CAISO Information Security Requirements for the Energy Communication Network (ECN)

REVISION HISTORY

VERSION	DATE	DESCRIPTION
DRAFT 0.1	11/27/2002	Initial Draft
1.0	10/13/2003	Initially Released Version
1.1	11/15/2005	Minor clean-up.
1.2	05/30/2006	New logo and appendix change
-	08/28/2008	Reviewed, no changes needed
-	09/04/2009	Annual Review, no changes needed
1.3	04/28/2011	Updated hyperlink to CPNI.
2.0	03/12/2013	Removed table 1. Modified acceptable use section to not regarding communication activities on the ECN. Removed old reference to CUDA in favor of Public Key Infrastructure (PKI).

COPYRIGHT © 2003-4 by California ISO. All Rights Reserved.

TABLE OF CONTENTS

1. INTRODUCTION

This document is in support of the California ISO (CAISO) stated Information Security to safeguard the reliable delivery of electricity, to facilitate markets, and to ensure equal access to a 25,526 circuit mile “electron highway.” Security is paramount in order to maintain the reliability of the California and neighboring states power grids and to settle the California electricity markets.

This document outlines the Information Security policy, standards, and guidelines for CAISO Connected Subscribers (CS) who utilizes the dedicated shared, high-reliability, and high-bandwidth communications network established by the CAISO called the Energy Communications Network (ECN) for CS to CAISO connectivity as well as CS to CS connectivity.

This document complies with the NERC Security Standards. Also note, if you are a WECC member, you may also be subject to comply with the WECC WON Policy.

1.1. TERMINOLOGY AND CONCEPTS

Logical Security – Describes the characteristics of access control devices that protect systems and data from unauthorized access.

Physical Security – Describes the physical environment in which access control to systems and data is defined.

2. POLICY

Information is a critical and valuable asset for the CAISO where strict confidentiality must be maintained. Protecting information assets from unauthorized, incorrect or accidental access, use, modification, destruction or disclosure is every employee and user’s responsibility and obligation. ECN access connectivity must be designed, developed, built, configured and maintained in such a way that only authorized users have access to all information and every tool permitted to do their job and nothing else.

The CAISO Information Security department is responsible for developing, implementing, and maintaining the CAISO ECN Access Policy and the related Procedures. The Information Security department is also responsible for developing ECN access security requirements and specifications.

Compliance with this Policy is mandatory. Non-compliance or a violation of this Policy is a serious offense and may result in the user’s revocation of ECN access service.

3. STANDARDS

3.1. APPROVED USE

Authorized Users of the ECN may use the ECN to communicate to the CAISO and to other CS's on the ECN as agreed upon by and between each CS. All CS's should consider the ECN as an untrusted network and should take appropriate steps to protect themselves (least privileged access, use of antivirus, only use known ports and services, etc.).

3.2. TECHNOLOGIES

3.2.1. Firewalls

Firewalls may be required according to the requirements detailed in Section 4 and Appendix A. Please refer to these sections for further information.

For configurations that require firewalls to be installed, best practices recommend you select one of the certified firewall products found at:

https://www.icsalabs.com/icsa/product.php?tid=fghhf456fgh

Best practices for deploying firewalls can be found at:

http://www.cpni.gov.uk/Documents/Publications/2005/2005007_TN1004_Understanding_firewalls.pdf

3.2.2. Routers

The perimeter router connecting the CS to the ECN shall be configured to restrict both ingress and egress traffic using Access Control Lists (ACLs). Ingress ACLs shall be designed to only allow trusted hosts and protocols. Egress ACLs shall be designed to only allow only traffic from assigned local IP addresses. Each CS is responsible for providing business justification for each of the protocols allowed to traverse their perimeter router.

The ECN was established and designed to safeguard the reliable delivery of electricity, to facilitate markets, and to ensure equal access to a 25,526 circuit mile "electron highway." Due to the risk of reliability associated with "router peering", peering between the local CS router and the ECN core routers is strictly prohibited, unless the local CS router is managed by the ECN communications provider.

4. CONNECTION CONSTRUCTS

4.1. INTER-CONTROL CENTER COMMUNICATIONS PROTOCOL (ICCP)

The Inter-Control Center Communications Protocol (ICCP – IEC60870-6 TASE.2), also known as TASE.2, was developed to allow two or more utilities to exchange real-time data, schedule, and control commands. When ICCP was developed, communication security was not given a high priority in the design of the protocol, thus making it inherently insecure. With the increase of interconnecting systems brought on by deregulation and the Internet revolution, ICCP faces more threats today then ever before. Additional information on ICCP security can be found at www.epri.com.

