Guide to CIP Cyber Vulnerability Assessment

Executive Summary

The North American Electric Reliability Corporation adopted Critical Infrastructure Protection standards in 2006. The standards establish the minimum requirements needed to ensure the security of electronic exchange of information needed to support the reliability and the bulk power system. Industry feedback at conferences and meetings indicate uncertainty about implementation of the standards. Sandia National Labs Center for Control System Security (C2S2) undertook a work package for the Department of Energy's Office of Electricity Delivery and Energy Reliability under the National SCADA Test Bed program to develop guidance for conducting assessments required by the new standards. Sandia built on experience performing over 100 critical infrastructure assessments to develop a project plan for a CIP Cyber Vulnerability assessment of an actual utility. They performed that assessment with the help and cooperation of the utility to gain lessons for inclusion in the guidance. As a result, the team believes that the most important aspects of these assessments are cooperation, safety, and developing actionable information for mitigation. We believe that any group or organization that plans to conduct CIP Cyber Vulnerability Assessments would do well to consider the guidance in this document.

i. Table of Contents

ii. How to use this Guide

If you are new to cyber vulnerability assessment, you should read sections 1 and 2 to gain a better understanding of the concepts. If you are an experienced assessor from the information technology world, you should start with section 2 to gain some understanding of assessment of control systems. If you are an experienced control systems assessor, then you may want to jump straight to section 3 and the detailed task descriptions.

1. Introduction

In 2006, the North American Electric Reliability Corporation (NERC) adopted the Critical Infrastructure Protection (CIP) standards. The standards establish the minimum requirements needed to ensure the security of electronic information exchange supporting the bulk power system. Industry feedback at conferences and meetings before and after the standards were released indicate uncertainty about implementation of the standards.

1.1. Purpose

The purpose of this document is to guide the planning, execution, and reporting of CIP Cyber Vulnerability Assessments of utilities' critical cyber assets and electronic security perimeter. Two different but related cyber vulnerability assessments are needed to meet the requirements of assessment of critical cyber assets per CIP-007 and to meet the requirements of assessment of the electronic security perimeter per CIP-005.

1.2. Scope

This guide discusses the overall process of conducting CIP Cyber Vulnerability Assessments, provides detailed information about the steps in the process, and points to resources that can help an assessment. This is a parent document that refers to other resources: a planning spreadsheet, an example of a filled-out spreadsheet, and an example of a project plan. These resources are not necessary but are very helpful in understanding the content of this guide; they should be included with and in the same location as this guide.

1.2.1. Resources

The useful resources associated with this guide include:

1. Planning Spreadsheet (SystemTemplate.xls)
2. Example filled-out planning spreadsheet (CIP_CyberAssessmentPlanningList.xls)
3. Microsoft Project template Plan (CIP assessment.mpp)

1.2.2. Document Overview

This document contains two major sections. The first section describes the overall process of planning, conducting, reporting and closing out a CIP Cyber Vulnerability Assessment using the resources. The second section describes the tasks that must be performed in the assessment. The tasks descriptions help with the planning and performance using the planning spreadsheet and/or the Microsoft Project plan.

1.3. Acronyms and Abbreviations

CIP – Critical Infrastructure Protection
EMS – Energy Management System
NERC – North American Electric Reliability Corporation
SCADA – Supervisory Control and Data Acquisition

2. Overview of Assessment Process

The NERC CIP cyber vulnerability process outlined in this guide is a custom form of a standard assessment process. This guide uses materials from more general Sandia assessment techniques that have been customized specifically for the CIP cyber vulnerability assessment. The process steps should be familiar with anyone who has performed an information system security assessment. The process includes planning, conducting, reporting and closing out the vulnerability assessment. The process should suffice to answer the requirements of CIP-005 and CIP-007 for annual cyber vulnerability assessments.

The process will not answer questions about the priority of vulnerabilities for mitigation, the consequences of exploiting a vulnerability, or the likelihood of a particular adversary attacking the system. There are other processes that take assessment further than the standard CIP cyber vulnerability assessment which answer further questions. While the CIP cyber vulnerability assessment will discover security possibilities, it makes no attempt to determine the probability of an attack or the probability of an undesired consequence. Those questions require considerably more analysis.

Before diving into the process, we need to understand the requirements that drive this process.

