

Reliability Compliance Tool (RCT) Training Webcast

August 25, 2016

Agenda

- Tool Overview
- Standard Self Certification Process Views
- EPP/RPA Self Certification Process Views
- Self Reporting Process Views
- Q&A

Reliability Compliance Tool Training

- **Objectives**

- The objective of this training is to provide participants the opportunity to become more familiar with the tool's look and functions in order to successfully perform self-certifications and self-reporting using the new Online IESO RCT.

- **Participation**

- The RCT is available to the following registered participant roles:
- Market Participant Compliance Contacts
- Market Participant Escalation Contacts
- Market Participant Emergency Preparedness and Restoration Contacts

RCT Overview

- The IESO has developed a new RCT application using Online IESO framework, which replaces the existing Reliability Compliance Tool (RCT)
- The new application integrates with existing IESO systems for user authentication and interacts with various other existing IESO databases.
- It delivers the same level of business services to facilitate reliability compliance self-certification and self-reporting for all market participants and IESO users.

RCT Implementation Milestones

Key Milestone	Date
Project Initiation	March 9
Market Trials Testing (MTT) Complete	June 24
Build Complete	July 15
End-to-End UAT Complete	July 22
Training Complete	August 25
Documentation Complete	September 14
Production Release	September 14

Ensuring Access to the RCT

- Log onto Online IESO : <https://online.ieso.ca/>
- Enter your user ID/password
- If you have forgotten your password:
 - Click on the forgot password link – you will be redirected to the portal
 - Enter your user ID and click continue

Sign In with User Account Name and Password

Enter your User Account Name.

User Account Name:

Continue

Forgot your password?

Enter your user ID (Account Name) and click the forgot password link on the next screen

Not a registered user?

Ask your Organization's Rights Administrator to register you in Online IESO

Ensuring Access to the RCT (con't)

- Recovering your password (con't)
 - Click on 'Forgot your password'
 - You will be prompted to answer security question(s)
 - Once answered, you can reset your password
 - Finally, close down your browser and log in again

Sign In:

Please type your password and then click on the "enter" button.



What's this?
Forgot your password?

Reset Your Password

Please enter your new password below and click "enter", then type it again and click "enter" to confirm your password. Choose a new password that is easy to remember and meets these password rules:

- Case sensitive (The "Caps Lock" key should be off)
- Eight characters or longer
- Contains all of the following three types:
 - upper-case
 - lower-case
 - special character [NOTE - Do not use the following special characters in your password: & (ampersand), \ (backslash), < (less than sign), > (greater than sign), ' (single quote), " (double quote).]
- Includes no spaces
- Please make sure the "Num Lock" key is off

New Password

click to type

Confirm New Password

click to type



Reliability Compliance Tool

- Here's what you can expect to see after typing the following and pressing enter

<https://online.ieso.ca/> ...

Welcome to Online IESO

The initial sign in screen:

The image shows a screenshot of the IESO online sign-in interface. At the top left is the IESO logo, which consists of a stylized globe icon followed by the text "ieso". Below the logo are two input fields: "Username" and "Password". Under the password field is a checkbox labeled "Remember me on this computer". To the left of the "Sign In" button is a link that says "Forgot Password". The "Sign In" button is green with white text. Below these elements is a "Legal Disclaimer" section, which contains a paragraph of text regarding system ownership, confidentiality, and user agreement. The entire sign-in form is set against a light blue background with a subtle grid pattern.



Username

Password

☒ Remember me on this computer

[Forgot Password](#) [Sign In](#)

Legal Disclaimer:
Attention to Participants: This system is owned and operated by the IESO, and all use of this system is governed by the Market Rules. As a registered Participant, you have received a unique and confidential User Account and Password from the IESO to access this system and you agree to maintain their confidentiality. You specifically agree that you are exclusively responsible for all access to and any activity on this system that occurs through the use of your User Account and Password. If you become aware of any unauthorized use of your User Account or Password, you agree to immediately notify the IESO. The IESO is not liable for any loss or damage arising from any unauthorized access or use of your User Account and Password. If you do not agree with these terms and conditions, immediately advise the IESO and do not login to this system.

