

 <b>California ISO</b> Shaping a Renewed Future	<b>Human Resources</b>	<b>Procedure No.</b>	N/A
		<b>Version No.</b>	<b>1.3</b>
		<b>Effective Date</b>	May 15, 2008
<b>PERSONNEL RISK ASSESSMENT POLICY</b>		<b>Distribution Restriction:</b> CAISO CONFIDENTIAL	

## REVISION HISTORY

VERSION NO.	DATE	DESCRIPTION
1.0	5/15/08	Initial draft
1.1	9/21/09	Review; minor clarifying edits
1.2	9/13/2010	Review; update to clarify access granted only after completion or validation of PRA as required by CIP 004-2 effective April, 2010.
1.3	10/31/11	Annual review; no changes required

### I. INTRODUCTION

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation designed to “ensure that the bulk electric system in North America is reliable, adequate and secure.” Designated by the Federal Energy Regulatory Commission (FERC) in 2006 as an Energy Reliability Organization, NERC has approved Cyber Security Standards (NERC CIP) to protect electric utility assets from cyber security attack. All bulk power system owners and operators are required to comply with approved NERC CIP Standards. NERC CIP Standard 004 requires Personnel Risk Assessments be conducted on all California ISO Personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.

### II. PURPOSE

This Personnel Risk Assessment Policy (“Policy”) is intended to support the California ISO’s mandatory compliance with NERC CIP-004, to further the California ISO’s interest in promoting and maintaining a safe and secure working environment for Personnel, and to provide meaningful actions to protect Critical Cyber Assets.

**CAISO CONFIDENTIAL**

For use by authorized CAISO personnel with a need-to-know.

Do not release or disclose outside the ISO.

Human Resources:

Page 1

	<b>Human Resources</b>	<b>Procedure No.</b>	<b>N/A</b>
		<b>Version No.</b>	<b>1.3</b>
		<b>Effective Date</b>	May 15, 2008
<b>PERSONNEL RISK ASSESSMENT POLICY</b>		<b>Distribution Restriction:</b> CAISO CONFIDENTIAL	

### III. DEFINITIONS

For purposes of this Policy:

(1) “Personnel Risk Assessment” may include identity verification, criminal background checks, credit checks, and reference checks as appropriate for the level of security access.

(2) “Criminal Background Check” means identifying any misdemeanor and felony convictions of applicants and existing personnel in every identified county of residence for a seven (7) year period.

(3) “Convicted” means any plea of guilty or nolo contendere or any finding of guilt.

(4) “Personnel” includes employees of the California ISO, as well as consultants, contractors, subcontractors, and service vendors and their employees.

(5) “Employment” includes employment as a California ISO employee, as well as services of consultants, contractors, and service vendors.

(6) “Applicants” include any person applying for regular employment who has received a conditional job offer, or persons engaged to provide service on the California ISO campus as a temporary or contract employee, or service vendor where logical or physical access will be granted as a condition of assignment.

(7) “Critical Assets” means facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.

(8) “Cyber Assets” means programmable electronic devices and communication networks including hardware, software, and data.

(9) “Critical Cyber Assets” means Cyber Assets essential to the reliable operation of Critical Assets.

(10) “Authorized Cyber Access” means any person that has been approved by management to have access to Critical Cyber Assets.

**CAISO CONFIDENTIAL**

Human Resources:

For use by authorized CAISO personnel with a need-to-know.

Page 2

Do not release or disclose outside the ISO.

 <b>California ISO</b> Shaping a Renewed Future	<b>Human Resources</b>	<b>Procedure No.</b>	<b>N/A</b>
		<b>Version No.</b>	<b>1.3</b>
		<b>Effective Date</b>	May 15, 2008
<b>PERSONNEL RISK ASSESSMENT POLICY</b>		<b>Distribution Restriction:</b> CAISO CONFIDENTIAL	

(11) “Authorized Unescorted Physical Access” means any person that has been approved by management to have unescorted physical access to Critical Assets and Critical Cyber Assets.

#### **IV. POLICY**

In accordance with this Policy, as well as federal, state and local laws, a Personnel Risk Assessment shall be conducted on all California ISO Personnel having or potentially having Authorized Cyber or Authorized Unescorted Physical Access to Critical Assets and Critical Cyber Assets. Authorization for access to Critical Assets or Critical Cyber Assets will not be granted prior to the completion or verification of a current Personnel Risk Assessment.

Each Personnel Risk Assessment conducted shall include, at a minimum, identity verification (e.g., Social Security Number verification in the U.S.) and a seven-year Criminal Background Check. The California ISO reserves the right to conduct more detailed reviews, as permitted by law, depending on the criticality of the position and as appropriate for the level of security access granted.

The California ISO shall update each Personnel Risk Assessment at least every seven years after the initial Personnel Risk Assessment or for cause for all Personnel having or with the potential to have Authorized Cyber or Authorized Unescorted Physical Access to Critical Cyber Assets. Personnel Risk Assessments necessary pursuant to the initial implementation of this policy shall be conducted by July 1, 2008.

The California ISO shall document the results of all Personnel Risk Assessments conducted.