2.1. CIP Cyber Vulnerability Requirements

The NERC CIP standards require annual cyber vulnerability assessments of critical cyber assets and their networks. NERC CIP-005, Electronic Security Perimeter requires:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> > R4.1. A document identifying the vulnerability assessment process;
> >
> > R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
> >
> > R4.3. The discovery of all access points to the Electronic Security Perimeter;
> >
> > R4.4. A review of controls for default accounts, passwords, and network management community strings; and,
> >
> > R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

NERC CIP-007, Cyber Security – Systems Security Management, requires:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> > R8.1. A document identifying the vulnerability assessment process;
> >
> > R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
> >
> > R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

A key point related to the requirements of NERC CIP-005 is the interaction between the Electronic Security Perimeter and the Physical Security Perimeter specified in CIP-006. From CIP-006, Cyber Security – Physical Security of Critical Cyber Assets:

> R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

Correspondingly, CIP-005 refers to CIP-006 in this requirement:

> R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

These requirements determine the nature of a CIP cyber vulnerability assessment as well as the scope of that assessment. Much of the work to meet both requirements is the same, so the assessment should be a single activity with the dual goal of satisfying the two primary requirements.

The first commonality across the requirements is the emphasis on ports and services. Clearly, for both types of CIP cyber vulnerability assessment, the ports and services running on all cyber assets in or protecting the ESP should be collected. The need for determining account security applies to both requirements.

The difference arises with the determination of access from outside the ESP. CIP-005 requires either penetration testing (which we do not recommend) or analysis of external access controls. Fortunately, CIP-005, R3.2 and R5.3 between them require retention of electronic access logs for ninety days. These logs can be used in conjunction with analysis of firewall rules and router ACLs to arrive at the same information as would be gained from penetration testing.

Thus, we can see that the CIP cyber assessment process will need to answer the requirements of CIP-005 and CIP-007, while keeping in mind the requirements of CIP-006. The CIP cyber assessment process can take advantage of commonality of data that must be collected to save resources, but some analysis will need to be performed for each CIP standard requirement.

2.2. Process Overview

The CIP cyber assessment process begins with the recognition by a responsible entity that they are required to meet the requirements discussed in the previous section. Since the CIP cyber assessment process results will include detailed understanding of the ESP and system services, the results of a first assessment can be used to satisfy other documentation requirements. For example, a responsible entity may use an initial CIP cyber assessment both to fulfill the requirement for that assessment as well as the initial requirement for documentation about the ESP (CIP-005, R1.6).

The real first step of the assessment process is planning for the assessment. The next step in the assessment process is conducting the assessment. The third step in the process is reporting the results. The final step is planning mitigation once the report is accepted.

2.2.1. Planning

A CIP cyber assessment is not something that can or should be done off-the-cuff. The assessment team will need to plan the assessment in close collaboration with the operations and engineering personnel at the responsible entity. There are multiple reasons for careful, collaborative planning.

The assessment activity will require more resources than just the assessment team. System and network administration personnel will need to support the assessment by providing data and access. This can be a stress on key personnel, especially in conjunction with other audits, assessments, system changes or other activity.

The assessment will need to be scheduled at a time when operational stresses do not complicate the situation. For example, some regions have bad weather that causes outages during certain seasons. Adding the stress of an assessment to the stresses of responding to outages will cause problems with the operations and engineering personnel who need to work with the assessment.

The assessment team will need to consider the scope of the effort – how long will it take, how many assessors will be required, how will data be collected, who will collect the data, how many systems will be assessed at how many locations – all of these questions will need to be answered to plan the assessment.

2.2.2. Planning process

The first step in the planning process is to determine the scope of the assessment. The process will proceed from there through determining performance requirements, estimating resources, travel costs, project plan, rules of engagement, and team identification.

2.2.2.1. Assessment team roles and responsibilities

Team identification is the last step in the planning process, but the understanding of team roles and responsibilities is necessary from the beginning of the planning process. Team identification is the assignment of specific individuals to team roles based on knowledge and skills. The roles should be known from the start of planning.

Ideally, an assessment organization can draw upon a diverse set of people and skills to form assessment teams that best fit the requirements of a particular assessment. In the case of CIP cyber vulnerability assessments, the assessment organization needs access to the skills of information technology assessors, control systems engineers, and physical security assessors.

The team lead is the first role to be fulfilled. The team lead will perform or supervise all of the planning of the assessment. The team lead will lead the team during the phase of conducting the assessment and will manage any changes necessary during that phase. The team lead will ensure the results are reported and the responsible entity gets the support they need during mitigation planning. The team lead will need to have both managerial skills and technical skills to accomplish all of these tasks. In some cases, the assessment organization may need to split the team lead role into two parts: project management and technical management.

There will be one or more team members. These persons will perform the actual technical assessment tasks during the assessment. The team members will also provide their part of the

results reporting. Team members may also be called on to support mitigation planning. Team members are assigned during team identification unless the team lead needs specialized expertise during planning.