Once Signed in ...

You will be taken to the News Tab View for Online IESO

News Tasks Records Reports Actions

Click here to post...

Manage Participation A participation service provider request has been created for TEST ORGANIZATION 1: Meter Data Associate #amp
May 17, 2016 ☆ Comment More Info ▾

Manage Participation A market participation request has been created for DR TEST ORGANIZATION: DRMP - Owner; DRMP - Operator; DRMP - RMP; DRMP - MMP #amp
Apr 7, 2016 ☆ Comment More Info ▾

IESO System The configuration instructions have been sent
Apr 7, 2016

IESO System The training information has been sent
Apr 7, 2016

Add your comment here...

Manage Participation A market participation request has been created for ENERCON: Load - Meter Market Participant; Load - Operator; Load - Owner; Load - Registered Market Participant #amp
Mar 18, 2016 ☆ Comment More Info ▾

IESO System The configuration instructions have been sent
Mar 18, 2016

IESO System Peter Primary confirmed connectivity to IESO Information System(s)
Mar 18, 2016

Add your comment here...

ieso
Search news

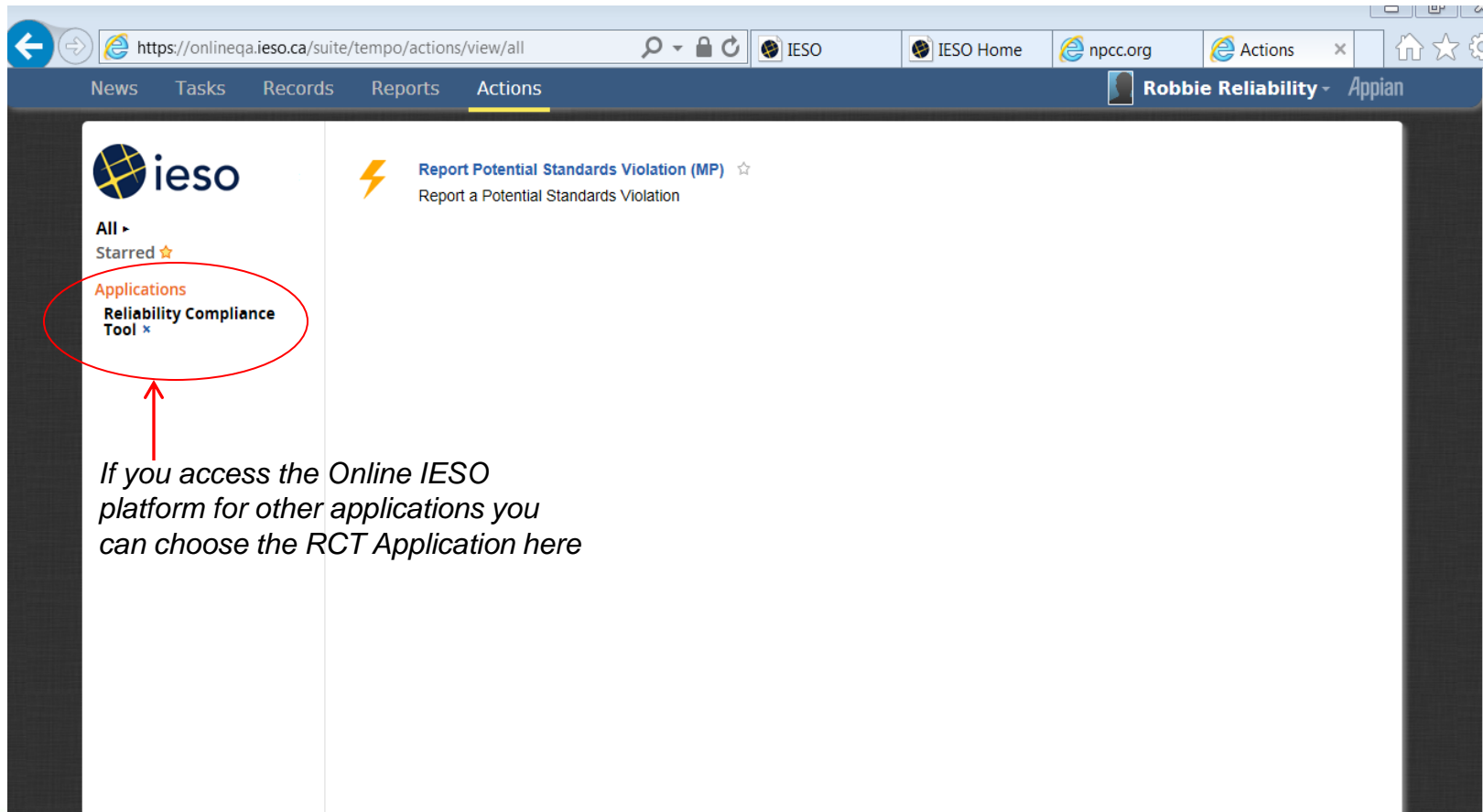
All ▶
Updates
Participating
Kudos
Starred