To increase reliability and reduce the risk associated with ICCP traffic, all ICCP communications will be established over the ECN. Logical separation between CS's SCADA ICCP devices and the ECN will be provided by a firewall. CSs' SCADA ICCP devices shall have logical (provided by firewall) or physical separation from RIGs', DPGs', revenue meters, Scheduling Coordinators, and a CS's LAN/WAN. The gateway for SCADA ICCP traffic must be a physically separate device than the gateway that supports CS's LAN/WAN communications. All SCADA ICCP communication equipment shall be in a physically secured area. All CS's are required to sign the CAISO Connectivity Security Requirements document.

In addition to these requirements, if you are a member of the WECC and connect to the WON (WECC Operations Network), you must comply with the WECC Operations Network (WON) Security Policy For Official Use By WECC Members document located at www.wecc.biz.

See Appendix A for an illustration of the required logical separation. Physical separation can be achieved by strategically removing the depicted links.

4.2. REMOTE INTELLIGENT GATEWAY (RIG)

The Remote Intelligent Gateway (RIG) is a system for collection and transmission of data between Generators' sites and other monitoring and supervisory control sites. RIGs are generally installed at generation facilities that participate in Automatic Generation Control (AGC). RIGs provide the ability, in real-time, to collect data and distribute supervisory control commands to and from generation and transmission/distribution sites, and transfer this data to and from multiple central monitoring and supervisory control sites. This exchange of data is performed using local interface units, or RIGs. To ensure secure communications, all RIG devices rely on the CAISO Public Key Infrastructure (PKI) to provide strong authentication and encrypted communications. To find out more about the RIG and PKI program, please refer to the documentation located at http://www.caiso.com/pubinfo/info-security/index.html for further details.

To increase reliability and reduce the risk associated with RIG traffic, all RIG communications will be accomplished over the ECN. RIG devices have the option to connect directly to the ECN or logically via the CS's router. RIG devices shall have logical or physical separation from DPGs', revenue meters, Scheduling Coordinators, and a CS's LAN/WAN. Logical separation can be achieved using a firewall or a set of router ACL's as described in Appendix A. The gateway for RIG traffic must be a physically separate device than the gateway that supports CS's LAN/WAN communications. All RIGs' and RIG communication equipment shall be in a physically secured area. All CS's are required to sign the CAISO Connectivity Security

COPYRIGHT © 2003-4 by California ISO. All Rights Reserved.

Requirements document, located at http://www.caiso.com/pubinfo/info-security/index.html for further details.

See Appendix A for an illustration of the required logical separation. Physical separation can be achieved by strategically removing the depicted links.

4.3. DATA PROCESS GATEWAY (DPG)

In accordance with the requirements of the CAISO Tariff, the CA ISO initiated a project for the establishment of a direct monitoring and communication's system for Non-AGC Generating Units and Participating Loads. The technology that the CAISO Direct Telemetry Working Group selected for meeting these requirements and standards is generically referred to as a Data Processing Gateway (DPG) unit. To ensure secure communications, all DPG devices rely on the CAISO PKI to provide strong authentication and encrypted communications. To find out more about the DPG and PKI program go to http://www.caiso.com/pubinfo/info-security/index.html for further details.

DPGs' have the option to transmit data to the CAISO over the Internet or the ECN. In this document we are only addressing ECN connectivity. The ECN provides increased reliability and reduces risk compared to the Internet option. DPG devices shall have logical (e.g. firewall) or physical separation from SCADA ICCP devices. DPGs' shall also have logical (e.g. firewall or router ACL's) or physical separation from RIGs', Revenue Meters, Schedule Coordinators, and CS's LAN/WAN. The gateway for DPG traffic must be a physically separate device from the gateway that supports CS's LAN/WAN communications. All DPGs' and DPG communication equipment shall be in a physically secured area. All CS's are required to sign the CAISO Connectivity Security Requirements document, which can be located at http://www.caiso.com/pubinfo/info-security/index.html.

See Appendix A for an illustration of the required logical separation. Physical separation can be achieved by strategically removing the depicted links.