The assessment team needs one or more report writers. The report writer can also play another role in the assessment team, such as team lead or member. The report writer will collect and edit the contributions of the team members and produce the assessment report.

2.2.2.2. Planning performance requirements

The first step in planning is scoping the assessment and determining the performance requirements. The numbers and types of critical cyber assets and applications that execute on those cyber assets determine the scope of the assessment project. The size of the electronic security perimeters will affect the scope as well – larger enclaves imply more complex internal network infrastructure requiring more assessment. The number of electronic security perimeters and communication paths between them are important to determining the scope and performance requirements. Another factor is the number and physical dispersal of locations of critical cyber assets.

2.2.2.3. Estimating resources

The second step in planning is to estimate the resources required. The planning tools supplied with this guide can help in estimating the resources.

2.2.2.4. Estimating travel costs

Travel is a fact of life in performing CIP cyber vulnerability assessments. If the assessment organization is based in the same location as the responsible entity, the travel costs will be limited to trips to outlying locations such as alternate control centers, generation plants, and substations. More likely, the assessment organization is based far enough away from the responsible entity that travel, lodging, and food costs can be significant contributors to the total cost of the assessment.

2.2.2.5. Writing the project plan

Conducting the assessment will require a careful coordination of resources and access to critical cyber assets to balance the needs of the assessment against the operational requirements of the responsible entity. A project plan that includes all the necessary actions of all the participants in a schedule is necessary to the safe execution of the assessment.

2.2.2.6. Rules of engagement

Cyber security assessments can be limited to paper exercises but CIP cyber vulnerability assessment inherently involves active engagement. The assessors must either access or watch others access critical cyber assets within the responsible entities control systems. The assessment team lead must work with her counterpart in the responsible entity to develop rules for those activities that protect the operation of the responsible entity and limit the liability of the assessment team.

The rules of engagement should include direction about what activities may take place in what systems of the responsible entity and who may perform those activities.

The rules of engagement need to include decisions about whether activities take place within the primary active control system or some credible substitute. The safest solution is to avoid any active measures in the primary, active control system. Passive activities such as network sniffing may be allowed if all parties agree. Credible substitutes for the active control system can include a backup or secondary control system, a testing network, or stand-alone systems. All substitutes need to be compared to the active systems to ensure that they are identical in operation and therefore assessment.

The assessment team and the responsible entity will need to agree on who will have the "hands on the keyboard" during access to active control systems. The safest choice is for the responsible entity personnel to perform all actions within the active control system, providing the "hands on the keyboard" at the direction of the assessment team.

2.2.2.7. Team identification

This should be the last step in the planning process. The assessment team leader should have all the knowledge necessary to pick the best people for the team. The scope, performance objectives, resource requirements, travel, project plan, and rules of engagement should all inform the decision of who to pick. Just as significant is the need to pick a team that is as diverse as possible. A team of nearly uniform composition will all see the same vulnerabilities. A diverse team, even at the cost of specific technical expertise, will discover more vulnerabilities.

2.2.2.8. Planning Tools

We have provided two tools to help planning (not including section 3 and 4 of this guide). The first tool is a Microsoft Excel-format spreadsheet, CIP_CyberAssessmentPlanningList.xls. The second tool is a Microsoft Project plan, CIP_CyberAssessmentPlan.mpp. An assessor may want to use one or the other or both in planning an assessment.

2.2.2.8.1. Assessment Planning Spreadsheet

The spreadsheet follows the task structure and descriptions in Section 3. Each row of the spreadsheet corresponds to a task in the Work Breakdown Structure (WBS) in Section 3. Columns include the WBS number, which assessment (CIP-007 or CIP-005) the task is part of, the work location for that task, the task name, estimated number of man-hours to accomplish the task, estimated elapsed time to accomplish the task, the number of instances of the work described in the task, who can do the work, task dependencies, required utility assets, and an attempt at calculating the total man-hours.