You will see your name in the top right hand corner

You can then navigate through the Online IESO tabs to perform your required work.

RCT Actions Tab

MPs will be able to see the Report Possible Standards Violation Action only in the Actions Tab



ieso

All ▾

Starred ★

Applications

Reliability Compliance Tool ✕

Report Potential Standards Violation (MP) ☆

Report a Potential Standards Violation

If you access the Online IESO platform for other applications you can choose the RCT Application here

RCT Tasks Tab

Self Certifications will appear as Tasks in the MP Task Folders and can only be initiated by the IESO

The screenshot displays the IESO Appian interface. The top navigation bar includes 'News', 'Tasks (1)', 'Records', 'Reports', and 'Actions'. The user profile 'Robbie Reliability' is shown in the top right. The left sidebar contains the IESO logo and filters: 'Assigned to Me' (with sub-filters 'Sent by Me' and 'Starred'), 'Status' (with 'Open'), and 'Deadline' (with 'Overdue Today' and 'Within 7 days'). The main content area shows a task card for 'Submit Self Certification | Cert: SC-2016-00309'. A red arrow points to the text 'Unique Identifier' below the task title.

RCT Records Tab

MPs will have a record of their submissions kept in the tool.
MPs will only be able to view their own records.

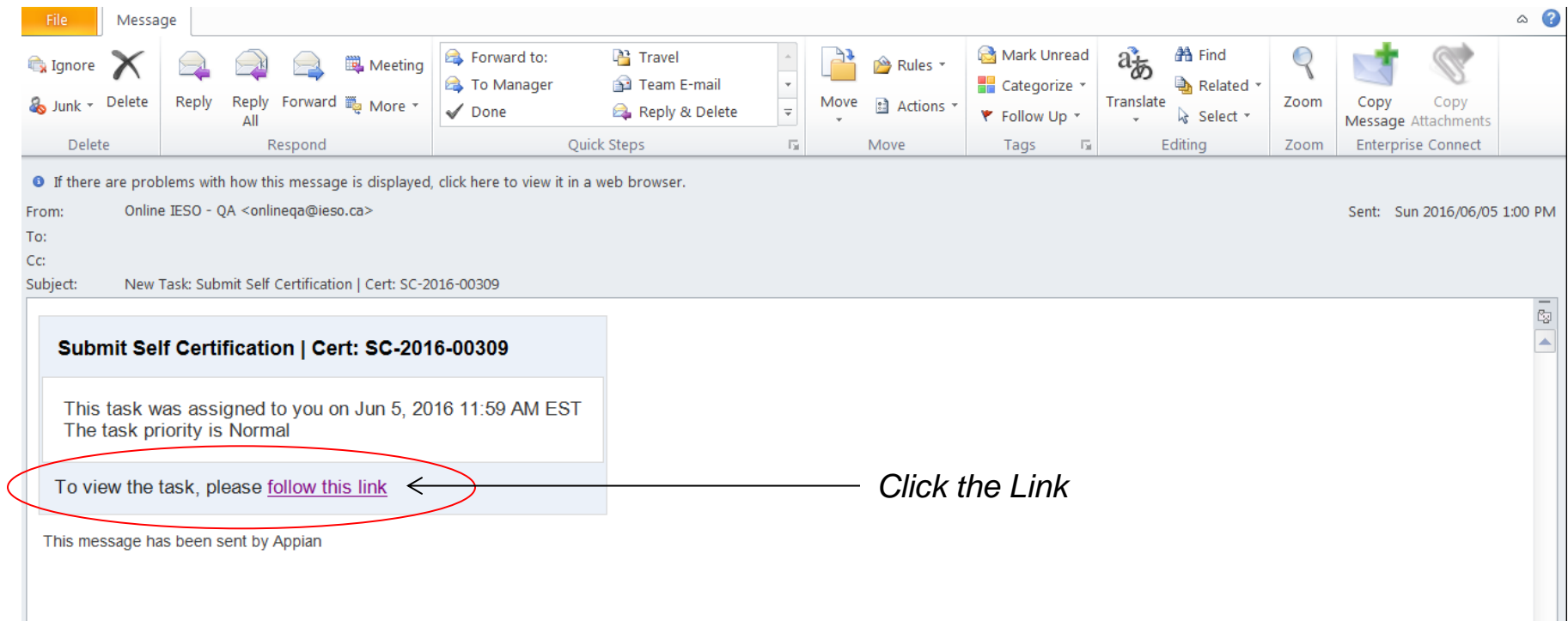
The screenshot displays the IESO RCT Records Tab interface. At the top, a navigation bar includes links for News, Tasks, Records (which is highlighted with a yellow underline), Reports, and Actions. On the right side of the navigation bar, there is a user profile icon and the text 'Robbie Reliability' followed by a dropdown arrow and the word 'Appian'. The main content area is divided into two sections. On the left, there is a sidebar with the IESO logo and the text 'All >'. On the right, the 'Records' section is titled and contains three items, each with a document icon: 'RCT MP Potential Violations' (Provides details of all of your organization's potential violations and status), 'RCT MP Self Certifications' (Provides details of all of your organization's Self-Certification Requests), and 'Users' (Directory of users).

Self Certifications

- The ERO and MACD are transitioning to a self-certification program that focuses on the most critical reliability standards and that is tailored to each market participant's risk profile. In addition, to increase the level of compliance assurance, in the future MACD will require market participants to attach evidence of compliance to their self-certifications.