4.4. METERING

For market settlement purposes, an accurate method is needed to determine the amount of energy being delivered into and out of the transmission grid. This will involve the use of revenue quality metering at all generating units, tie points, or any locations that are electrically connected to the transmission grid under CAISO jurisdiction. The CAISO is responsible for establishing and maintaining the revenue meter data acquisition and processing system (MDAS). MDAS will acquire revenue quality meter data for use in the CAISO's settlement and billing process.

To increase reliability and reduce the risk associated with MDAS traffic, all MDAS communications will be accomplished over the ECN. MDAS devices shall have logical (e.g. firewall) or physical separation from SCADA ICCP devices. MDAS devices shall also have logical (e.g. firewall or router ACL's) or physical separation from RIGs', Scheduling Coordinators, and a CS's LAN/WAN.

The gateway for MDAS traffic must be a physically separated device from the gateway that supports CS's LAN/WAN communications. All MDAS and MDAS communication equipment shall be in a physically secured area. All CS's are required to sign the CAISO Connectivity Security Requirements document, which is located at http://www.caiso.com/pubinfo/info-security/index.html.

See Appendix A for an illustration of the required logical separation. Physical separation can be achieved by strategically removing the depicted links.

4.5. SCHEDULING COORDINATORS (SC)

Scheduling Coordinators (SC) is certified to submit energy schedules and bids directly to the CAISO. The CAISO settles directly with the Scheduling Coordinators for market transactions such as supplemental energy, ancillary services, congestion, wheeling, imbalance energy and unaccounted-for energy.

Some of the CAISO applications require SC's to submit transactions via the Internet while other applications require them to submit transactions via the ECN. In this document we are only addressing ECN connectivity.

SC's connected to the ECN to submit transactions shall have logical (e.g. firewall) or physical separation from SCADA ICCP devices. SC devices shall also have logical (e.g. firewall or router ACL's) or physical separation from RIGs', DPGs', and Revenue Meters. The gateway for SC's traffic must be a physically separated device than the gateway that supports SCADA ICCP, RIGs', DPGs', and Revenue Meters. All CS's are required to sign the CAISO Connectivity Security Requirements document, which can be located at http://www.caiso.com/pubinfo/info-security/index.html.

See Appendix A for an illustration of the required logical separation. Physical separation can be achieved by strategically removing the depicted links.

5. AUTHENTICATION

Each of the Connection Constructs listed in Section 4 must enforce authentication. Implementation of the following passwords standards is subject to the restrictions of the operating systems or security software. The intent of these standards is to maximize ease-of-use without sacrificing security for any portion of the computing infrastructure and communications environment. Password minimum-security requirements include:

- Passwords must be a minimum of eight characters in length.
- Passwords must be alphanumeric.
- Passwords must have at least two numeric characters.
- Passwords must not contain the user ID, logon ID or their reverse.
- Passwords may be initially assigned by an Administrator, but must be changed at initial logon by the user. The user changes the password thereafter to maintain security and access control.
- Passwords must be set to expire annually.

COPYRIGHT © 2003-4 by California ISO. All Rights Reserved.

- Passwords must not contain three or more consecutive occurrences of the same character (e.g., 222, or aaa).
- Password must not contain four or more characters in a sequential order (e.g., 1234, or abcd).
- Users must keep their password secret.
- Users must not share their password with anyone
- Default passwords must be changed when products are installed.

RIG, DPG, and some SCs' applications require the use of the CAISO PKI. See this specific application documentation for their authentication requirements, which is located at http://www.caiso.com/pubinfo/info-security/index.html.

6. VIRUS SCANNING

The use of virus scanning software is required where technically feasible.

7. ENCRYPTION

The RIG, DPG, and some SC's applications require encryption. These applications are required to comply with the CAISO PKI program. Information can be found at http://www.caiso.com/pubinfo/info-security/index.html.

8. BANNERS

All network devices (e.g., routers, firewalls, etc.) connected to the CAISO ECN must have the following CAISO approved login banner or equivalent installed.

