SANDIA REPORT
SAND2007-7328
Unlimited Release
November 2007

Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment

Raymond C. Parks

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone:	(800)553-6847
Facsimile:	(703)605-6900
E-Mail:	orders@ntis.fedworld.gov
Online order:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-7328
Unlimited Release
Printed November 2007

Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment

Raymond C. Parks
Assurance Technology and Assessments Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0671

Abstract

This document describes a customized process for cyber vulnerability assessment in compliance with the Critical Infrastructure Protection standards adopted by the North American Electric Reliability Corporation in 2006. This guide covers the planning, execution, and reporting process.

Contents

Acronyms and Abbreviations

ACL	access control list
ANTFARM	(passive network mapping tool)
CC	control center
CIP	Critical Infrastructure Protection
DCS	distributed control system
DMZ	demilitarized zone
DOE	Department of Energy
DNS	domain name system
ESP	electronic security perimeter
ICCP	intercontrol center communications protocol
IPSec	internet protocol security
LDAP	lightweight directory access protocol
MIB	management information base
NERC	North American Electric Reliability Corporation
PDC	primary domain controller
PSP	physical security perimeter
SCADA	Supervisory Control and Data Acquisition
SNMP	simple network management protocol
VMS	virtual memory system
WBS	work breakdown structure

How to Use this Guide

Newcomers to cyber vulnerability assessment should read sections 1 and 2 to understand the basic concepts. Experienced assessors/auditors from the Information Technology sector should first review Section 2 before proceeding to Section 3. Experienced assessors/auditors of control systems should begin with Section 3 and the detailed task descriptions.

Executive Summary

The North American Electric Reliability Corporation (NERC) adopted Critical Infrastructure Protection (CIP) standards in 2006. The standards establish the minimum requirements needed to ensure the security of electronic information exchange to support the reliability of the bulk power system. Industry feedback at conferences and meetings indicate uncertainty about implementation of the standards. The Sandia National Laboratories Center for Control System Security undertook a work package for the Department of Energy (DOE)'s Office of Electricity Delivery and Energy Reliability under the National Supervisory Control and Data Acquisition (SCADA) Test Bed program. This work developed guidance for conducting assessments required by the new standards. Sandia built on experience performing more than 100 critical infrastructure assessments to develop a project plan for a CIP cyber vulnerability assessment of an actual utility. We 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 should consider the guidance in this document.

1 Introduction

In 2006, the North American Electric Reliability Corporation (NERC) adopted the Critical Infrastructure Protection (CIP) standards. The standards establish the minimum requirements to ensure the security of electronic information exchange to support the reliability of the bulk power system. Industry feedback at conferences and meetings before and after that release 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 (ESP). These are two different but related cyber vulnerability assessments required as per CIP-007 (critical cyber assets) and per CIP-005 (ESP).

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 parent document refers to other resources, including a planning spreadsheet and a sample project plan. These resources are not necessary but very helpful in understanding the content of this guide. These resources or suitable substitutes are necessary to carry out the process in this guide. The other resources should be found co-located with this guide.

1.2.1 Resources

The useful resources associated with this include—

- Planning spreadsheet.
- Microsoft Project template plan.

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. Task descriptions help with planning and performance by using the planning spreadsheet and/or the Microsoft Project plan.

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 to 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, about 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 and 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.

Initially, the CIP requirements that drive this process must be understood.

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, ESP requirements include—

> 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, requirements include—

> 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 ESP and the physical security perimeter (PSP) 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 to determine 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 require retention of electronic access logs for 90 days. These logs can be used in conjunction with analysis of firewall rules and router access control lists (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 meeting 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 it has committed 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).

Steps in the assessment process include—

1. Planning for the assessment.
2. Conducting the assessment.
3. Reporting the results.
4. Planning mitigation once the report is accepted.

2.2.1 Planning Overview

A CIP cyber assessment must be completed according to the prescribed steps. The assessment team must plan the assessment in close collaboration with the operations and engineering personnel at the responsible entity. Careful, collaborative planning is essential.