- The tool has been developed to accommodate these more detailed or “Guided” Self Certifications as well as EPP/RPA Self-Certifications.

NERC Standards Self-Certification Notification

- Guided Self-Certifications: MPs will receive an email notification with a link to the Self-Certification Task in their Online IESO account.



Online IESO Sign in Prompt



 **ieso**

Username

Password

☒ Remember me on this computer

[Forgot Password](#)

Legal Disclaimer:
Attention to Participants: This system is owned and operated by the IESO, and all use of this system is governed by the Market Rules. As a registered Participant, you have received a unique and confidential User Account and Password from the IESO to access this system and you agree to maintain their confidentiality. You specifically agree that you are exclusively responsible for all access to and any activity on this system that occurs through the use of your User Account and Password. If you become aware of any unauthorized use of your User Account or Password, you agree to immediately notify the IESO. The IESO is not liable for any loss or damage arising from any unauthorized access or use of your User Account and Password. If you do not agree with these terms and conditions, immediately advise the IESO and do not login to this system.

Self Certification Task

- A Self-Certification Task will be waiting for you in your Tasks area
- The task will identify it as a Self-Certification and have a unique Identifier for your records

The screenshot displays the IESO Appian interface. The top navigation bar includes 'News', 'Tasks (1)', 'Records', 'Reports', and 'Actions'. The user profile 'Robbie Reliability' is shown in the top right. On the left sidebar, the IESO logo is at the top, followed by filters for 'Assigned to Me', 'Sent by Me', 'Starred', 'Status' (with an 'Open' filter), and 'Deadline' (with 'Overdue', 'Today', and 'Within 7 days' options). The main content area shows a task card for 'Submit Self Certification' with a blue checkmark icon. The text 'Cert: SC-2016-00309' is circled in red, and a red arrow points to it with the label 'Unique Identifier'. A search bar at the top of the task list says 'Click here to send a task...'. A 'Newest' dropdown is in the top right of the task list.