Several ideas in the spreadsheet need some explanation. First, it does not include all of the WBS rollups – there are tasks 1.1.1 through 1.1.9 but no rows for the 1.1 or 1 rollups. Secondly, the spreadsheet includes sample WBS structures for one control center, one generation plant, and two types of substations. Most responsible entities have more than one control center, with at least a backup control center. Some responsible entities split control among more than one control center. Not all responsible entities have generation critical assets, but if they have any they may have more than one. Substations within responsible entities are rarely standardized, so the assessor will have to plan for different substation types. The spreadsheet has a start at that planning requirement with two substation types. The spreadsheet has two time columns, one to reflect actual hands-on man-hours and one to reflect the elapsed time for the activity. In certain cases, assessment activities involve simple setup and execution of computer programs that can take a long time to complete. In those cases, the man-hour time is short but the elapsed time can

be long. The "Who can do it" column was an early attempt to show the skill-set required. The assessment on which this spreadsheet is based included resources from Sandia as the assessors, a utility, and a university computer engineering graduate school. "Assessor" means that only someone with the skills expected of a security assessment organization can perform the work. "Utility" implies that Responsible Entity system and network administrators will have the necessary skills to perform the task. "Any" implies that any of the three types could perform the work, including Computer Science and Computer Engineering graduate students who have not performed assessments and have no knowledge of the utility networks and computers. The user of the spreadsheet will need to understand the technical skills of their personnel resources to plan. The Dependencies column shows how tasks depend upon other tasks having been completed. The Requirements column indicates what special resources from the Responsible Entity are required for the successful completion of the task. In most cases, the Requirements imply a level of access. A Responsible Entity may, if they choose, provide the credentials for that level of access to the assessor; however, we recommend that the Responsible Entity reserve access to their own personnel.

Requirements Name	Description
CC Local Admin	Local administrator on a particular host or host(s) within the control center(s)
CC Test Network	A test network separate from the operational control center network with systems that duplicate operational systems
CC Network Admin	A network administrator on the control center network – examples are a domain administrator in a Microsoft network or
CC Network Eqpmt Admin	Administrator for network equipment such as routers, firewalls, and switches
Gen Local Admin	Local administrator on a particular host or host(s) at a generation plant to be assessed.
Gen Network Admin	A network administrator on the control center network – examples are a domain administrator in a Microsoft network or…
Gen Test Network	A test network separate from the distributed control system (DCS) of the generation plant with systems that duplicate operational systems from the DCS
Gen Network Eqpmt Admin	Administrator for network equipment such as routers, firewalls, and switches
Substation Engineer	Engineer responsible for the design and maintenance of a substation and its control system equipment

Table 2-1: Responsible Entity Required Resources

2.2.2.8.2. Assessment Planning Project Plan

This tool is simply a Microsoft Project file that captures the tasks in the spreadsheet. Some of the dependencies have been included and there are placeholders for some of the resources. Users

will need to add tasks to reflect the assets of the responsible entity, modify the dependencies to fit with additional tasks, and modify the resources to reflect the reality of their situation.

2.3. Conducting the assessment

Conducting the assessment simply means carrying out the assessment plan. As in warfare, however, no plan survives contact with the enemy. In our case, our plan will not survive intact once we start the actual assessment. Surprises will start with last minute changes in personnel, personnel availability, and times of access to various locations. These surprises will arise from circumstances beyond anyone's control, from communication failures, and from changed direction within the leadership team of the responsible entity. The assessment team leader will need to adapt the plan, reschedule tasks, and reallocate resources to fit reality.

The assessment team lead should try to maintain the integrity of tasks within the plan to ensure no conflict with the operations of the responsible entity. Tasks may need to be rescheduled, but they shouldn't be broken up so that the active engagement period is longer or more fragmented.

Although tasks are distinct within the project, the assessment team lead needs to make sure they are conducted not by project order but in the order that makes the most sense and causes the least operational disruption. The services check and account check for each critical cyber asset should take place simultaneously, to minimize the time of access to the asset. Even though the external services check needs to supplement the internal, they don't have to take place at the same time. Instead, the internal and external activities can be done separately with a little extra checking to make sure there has been no change to the platform in the meantime.

2.4. Reporting the results

The key goal of the assessor in reporting the results is to provide actionable information. The responsible entity has the requirement within the CIP standards to present a document identifying the vulnerability assessment process, documentation of the assessment results, an action plan to remediate or mitigate vulnerabilities, and the execution status of that action plan. All but the last item are either in or derived from the assessment report.

The assessment report should include a full description of the assessment process. This can be derived from the assessment plan but needs to include specific technical information sufficient that the responsible entity can ask others to duplicate the results. Specific tools, methods, and techniques for the primary results need to be called out for future use. This section of the report needs to have enough information so that auditors can be assured the assessment process fulfills the requirements of the CIP standards.

The assessment report should include all of the vulnerabilities found during the assessment. This seems obvious, but the key to making the vulnerability reports useful is linking them to the assessment process and to all the circumstances that make the vulnerability possible.