The assessment activity will require more resources than just the assessment team. System and network administration personnel must 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 should be scheduled for 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 for the operations and engineering personnel who must work with the assessment.

The assessment team will need to consider the following questions regarding 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 these questions must be answered to plan the assessment.

2.2.2 Planning Process

Initially, the planning process will determine scope. Next, the planning process will determine performance requirements, estimate resources and travel costs, develop the project plan and rules of engagement, and identify team members.

2.2.2.1 Understanding Roles and Responsibilities

Although team identification is the last step in the planning process, understanding 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. (See Section 2.2.2.7 for further details on team identification.)

2.2.2.2 Determining Scope

As stated above, the first planning step is to determine the assessment scope. The team leader will work with the assessment customer to identify systems and facilities to be assessed. The assessment team may be asked to perform a complete CIP cyber vulnerability assessment of all critical cyber assets; or the assessment could be distributed among multiple assessment teams. The complete set of critical cyber assets will include control centers, generation plants, substations, and remote access points, such as power broker offices.

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 ESP will affect the scope as well; larger enclaves imply more complex internal network infrastructure requiring more assessment. The number of ESPs and communication paths between them are important to determining the scope.

2.2.2.3 Planning Performance Requirements

The second planning step is to determine the performance requirements. The number of ESPs and communication paths between them are important to determining performance requirements. Another factor is the number and physical dispersal of locations of critical cyber assets.

2.2.2.4 Estimating Resources

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

2.2.2.5 Estimating Travel Costs

Travel is a given 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.

2.2.2.6 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 necessary actions of all the participants in a schedule is necessary for the safe execution of the assessment.

2.2.2.7 Determining Rules of Engagement

Cyber security assessments can be limited to paper exercises, but the CIP cyber vulnerability assessment inherently involves active engagement. The assessors must either access or watch others access critical cyber assets within the responsible entity's control systems. The assessment team leader must work with his/her counterpart in the responsible entity to develop rules for 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 which systems of the responsible entity, and who may perform those activities.

The rules of engagement cover decisions on whether activities take place within the primary active control system, a secondary control system, or an off-line test system. 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 must be compared to the active systems to ensure that they are identical in operation.

The assessment team and the responsible entity must 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.

2.2.2.8 Team Identification

The last step in the planning process is team identification. The assessment team leader should have all the knowledge necessary to pick the best people for the team. (Also see section 2.2.2.1.) The scope, performance objectives, resource requirements, travel, project plan, and rules of engagement should all inform the decision of whom 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.

Team Members and Responsibilities

Team Leader—The first role to be filled, the leader will do the following:

- Perform or supervise all assessment planning.
- Lead the team during the assessment.
- Manage any changes necessary during assessment.
- Ensure that the results are reported.
- Ensure that the responsible entity gets all needed support during mitigation planning.

The team leader must have both managerial skills and technical skills. In some cases, the assessment organization may need to split the team leader role into two parts: project management and technical management.

Team Members—There will be one or more. They will do the following:

- Perform the technical assessment tasks.
- Report their results.
- Support mitigation planning if called upon to do so.

Team members are assigned during team identification unless the team leader needs specialized expertise during planning.

Report writer—There will be one or more. The report writer can also play another role in the assessment team, such as team leader or member. The report writer(s) will do the following:

- Collect and edit team contributions to the report.
- Produce the assessment report.

2.2.2.9 Planning Tools

We have provided two tools to help planning (not including sections 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 both in planning an assessment.

Assessment Planning Spreadsheet. The spreadsheet follows the task structure and descriptions noted in Section 3. Each row of the spreadsheet corresponds to a task in the Work Breakdown Structure (WBS) in Section 3. Column headings include—

- WBS number.
- Assessment (CIP-007 or CIP-005) that the task addresses.
- Work location for a given task.
- Task name.
- Estimated number of person-hours to accomplish the task.
- Estimated elapsed time to accomplish the task.
- Number of instances of the work described in the task.
- Task assignment/Human resource (who can do the task).
- Task dependencies.
- Required utility assets.
- Calculated estimate of total person-hours.