Self-Certification Submission Screen

News Tasks (2) Records Reports Actions Scott Berry Appian

Submit Self-Certification Request

Certification Request Details

Request ID SC-2016-00521 Organization ID 102007

Certification Name Electronic Security Perimeter Submission Due Date 9/30/2016

★ Certification Text Please complete the attachment and upload it. Please provide any supporting evidence. ★ Compliance Period Start Date 1/1/2015

Certification Type Guided Self-Certification Compliance Period End Date 12/31/2015

Standard Details

Standard ID CIP-005-3 Governing Body NERC

Standard Name CIP Standard Enforcement Date 1/1/2011

Standard Description Cyber Security - Electronic Security Perimeter(s)

Requirement Details

Req ID	Requirement Text	Compliance	Comments
CIP-005-3_R1	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	<input type="radio"/> Compliant <input type="radio"/> Non-Compliant	
CIP-005-3_R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	<input type="radio"/> Compliant <input type="radio"/> Non-Compliant	
CIP-005-3_R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	<input type="radio"/> Compliant <input type="radio"/> Non-Compliant	

3 items

Certification Documents

Guided Self-Certification Worksheet

[Guided Self-Certification Worksheet_Test_2016_08_16](#)

Upload Completed Worksheet and Supporting Document(s) as Needed *

Browse...

[Report Non-Compliance](#)

Click to Download any attached Worksheet, follow the instructions and Upload the Worksheet once complete

Guided Self Certification Worksheet



CONFIDENTIAL – Non-Public Information

Guided Self-Certification Worksheet

Standard: Test

Requirements: Test

Compliance Period: Jan 1 – Dec 31, 2015

SCOPE:

Provide summary of your compliance with the applicable Standard Requirements above.

Supporting Evidence and Documentation

Registered Entity Response:

Describe, in narrative form, how you meet (or do not meet) compliance with the Requirements.

Include a concluding statement stating the results of the self-certification.

Your narrative and concluding statement here.

Registered Entity Evidence:

Provide the following for all evidence submitted (Insert additional rows if necessary):

File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s),
Description

Your Evidence references here

Submit your evidence with this attachment.

Complete Self-Certification

News Tasks (2) Records Reports Actions Scott Berry - Applan

ieso
Save Changes
Reassign Task

Submit Self-Certification Request

Certification Request Details

Request ID	SC-2016-00521	Organization ID	102007
Certification Name	Electronic Security Perimeter	Submission Due Date	9/30/2016
Certification Text	Please complete the attachment and upload it. Please provide any supporting evidence.		
Certification Type	Guided Self-Certification	Compliance Period Start Date	1/1/2015
		Compliance Period End Date	12/31/2015

Standard Details

Standard ID	CIP-005-3	Governing Body	NERC
Standard Name	CIP	Standard Enforcement Date	1/1/2011
Standard Description	Cyber Security - Electronic Security Perimeter(s)		

Requirement Details

Req ID	Requirement Text	Compliance	Comments
CIP-005-3_R1	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	<input checked="" type="radio"/> Compliant <input type="radio"/> Non-Compliant	We have been Compliant over the entire compliance period.
CIP-005-3_R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	<input checked="" type="radio"/> Compliant <input type="radio"/> Non-Compliant	We have been Compliant over the entire compliance period.
CIP-005-3_R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	<input checked="" type="radio"/> Compliant <input type="radio"/> Non-Compliant	We have been Compliant over the entire compliance period.