Specific information collected with the tools, methods, and techniques needs to be associated with those tools in the vulnerability report section of the assessment report. One of the unfortunate realities of security assessment is that the tool one uses today may not be available tomorrow. In those cases, a later assessor may not be able to determine whether a vulnerability still exists with the same tool. However, the assessor can find an equivalent tool based on the report of the vulnerability and the past tool.

The mere existence of a vulnerable service or outdated user login on a critical cyber asset does not constitute a vulnerability. The assessment report needs to show how that vulnerability can or cannot be exploited by a credible adversary. This is particularly true in CIP cyber vulnerability assessments with their inherent association to physical security. One example might be the use of a single login for all operators within the control center. On the surface, that appears to be a vulnerability. If the physical access controls of the control center prevent anyone other than operators from entering, those physical security perimeter components provide strong authentication. If a service running on a critical cyber asset is vulnerable, the report should include information about how an adversary would gain access to that service on that asset through the electronic security perimeter. In both of these examples, the responsible entity can take action by choosing from a number of mitigation strategies and ensure mission performance.

2.5. Planning the mitigation

There is no point to any form of assessment and particularly security assessment unless the owner of the assessment target uses the information provided in the assessment. Assessors must provide enough information to the owner of the assessment target to make an informed choice of mitigation strategies. Assessors should not get deeply involved in planning and executing the mitigation for fear of losing perspective and objectivity. However, assessors can make recommendations at a general level. The assessors should also be available to the mitigation planning team as an information resource and critical feedback source.

3. Detailed Tasks Descriptions

A CIP cyber vulnerability assessment will draw on both human and technology resources to perform the assessment within the project constraints. Human resources include security analysts from the responsible entity, the assessment organization, and any third-parties. Technology resources include tools and techniques that are industry standard as well as tools unique to the assessment organization.

For some purposes, the human resources are interchangeable. However, some tasks may require re-definition or interpretation during execution and would be better performed by analysts with the experience to do that function. Some tasks may require considerable time on-site at the Responsible Entity and would be better performed by their own security analysts and confirmed by the assessors. Some tasks may require access to a particular software system in a controlled environment in an off-line mode.

3.1. CIP-007 Critical Cyber Assets Vulnerability Assessment

CIP-007 calls for a Cyber Vulnerability Assessment of all cyber assets within the Electronic Security Perimeter, including a document identifying the vulnerability assessment process (this document), a review to verify that only the ports and services required for operation of the Cyber Assets within the ESP are enabled, a review of controls for default accounts, and documentation of the results, mitigation plan and mitigation status.

Assumptions

The folowing assumptions were made to allow the plan for this assessment to be developed:

- The control center scope is usually well known.
- The generation plan scope is less known – while the Responsible Entity may have determined that generation assets are critical per the CIP-002 standard, the cyber assets critical to control those generation assets are usually not well known.
- The substation plan scope is less known – while the Responsible Entity may have determined that certain substation assets are critical per the CIP-002 standard, the cyber assets critical to the control of those substation assets are usually not well known.
- There are at least two different substation architectures (seen during the scoping visit) with an unknown number of critical cyber assets within each architecture.

3.1.1. Control Center

Control centers are the first part of the responsible entity required to comply with the CIP standards and they have usually identified their critical cyber assets. There may be network equipment that is not on the current list; however, that will make a minimal difference. Every control center will have unique characteristics that make each assessment different.

3.1.1.1. Application Platform Services Check

This task is a simple check of the relevant configuration of the application platform operating system. For Microsoft operating systems, Windows registry settings and network status confirm the services that are exposed. In Unix-like operating systems, the daemons and init scripts along with a network status should show the services. Each platform check is simple, but the number of platforms can make this task costly. Various commercial and open source tools can greatly aid

this check, sometimes in combination with the account check. The technical requirements are within the capability of any team member, given the right procedures. Although any of the security analysts on the team could perform these tasks, they will require support from someone with the correct access rights from the Responsible Entity's control center administrators. Alternately, the assessors could develop the procedure and let a control center administrator do the actual collection, saving the time of the assessors and administrator. This latter course will require confirmation by the assessors through spot checks. If the spot checks turn up discrepancies, then the check will need to be performed on all application platforms.

3.1.1.2. Application Platform External Scan

This task is simple, technically, but can be more complex logistically. The best choice for this task is to perform it on a test network against system images from the control center network. In that case, the assessors can safely use standard vulnerability scanning tools to examine copies of the operational systems. If that is not possible, the next best choice is to use a redundant or back up system and perform the check over a redundant or backup network separate from the operational network. Because of the nature of scanning, the wall-clock time for this will be much greater than the effort time. Assessors can expect that they can scan one system per eight-hour period with no more than two hours of effort. This might also complicate the use of the testing network – after all, it is there for reasons other than the vulnerability assessment.

