls
    - Security lighting
    - Intrusion detection systems
    - Video surveillance
    - Security personnel
    - Security policies and procedures
- Relationships with law enforcement and other emergency responders

Applicants should consider submitting information and documentation to support the following characteristics of its physical security measures:

- Mature, documented, and actively implemented and monitored policies, procedures, processes and controls
- Adequate resources including sufficient staff with required skills and training
- Leadership engagement at all levels
- An environment conducive to self-evaluation, continuous learning, adaptation, and improvement
- The incorporation of robust security standards and practices

In addition, evaluators reviewing these types of applications will consider the following standards as they review your materials:

- NERC Security Guideline for the Electricity Sector: Physical Security
- NERC Security Guideline for Physical Security Response
- ASIS International General Risk Assessment Guidelines
- ASIS International Facilities Physical Security Measure Guidelines
- ASIS International Security Management Standard: Physical Asset Protection
- Whole Building Design Guide
- Threat/Vulnerability Assessments

You should be familiar with these standards and ensure that your application shows familiarity and compliance with them.

C. Cybersecurity Measures for Utilities

In submitting this type of application, applicants should provide sufficient information to define an operational control system or systems subject to cyber risks, the critical components of the system, their interconnections, external dependencies, and the adequacies of the protective defense measures. Applicants should implement, monitor, and document operational and technical controls to achieve optional cybersecurity for their specific environment(s).

The following are examples of key documentation and information that should be submitted with this type of application:

- A diagram of the operational systems that shows network the network topography and segmentation. It should include key end-points and security components such as firewalls, bastion hosts, and similar devices. Diagrams should be annotated and describe data flows and connections to external systems, including interconnections to supporting business systems and remote systems.

- Provide location data—to what locations does this network architecture apply?
- Provide a listing of technology components. These typically are servers, network components, PLCs, SCADA, ICS, and other connected or remotely accessible devices that are able to affect system integrity, resiliency, reliability, and availability. Provide the characteristics of the devices.
- Outline the key uses or roles with access to critical operational and security components. Indicate if access is remote.
- Provide an inventory of software integral to systems operations and security.
- A list of ports, protocols, and services, and their associated purposes and uses.
- Provide policies and procedures for the recruitment, hiring, vetting, and training of cybersecurity personnel.
- Provide procedures, process documentation, configuration files, systems logs, or comparable records that provide evidence of:
    - Access control enforcement in accordance with established policies and procedures.
    - Vulnerability scanning and active network/security monitoring.
    - Active and current patching, malware protection, and configuration management.
    - Ability to identify and actively manage connected, remotely accessible, and automated operational devices.
    - Required security device features are enabled and properly configured.
    - Effective media management and disposal.
    - Active security auditing and oversight.

In addition, evaluators reviewing these types of applications will consider the following standards as they review your materials.

- The NIST Cybersecurity Framework
- NERC CIP Standards
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- NIST SP 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

You should be familiar with these standards and ensure that your application shows familiarity and compliance with them.

Relationship to the NERC CIPs

Assessing electricity sector applications for SAFETY Act protections presents unique challenges. United States electric utilities operate the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards (NERC CIPS). Conformity to the NERC CIPS, while necessary, does not guarantee SAFETY Act coverage. A SAFETY Act assessment will focus on cybersecurity and physical program execution elements “above and beyond” the NERC CIPS requirements. A heavy emphasis will be placed on how an organization documents that its programs are effective, particularly through the use of performance measures.

Prepared: September 25, 2017