Several ideas in the spreadsheet need explanation. First, the spreadsheet does not include all of the WBS subtask levels; there are subtask levels 1.1.1 through 1.1.9 but no rows for task levels 1.1 or 1.

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: 1) actual hands-on person-hours and 2) 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, person-hour time is short, but the elapsed time can be long.

The Task assignment/Human resource column was an early attempt to show the skill set required. The assessment on which this spreadsheet is based included resources from Sandia National Laboratories such 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 spreadsheet user must understand the technical skills of their personnel resources in order to plan.

The dependencies column shows how tasks depend upon other tasks being 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 choose to provide credentials for that level of access to the assessor; however, we recommend that the responsible entity reserve access to their own personnel.

Table 2.1 describes each resource that the responsible entity must provide.

Table 2.1 Responsible Entity Required Resources

Requirements Name	Description
CC Local Admin	Local administrator on a particular host or host(s) within the control center(s)
CC Test Network	Test network separate from the operational control center network with systems that duplicate operational systems
CC Network Admin	Network administrator on the control center network. Examples: 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	Network administrator on the control center network. Examples: Domain administrator in a Microsoft network or…
Gen Test Network	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

CC—control center; Admin—administrator; Gen—general; Eqpmt—equipment.

Assessment Planning Project Plan. This tool is a Microsoft Project file that captures the tasks in the spreadsheet. Some dependencies have been included, and there are placeholders for some resources. Users must 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 means carrying out the assessment plan. As in warfare, no plan survives contact with the enemy. Therefore, our plan will not survive intact once the actual assessment begins. Unexpected events will occur, such as last minute changes in personnel, personnel availability, and times of access to various locations. These unexpected events 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 leader should try to maintain task integrity within the plan to ensure no conflict with the operations of the responsible entity. Tasks may be rescheduled, but they should not be further subdivided such that the active engagement period becomes longer or more fragmented.

Although tasks are distinct within the project, the assessment team leader needs to ensure tasks are conducted, not by project order, but in the order that is most logical 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, these services do not have to take place at the same time. Instead, internal and external activities can be done separately while checking regularly to ensure the platform has not changed.

2.4 Reporting the Results

The assessor’s key goal in reporting the results is to provide actionable information. The responsible entity has the requirement within CIP standards to present a document that contains the following:

- Description of the vulnerability assessment process.
- Documentation of the assessment results.
- Action plan to remediate or mitigate vulnerabilities.
- Execution status of that action plan.

All but the last item are 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 the description must include enough specific technical information so 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 must contain sufficient information to assure auditors that the assessment process fulfills CIP requirements.

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

Specific information collected with the tools, methods, and techniques needs to be recorded with those tools in the vulnerability report section of the assessment report. One unfortunate reality of security assessment is that the tool used today may not be available tomorrow. In such a case, a later assessor may not be able to determine—by using the same tool—whether a vulnerability still exists. However, the assessor can find an equivalent tool based on the report of the vulnerability and a description of the past tool.

The existence of a vulnerable service or outdated user login on a critical cyber asset does not constitute a vulnerability. The assessment report must show how a credible adversary can or cannot exploit that service or login as a vulnerability. This is particularly true in CIP cyber vulnerability assessments with 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 PSP 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 ESP. In both examples, the responsible entity can take action by choosing from a number of mitigation strategies and by ensuring mission performance.

2.5 Planning the Mitigation

There is no point to any assessment—and particularly a 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 because they may lose perspective and objectivity. However, assessors can make general recommendations. The assessors should also be available to the mitigation planning team as an information resource and critical feedback source.

3 Detailed Task 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.
- Any third-parties.

Technology resources include—

- Tools and techniques that are the industry standard.
- 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 ESP, including—

- A document identifying the vulnerability assessment process (e.g., 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.
- Documentation of the results.
- Mitigation plan and mitigation status.