3.1.1.3. Application Platform Account Check

This task would be combined with Application Platform Services Check. This addresses a specific requirement of the CIP to look for default accounts. The task would also look for easily guessed or cracked account security. Any of the team's security analysts could do this work with confirmation by spot checks done by the assessment team.

3.1.1.4. Network Account Check

This task is the network (PDC/LDAP/Active Directory) equivalent of the platform account check. This work could be performed by any of the team members with the cooperation of the Responsible Entity's control center administrators.

3.1.1.5. Network Server Services Check

There are some servers that provide infrastructure upon which the critical control systems depend which are, therefore, critical cyber assets. Examples include the Active Directory servers and the DNS servers. This task is the same as the platform service check and, as such, can be performed by any member of the team.

3.1.1.6. Network Server External Scan

This task is similar to the platform external scan and should also be performed in the test network or other non-operational network. This is slightly more complex, technically, than a standard platform scan, but not enough to preclude performance by any security analyst on the team.

3.1.1.7. Network Equipment Services Check

This task is to switches and routers what the services check is to application platforms. This requires knowledge of network equipment configuration. Much of the configuration information obtained is also collected in task 2.1.1.1, below, so these could actually be combined. This task

would best be performed with Responsible Entity supervision if not done solely by their analysts since only they have access to obtain the configuration information.

3.1.1.8. Network Equipment External Scan

This task is problematic unless the test network allows for the test of network equipment (switches and routers). If that is not possible, the assessment may have to rely solely on the services check for network equipment. If that is unacceptable to auditors, then the assessors may need to collect the configurations as in task 1.1.7, install those configurations in identical equipment in an off-site test network and conduct the scans.

If it is possible to perform this on the test network, then any security analyst on the team will be able to perform it. Although this task has no more effort time than any other scan, the assessment team will need to allow considerably more wall-clock time – scans of routers and firewalls always take longer than application platforms and assessors will need to scan each network interface of the equipment.

3.1.1.9. Network Equipment Account Check

This task will involve checking default and simple authentication mechanisms at the console interface, at any configuration service ports offered over the network (http, telnet, ssh), and SNMP MIBs (i.e community strings). This should be within the capacity of all security analysts within the team, although the simplest way to do this would be via configuration information gathered in task 1.1.7.

3.1.2. Generation

Assumptions

The primary assumption in performing the CIP Cyber Vulnerability Assessment of critical cyber assets at generation critical assets is that they are identified. For purposes of description, we will assume that there is a single generation critical asset (not necessarily a good assumption) and four different computer application platforms at that asset (not unreasonable). The assessment team lead will need to modify these tasks to suit the actual scope.

3.1.2.1. Application Platform Services Check

This task is a simple check of the relevant Windows registry settings or Unix control files or VMS startup files and network status to confirm the services that are exposed. It may require little or a lot of effort for each check depending upon the operating system of the application platform. Because of the flexibility required and the possible use of less-known operating systems, this is a task best performed by experienced security analysts with assistance from a local administrator.

3.1.2.2. Application Platform External Scan

This task is simple, technically, but very complex logistically. Generation critical assets infrequently have a test network and may not easily image systems to that network. If that is the case, then assessors will need to image operational systems and use standard vulnerability scanning tools to examine copies of the operational systems. If that is not possible, then the assessors would only be able to perform this if the generation asset is off-line as it would be too dangerous to use those same tools on the operational systems. If the assessors can use a test

network, then this is well within the capability of any security analyst on the team. Because of the nature of scanning, the wall-clock time for this will be much greater than the effort time. Assessors should expect that they can scan one system per eight-hour period with no more than two hours of effort. This might also complicate the use of any testing network – after all, it is there for reasons other than the vulnerability assessment.

3.1.2.3. Application Platform Account Check

This task would be combined with Application Platform Services Check. This addresses a specific requirement of the CIP to look for default accounts. The task would also look for easily guessed or cracked account security. Again, since the nature of this task is uncertain, experienced security analysts should perform this work.

3.1.2.4. Network Account Check

This task is the network (PDC/LDAP/Active Directory) equivalent of the platform account check. An experienced security analyst should perform this with the cooperation of the generation network administrators.

3.1.3. Network Server Services Check

There are some servers that provide infrastructure upon which the critical generation systems depend which are, therefore, critical cyber assets. Examples include the Active Directory servers and the DNS servers. This task is the same as the platform service check and, as such, will require an experienced security analyst.

