**External Network Guidelines**

**Version:** **1.0
9/4/2023**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 9/4/2023 | 1.0 | Initial Draft | R. Melis |

***Note: This technical bulletin is provided for the convenience of the market participant for the purpose of communicating complex and technical information. The technical bulletin is intended to be consistent with the ISO tariff, however, the ISO is bound to operate in accordance with the tariff in all cases. In the event there is any conflict between this technical bulletin and the ISO tariff, the ISO tariff will control. Any provision of the ISO tariff that may have been summarized or repeated in this technical bulletin is provided only to aid in the understanding of this technical bulletin and in no event shall any of the information in this technical bulletin be deemed an interpretation of the tariff, or in any way binding. While the ISO endeavors to update the information and analysis in this technical bulletin and to notify market participants of changes pertinent to this technical bulletin, it is the responsibility of each market participant to ensure that he or she is using the most recent version of this technical bulletin that it has not been retired or withdrawn, that the information in the technical bulletin is current, and to comply with all applicable provisions of the ISO’s tariff. The market participant use of this technical bulletin, and all information contained herein, is at its sole risk.***

**Table of Contents**

[Executive Summary 4](#_Toc146867107)

[Background and Business Need 4](#_Toc146867108)

[Legal and Tariff Requirements 5](#_Toc146867109)

# Executive Summary

The ISO manages the flow of electricity across the high-voltage, long-distance power lines for the grid serving 80 percent of California and a small part of Nevada. The nonprofit public benefit corporation keeps power moving to homes and communities. As the only independent grid operator in the western U.S., the ISO grants equal access to nearly 26,000 circuit miles of transmission lines and coordinates competing and diverse energy resources into the grid where it is distributed to consumers. It also operates a competitive wholesale power market designed to promote a broad range of resources at lower prices. Given the mission of the ISO, the security of its critical computer systems, software applications and confidential data is of the highest importance. This document provides technical guidance for ISO Market Participants, generation resource owners and operators, Reliability Coordination customers and others doing business with the ISO. The guidance in this document is based on industry best practices and respected cyber security frameworks.

# Background and Business Need

The ISO requires data from grid assets as well as from Market Participants (Scheduling Coordinators and others) in order to fullfil its mission to manage the reliability of its balancing areas as well as to manage the overall reliability of the bulk electric system in the western United States (the Western Interconnect). The exchange of data between the ISO and its customers takes place across the public Internet and the ISO’s Energy Communications Network (ECN), a virtual private network (VPN) open only to approved ISO customers.

The ISO considers both the Internet and the ECN as external networks, and those networks are therefore untrusted and potentially hostile. Therefore, the ISO takes a multilayered approach to protecting its cyber systems from potentially harmful connection attempts sourced from either the Internet or the ECN. The ISO recommends all of its customers to take the same approach to cyber security with regards to these external networks.

The ISO recommends each of its customers consider industry best practices and established frameworks when establishing cyber security protections. The International Organization for Standarization (ISO) 27001 information security management systems and the National Institute for Standards and Technology (NIST) Cyber Security Framework (CSF) are 2 well known frameworks to use as a reference.

The NIST CSF outlines five areas to consider when establishing a cyber security program:

1. **Identify**
	1. Identify the assets that need to be protected. This includes both physical and digital assets.
	2. Identify the threats and vulnerabilities that these assets are exposed to.
	3. Assess the risk to these assets.
2. **Protect**
	1. Implement appropriate security controls to mitigate the risks to your assets. This could include things like firewalls, intrusion detection systems, and encryption.
	2. Implement controls at the edge of your connections to external networks (Internet, ECN, etc.) using the principle of least privileged access. Allow only access inbound and outbound that is required by a business need, and deny all else. Limit inbound access from external networks to only known host Internet Protocol (IP) addresses or a limited number of networks. Limit inbound access from those IP addresses to only necessary transmission control protocol (TCP) or user datagram protocol (UDP) well known port numbers. Common supervisory control and data acquisition (SCADA) protocols used on the ECN include (but are not limited to) distributed network protocol version 3 (DNP3) for generation telemetry from remote terminal units (typically TCP 7700) and intercontrol center protocol (ICCP) for control center to control center communication (typically TCP 102).
	3. Implement a strong identity and access management (IAM) system to control who has access to your assets.
	4. Keep your security controls up to date (including applying security patches when made available by vendors).
3. **Detect**
	1. Implement monitoring and logging systems to detect suspicious activity.
	2. Have a process in place to investigate and respond to security incidents.
4. **Respond**
	1. Have a plan in place to respond to security incidents. This should include things like containment, eradication, and recovery.
	2. Communicate with affected parties during a security incident.
5. **Recover**
	1. Have a plan in place to recover from a security incident. This should include things like restoring data and systems.

Here are some additional considerations for securing a connection to an external network:

* Use strong passwords and multi-factor authentication.
* Keep your software up to date.
* Use encryption where possible to protect data integrity of traffic between your internal network and the external network.
* Segment your network to isolate different parts of your infrastructure.
* Implement a security awareness training program for your employees.

# Legal and Tariff Requirements

Each ISO customer who remotely connects to ISO systems and applications via an external network (Internet or ECN) is responsible for any network activity that originates from or passes through its facilities and terminates on ISO computer systems. If, in the course of conducting network problem diagnosis, cyber security incident management, or other administrative functions, the ISO or its customers discover evidence of possible malicious activity originating from its facilities, the party discovering such activity (the “Notifying Party”) will immediately notify the other party and provide information as to such evidence (to the extent the Notifying Party determines that providing such information does not increase the likelihood of further malicious activity). The other party may ask for the Notifying Party’s assistance in investigating the malicious activity and may request the Notifying Party to take additional precautionary measures if warranted. If this joint investigation reveals possible evidence of criminal activity, upon the written consent of the Notifying Party, that evidence will be provided to the appropriate law enforcement agency.

If, as a result of the joint investigation, a party claims that the malicious activity resulted from negligence on the part of the other party and if the claiming party wishes to pursue a remedy for any resulting damages, the parties will adhere to the dispute resolution procedures of Section 13 of the ISO Tariff in connection with such claim.

ISO Tariff Section 14, Force Majeure Indemnification and Limitations on Liability will apply to all ISO responsibilities stated herein.

ISO Tariff Section 22.8, Applicable Law and Form, and 22.9, Consistency with Federal Laws and Regulations, are incorporated herein by reference.

On behalf of the Entity listed below, I acknowledge receipt of this Guideline and agree to consider the Guideline in the implementation of the Entity’s network connection to the ISO ECN and the ISO’s Internet network presense and to comply with the Legal and Tariff Requirements described herein.

Print Name and Title Entity Name Email Address

Signature Date

Where Applicable:

Project Name Resource ID New Resource Interconnect/CAISO Project #