CAISO approved login banner:

*** AUTHORIZED USERS ONLY ***

> This is a Private computer system. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.
>
> Any or all uses of this system and all files may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site and law enforcement personnel. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site.
>
> Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

*** AUTHORIZED USERS ONLY ***

9. PHYSICAL SECURITY

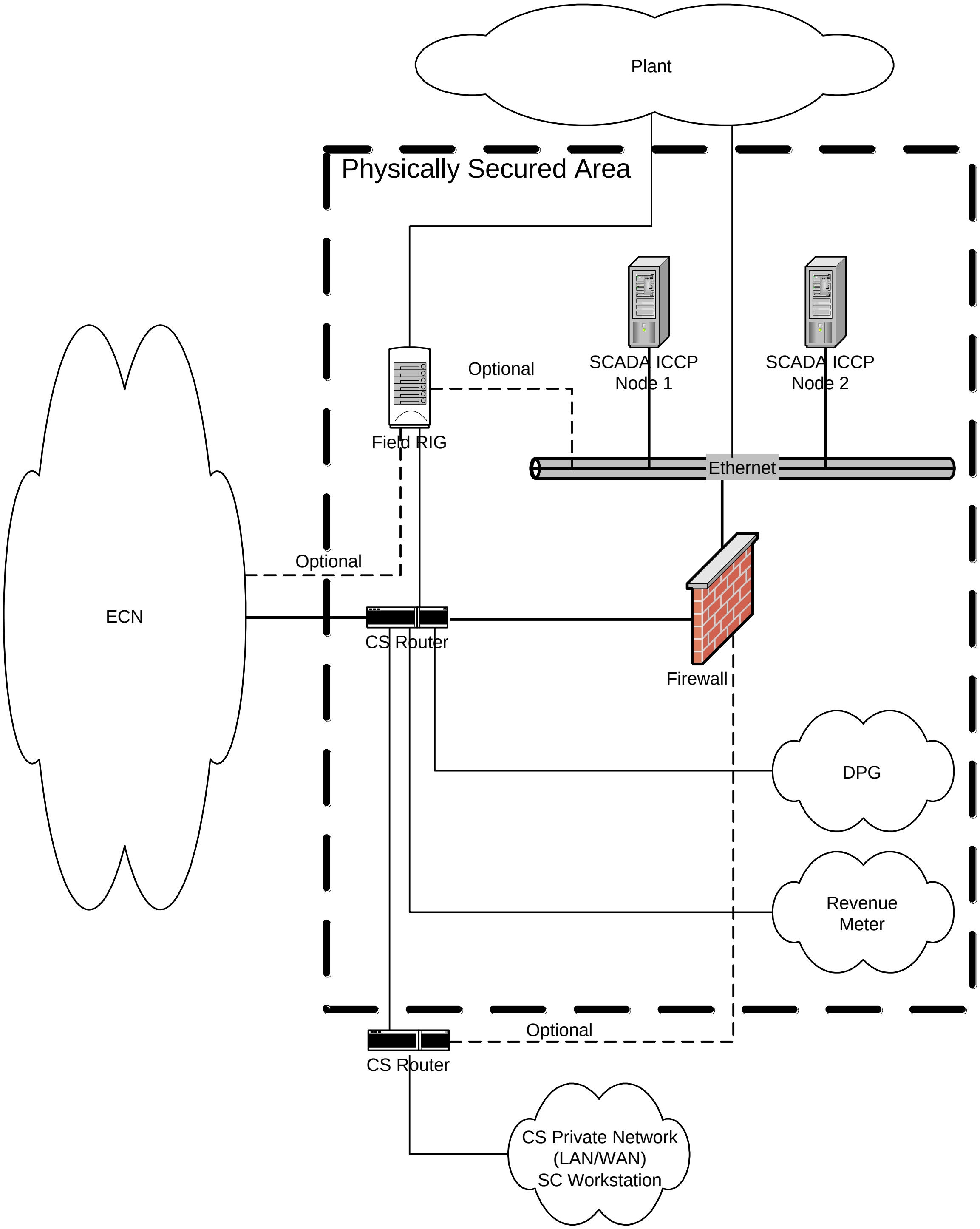
CAISO requires that computer and networking equipment associated with the ECN connections be physically secured from unauthorized access.

10. COMPLIANCE MONITORING AND NETWORK REVIEW

All CS's are required to sign the CE Connectivity Security Requirements and Agreement document. This document outlines compliance and review requirements. Please refer to the documentation located at http://www.caiso.com/pubinfo/info-security/index.html for further details.

COPYRIGHT © 2003-4 by California ISO. All Rights Reserved.

APPENDIX A


Plant
Physically Secured Area
Optional
SCADA ICCP Node 1
SCADA ICCP Node 2
Field RIG
Ethernet
Optional
ECN
CS Router
Firewall
DPG
Revenue Meter
Optional
CS Router
CS Private Network (LAN/WAN) SC Workstation