Assumptions

Certain assumptions had to be made to develop the plan for this assessment:

- 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 time for 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

Technically, this task is simple, but logistically, it can be more complex. 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 back-up 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 to 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 exists for reasons other than the vulnerability assessment. Another issue with performing external scans is that some platforms may use a host-based firewall or communicate with other platforms solely through IPSec. In either case, the scan must be performed both with the security mechanism turned on and with the security mechanism turned off.

3.1.1.3 Application Platform Account Check

This task would be combined with the 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. The assessment team would then confirm the work through spot checks.

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

Some servers provide infrastructure upon which the critical control systems depend and 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 team member.

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. Technically, this is slightly more complex than a standard platform scan, but not complex 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 the task described below in Section 3.2.1.1 (Collect Network Configurations); therefore, these tasks could 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 the task described above in Section 3.1.1.7), install those configurations in identical equipment in an off-site test network, and conduct the scans.

If this can be performed 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 through configuration information gathered in the task described above in Section 3.1.1.7.

3.1.2 Generation

This section of tasks refers to assessment performed in a separate ESP associated with a power generation plant.

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 leader 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

Technically, this task is simple, but logistically, it is very complex. 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 exists for reasons other than the vulnerability assessment.

3.1.2.3 Application Platform Account Check

This task would be combined with the 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

Some servers provide infrastructure upon which the critical generation systems depend and 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. Technically, this is slightly more complex than a standard platform scan, and like that task, it will require the flexibility and expertise 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 the task described below in Section 3.2.1.1 (Collect Network Configurations), so these could be combined. This task would best be performed with responsible entity supervision if not done solely by responsible entity analysts because 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 the task described above in Section 3.1.3.2), 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 through configuration information gathered in the task described in Section 3.1.3.2.

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 wardialing or it might be network scanning. Again, because of the uncertainty, experienced security analysts should perform this task with the 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 delivered 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 ESP. This should include—

- A document identifying the vulnerability assessment process (e.g., this document).
- A review to verify that only ports and services required for ESP operations are enabled.
- Discovery of all access points to the ESP.
- A review of controls for accounts, passwords, and community strings.
- 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 because they will not be networks.

3.2.1 Electronic Mapping

3.2.1.1 Control Center

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 (a passive network mapping tool). Assessors should keep in mind that network hardware configuration information can vary, even from the same vendor and model. Firewall rule sets and router ACLs are an implementation of a policy for authorized data flows crossing the ESP. This task will help fulfill requirements R4.2, R4.3, and R4.4. Any of the security analysts on the team can perform this task with the cooperation of the relevant network administrators.

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. Collecting network traffic patterns provides a picture of all data flows at the collection points.

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 depict, in part, 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.

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 security analyst on the team.

3.2.1.2 Generation

This subtask 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: 1) discovery of all access points to the ESPs; and 2) to help understand the ESPs and network segments for comparison to the PSP. 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 ESPs. Since this involves analysis of the maps—and possible drilldown into any underlying database and inputs to that database—it should 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 should be performed by experienced analysts.

3.2.1.6 Determine Network Direction

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 should 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 PSP monitoring 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

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

Determine Zone Access Control. This task requires the physical security analyst to discover access control mechanisms (the *Delay* function of Detect—Delay—Respond) for each of the physical security zones. An experienced physical security analyst should perform this work.

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.

Verify Physical Location of Cyber Assets. This task requires a security analyst (physical or cyber) to verify the physical location of cyber assets, i.e., 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 and outlets to ensure they are run or located inside the physical perimeter, and similar activities.

3.2.2.2 Generation

This subtask 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. Each ESP must be within a PSP, but there may be non-critical cyber assets within the ESP and PSP. 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 ESP assessment into a single report for delivery to the utility. This will be performed by the assessor.

Distribution

1		Mr. Hank Kenchington US Dept of Energy OE-10 1000 Independence Ave SW Washington, DC 20585
1	MS 0671	Raymond C. Parks, Org. 05627
1	MS 0899	Technical Library, Org. 09536

Sandia National Laboratories