3 items

Certification Documents

Guided Self-Certification Worksheet
Guided Self-Certification Worksheet_Test_2016_08_16
Upload Completed Worksheet and Supporting Document(s) as Needed *
Guided Self-Certification Worksheet_Test_2016_08_16_Response.docx (63.99 KB) x

Browse

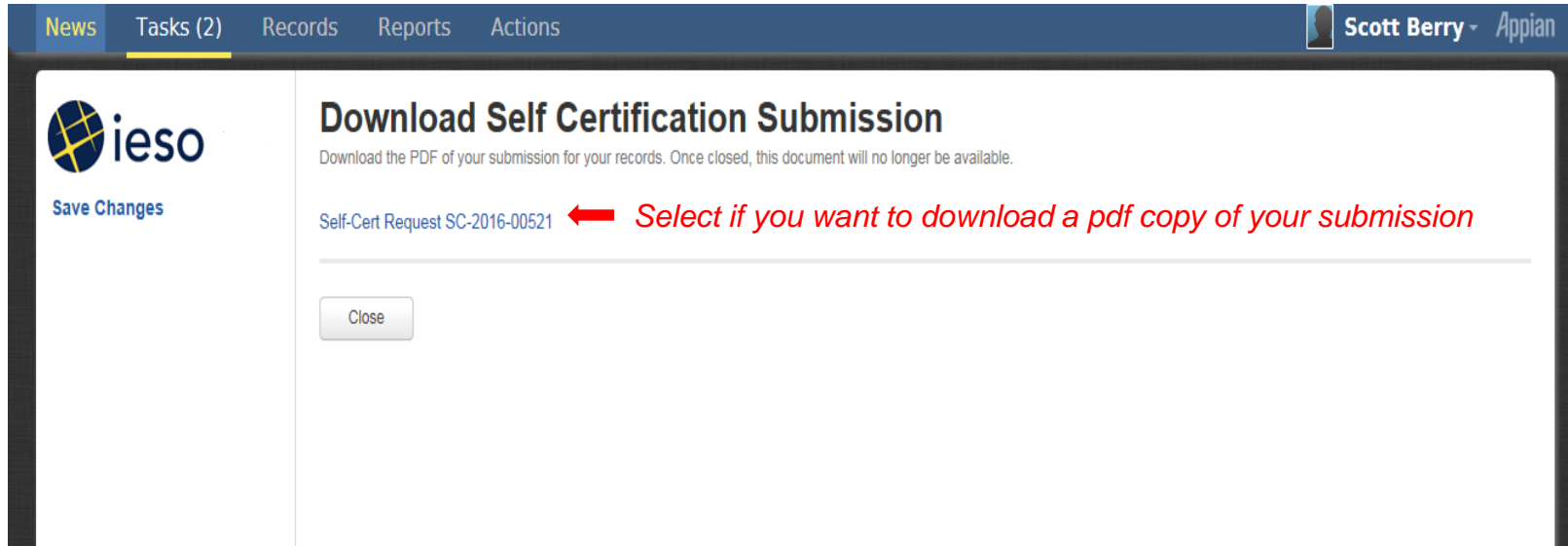
1. Indicate your Compliance Status