3.1.3.1. Network Server External Scan

This task is similar to the platform external scan and should also be performed in the test network. This is slightly more complex, technically, than a standard platform scan, and like that task will require the flexibility and experience of an experienced security analyst.

3.1.3.2. Network Equipment Services Check

This task is to switches and routers what the services check is to application platforms. This requires knowledge of network equipment configuration. Much of the configuration information obtained is also collected in task 2.1.1.1, below, so these could actually be combined. This task would best be performed with Responsible Entity supervision if not done solely by Responsible Entity analysts since only they have access to obtain the configuration information.

3.1.3.3. Network Equipment External Scan

This task is problematic unless there is a test network that allows for the test of network equipment (switches and routers). If that is not possible, the assessors may have to rely solely on the services check for network equipment. If that is unacceptable to auditors, then the assessors may need to collect the configurations as in task 1.3.2, install those configurations in identical equipment in an off-site test network and conduct the scans.

If it is possible to perform this on the test network, then any security analyst on the team will be able to perform it. Although this task has no more effort time than any other scan, assessors will need to allow considerably more wall-clock time – scans of routers and firewalls always take longer than application platforms, and the assessors will need to scan each network interface of the equipment.

3.1.3.4. Network Equipment Account Check

This task will involve checking default and simple authentication mechanisms at the console interface, at any configuration service ports offered over the network (http, telnet, ssh), and SNMP MIBs (i.e community strings). This should be within the capacity of all security analysts within the team, although the simplest way to do this would be via configuration information gathered in task 1.3.2.

3.1.4. Substation Type A

Assessors will likely discover that the responsible entity has more than one type of substation if one considers the cyber assets at the substations. This may be totally a factor of which company originally built that substation in the current climate of mergers and takeovers. However, the critical question is which substations are critical assets.

Assumptions

Substation critical cyber asset configurations are similar between critical asset substations of the same type. Thus, the assessment need only look at a single substation's critical cyber assets for each type of substation. There will be no more than four different critical cyber assets at this type of substation.

3.1.4.1. Platform Inventory

Determine what, if any, critical cyber assets are typically located at this type of substation.

3.1.4.2. Platform Research

Research the substation critical cyber assets to determine how to perform the services check, any scans, and account checks.

3.1.4.3. Platform Services Check

This task is highly dependent on the type of cyber asset at the substation. Most equipment has some method to obtain configuration information from a console port or other access. Fortunately, much of the equipment is likely to be from the same vendor. Because of the uncertainty, experienced security analysts should perform this task with Responsible Entity substation engineer assistance.

3.1.4.4. Platform External Scan

This task is highly dependent on the type of cyber asset at the substation. Scanning might be war-dialing or might be network scanning. Again, because of the uncertainty, expereinced security analysts should perform this task with Responsible Entity security analyst and substation engineer assistance.

3.1.4.5. Platform Account Check

This task is highly dependent on the type of cyber asset at the substation. Many substation cyber assets will have no access control and thus no accounts. Because of the uncertainty, experienced security analysts should perform this task with Utility substation engineer assistance.

3.1.5. Substation Type B

This is a placeholder under the assumption of more than one type of substation. The tasks are identical to those for a Type A substation.

3.1.6. Generate Report

This task will assemble the information about all the critical cyber asset vulnerability assessments into a single report for deliver to the Responsible Entity. The assessment team should perform this task.

3.2. CIP-005 Security Perimeter Cyber Vulnerability Assessment

CIP-005 requires an annual cyber vulnerability assessment of the Electronic Security Perimeter (ESP), including a document identifying the vulnerability assessment process (of which this is an example), a review to verify that only ports and services required for operations at the ESP are enabled, discovery of all access points to the ESP, a review of controls for accounts, passwords, and community strings, and documentation of results, mitigation and progress. Assessors should expect to find that Responsible Entities have many ESPs connected by various communication paths. Each ESP needs to be assessed, separately and together with connected ESPs. Substation ESPs will not need major assessment as they will not be networks.

3.2.1. Electronic Mapping

3.2.1.1. Control Center

3.2.1.1.1. Collect Network Configurations

Much of this task overlaps the critical cyber assets vulnerability assessment. This information will be collected as text files. Assessors can parse these files manually, write scripts to parse them, or use an automated parsing tool such as Sandia's ANTFARM. Assessors should keep in mind that network hardware configuration information can vary, even from the same vendor and model. This task will help fulfill the R4.2, R4.3, and R4.4 requirements. Any of the security analysts on the team can perform this task with the cooperation of the relevant network administrators.