#### **V. FAILURE TO CONSENT**

All Personnel or applicants subject to a Personnel Risk Assessment will be asked to provide the California ISO permission to conduct the Personnel Risk Assessment by signing an authorization form. Permission must be given any time a Personnel Risk Assessment is requested, except when conducted as part of an investigation into suspected wrongdoing. Refusal to sign the permission form, or submit to the Personnel Risk Assessment, may result in the following: revocation of an applicant’s conditional

 <b>California ISO</b> Shaping a Renewed Future	<b>Human Resources</b>	<b>Procedure No.</b>	<b>N/A</b>
		<b>Version No.</b>	<b>1.3</b>
		<b>Effective Date</b>	May 15, 2008
<b>PERSONNEL RISK ASSESSMENT POLICY</b>		<b>Distribution Restriction:</b> CAISO CONFIDENTIAL	

job offer; termination of assignment for a contract, temporary or vendor-supplied employee; reassignment to a position that does not require a Personnel Risk Assessment (if available); or termination of employment and/or contract.

## **VI. FELONY OR MISDEMEANOR CONVICTIONS**

In the event a felony or misdemeanor conviction is revealed or reported, the California ISO will review the conviction with the consideration of additional relevant information such as:

- Seriousness of the felony or misdemeanor conviction and disposition issued by the courts;
- Relevance of the conviction to the work and level of responsibility the individual holds within the California ISO;
- Compliance with laws governing the use of information acquired in a Criminal Background Check;
- The California ISO's policies and procedures;
- Consistency with the disclosure required on the authorization form; and
- Potential risk of non-compliance by NERC.

### **A. Withdrawal of Employment Offer**

Offers of employment or contract assignments are contingent upon successful completion of the Criminal Background Check. In the event a conviction is revealed and the Company intends to take adverse action, the applicant will be notified of the Company's intent to take adverse action and will be given one (1) week to provide appropriate evidence to refute the finding. In the event no evidence is provided, the California ISO will rescind the offer of employment.

### **B. Termination of Employment**

After considering all relevant information, the California ISO will make a determination on any resulting adverse disciplinary action, up to and including termination of employment. Prior to taking adverse disciplinary action, the California ISO will notify the employee of its intent to take adverse action. The employee will have a two (2) week opportunity to refute the finding by providing appropriate documentation. During that

**CAISO CONFIDENTIAL**

For use by authorized CAISO personnel with a need-to-know.

Do not release or disclose outside the ISO.

Human Resources:

Page 4

 <b>California ISO</b> Shaping a Renewed Future	<b>Human Resources</b>	<b>Procedure No.</b>	<b>N/A</b>
		<b>Version No.</b>	<b>1.3</b>
		<b>Effective Date</b>	May 15, 2008
<b>PERSONNEL RISK ASSESSMENT POLICY</b>		<b>Distribution Restriction:</b> CAISO CONFIDENTIAL	

period, the California ISO may place the employee on paid administrative leave, or suspend authorized Critical Cyber Asset access, at its discretion.

### **C. Discretion Not to Terminate Employment**

The California ISO, in the discretion of management, may choose not to terminate employment based on a misdemeanor or felony conviction. The California ISO may include, as a condition of continued employment, such actions as reassignment to another position, removal of certain privileges, such as driving a company vehicle, removal of access to certain Critical Cyber Assets, or other provisions deemed appropriate to be in compliance with the NERC CIP Standard.

### **D. Effect of Termination on Eligibility for Rehire**

Employees who are terminated as a violation of this Policy are not eligible for rehire until a seven (7) year period since the conviction has elapsed.

Any Personnel Risk Assessment conducted shall be maintained and/or disposed of in accordance with all applicable federal state and local laws.

## **VII. SELF REPORTING**

Personnel must notify the California ISO of any felony or misdemeanor conviction that occurs during the course of employment, assignment or engagement with the Company. Employees must notify the California ISO within five days after any such conviction. Disciplinary action will be considered pursuant to Section VI of this Policy.

Failure to self-report may be grounds for immediate termination of employment.

## **VIII. CONFIDENTIALITY**

All information disclosed to the California ISO in any Personnel Risk Assessment is and shall remain confidential, and under no circumstances shall such information be made available to anyone without a legitimate need-to-know.

Any record of information disclosed in any Personnel Risk Assessment shall be kept and maintained by the California ISO in a secure location physically separate and apart

**CAISO CONFIDENTIAL**

Human Resources:

For use by authorized CAISO personnel with a need-to-know.

Page 5

Do not release or disclose outside the ISO.

 <b>California ISO</b> Shaping a Renewed Future	<b>Human Resources</b>	<b>Procedure No.</b>	<b>N/A</b>
		<b>Version No.</b>	<b>1.3</b>
		<b>Effective Date</b>	May 15, 2008
<b>PERSONNEL RISK ASSESSMENT POLICY</b>		<b>Distribution Restriction:</b> CAISO CONFIDENTIAL	

from any application or personnel file, and shall be prominently marked "CONFIDENTIAL."

## DOCUMENT APPROVAL

### Responsible Manager:

Jodi Ziemathis, Manager, Human Resources Operations

x7023

Print Manager's Name and Title

Telephone

**CAISO CONFIDENTIAL**

Human Resources:

For use by authorized CAISO personnel with a need-to-know.

Page 6

Do not release or disclose outside the ISO.