3.2.1.1.2. Collect Network Traffic Patterns

This task will involve either simple network sniffing or collection of access log data from access control equipment such as firewalls.

Sniffing usually takes place at various points on the control center network. As that network is frequently simple, assessors should be able to limit the sniffing to the access points – the communications processors that connect to substations, ICCP DMZs, and a spot in the core network. Traffic captures can be collected and parsed by various commercial and open-source tools to generate part of the picture of the entire control center network and its connections. The sniffing portion of this task can be performed by any of the security analysts on the team and may not need to take place at all points at the same time. Sandia's ANTFARM system can also be used to process traffic captures.

Access log data from access control equipment should be kept for 90 days per CIP-005, so this data can be used to collect network traffic patterns at the access points to the ESP. Sandia's ANTFARM can process access logs to generate network maps.

3.2.1.1.3. Verify Network Routing

This is the only task in the control center network mapping that involves an active component. Any active network mapping in this task should be performed with the permission of the control center network administrators if not by them. Passive network mapping tools such as ANTFARM sometimes requires route verification to help map the interconnections between networks. The two primary tools are traceroute and ping with routerecord. The results are parsed by the Ruby scripts into the ANTFARM database. This task can be performed by any of the security analysts on the team.

3.2.1.2. Generation

This sub-task tree is identical to that of the control center.

3.2.1.3. Create network maps

Once the assessors have collected network traffic pattern information, they can create network maps. These will serve two purposes – first, as part of discovery of all access points to the ESPs and, second, to help understand the ESPs and network segments for comparison to the physical security perimeter. This task can be performed by any of the security analysts on the team.

3.2.1.4. Determine Network Separation

This task depends upon the network maps to determine what separation points exist within and external to the various Electronic Security Perimeters. Since this involves analysis of the maps and possible drill-down into any underlying database and inputs to that database, it would best be performed by experienced network analysts.

3.2.1.5. Determine Network Zones

This task will involve assignment of the network segments into separate zones for cyber-physical analysis. This task would best be performed by experienced analysts.

3.2.1.6. Determine Network Detection

This task involves determining the network detection and protections at the points where different network zones meet. Although the electronic access controls of CIP-005 are part of this information, there may also be access controls between zones internal to the ESP. This would best be performed by experienced analysts.

3.2.2. Physical Mapping

CIP-005 does not require a physical security vulnerability assessment nor does CIP-006. However, CIP-006 does require that all cyber assets used in the access control and monitoring of the Physical Security Perimeter be afforded the protective measures specified in CIP-005. Therefore, a CIP-005 cyber vulnerability assessment involves determining what cyber assets are used for physical security. Physical security involves three tasks – Detecting the adversary, Delaying the adversary, and Responding to the Adversary before they achieve their goal. Sandia's physical security personnel have shortened this to the mantra, Detect – Delay – Respond.

3.2.2.1. Control Center

3.2.2.1.1. Determine Physical Security Zones

This task involves mapping the physical security zones that make up the physical security perimeter. An assessor with physical security experience should perform this work. Once the physical security zones are determined, the analysts can move on to determining access control and intrusion detection for the zones.

3.2.2.1.2. Determine Zone Access Control

This task requires the physical security analyst to discover access control mechanisms (the Delay part of Detect – Delay – Respond) for each of the physical security zones. An experienced physical security analyst should perform this work.

3.2.2.1.3. Determine Zone Intrusion Sensors

This task requires the physical security analyst to discover zone intrusion sensors (the Detect function of Detect – Delay – Respond) for each of the physical security zones.

3.2.2.1.4. Verify Physical Location of Cyber Assets

This task requires a security analyst (physical or cyber) to verify the physical location of cyber assets – to determine the physical security zone in which each cyber asset resides. This can and will include walking around physical security zones and confirming the location of specific cyber assets, tracing network cables to ensure they are run inside the physical perimeter and similar activities.

3.2.2.2. Generation

This sub-task tree is identical to that for the control center.

3.2.3. Correlating Electronic to Physical

The assessors will need to create zone maps of both the electronic and physical security zones, including the locations of critical cyber assets in the physical security zone map. Zones are separated by the access control and detection mechanisms at each access point. That information, summarized, should be included in the zone maps.

3.2.4. Analyzing Exposures

The assessors should determine the most vulnerable paths through the physical and electronic security zones to understand exposures. The analysis should allow the possibility that an adversary might switch back and forth between zones to gain access.

3.2.5. Generate Report

This task will assemble the information about electronic security perimeter assessment into a single report for deliver to the Utility. This will be performed by Sandia.