2. Provide any relevant comments

3. Attach the completed Worksheet and any relevant evidence to support your compliance status.

4. Press Submit

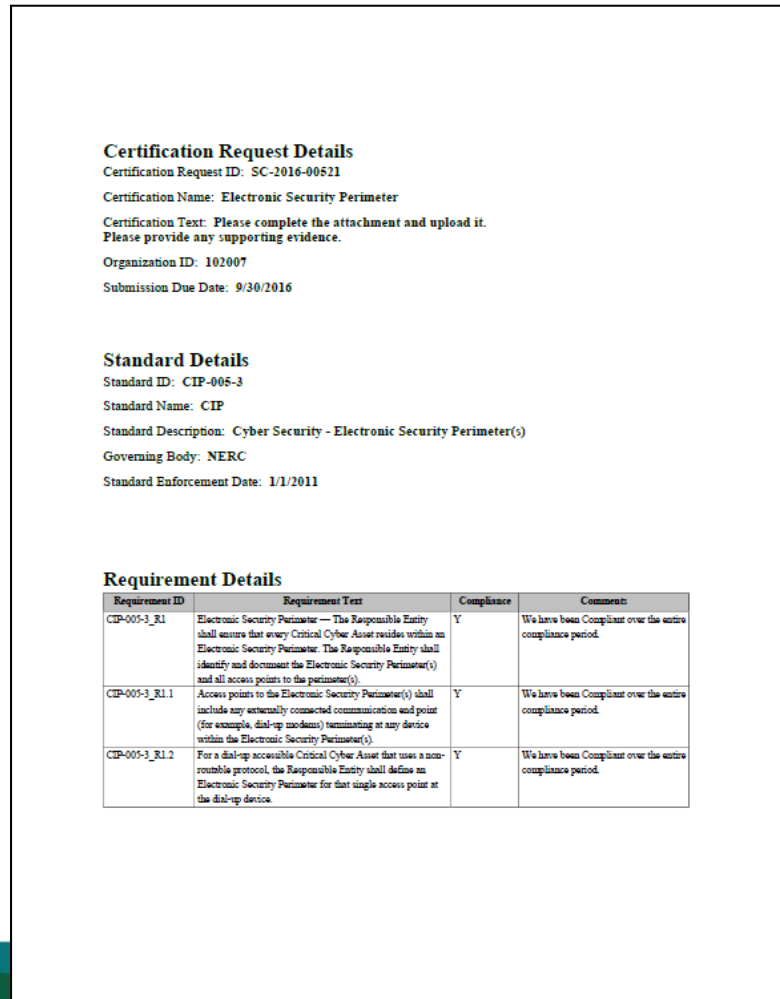
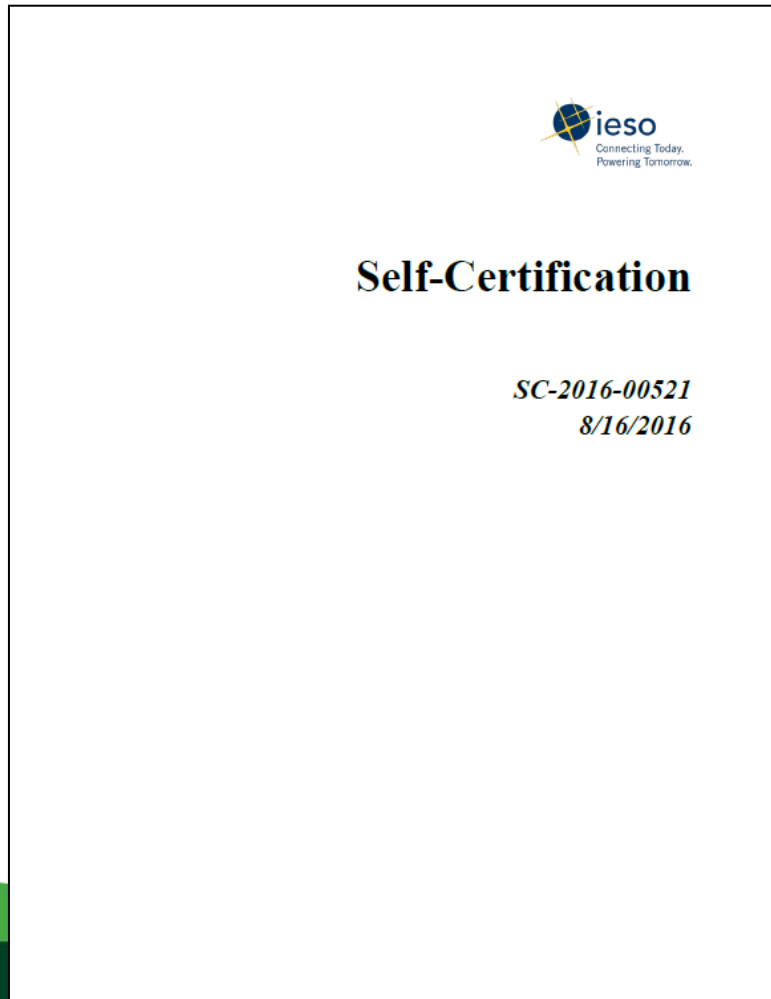
Optional PDF Download



The screenshot displays the IESO Appian user interface. At the top, a navigation bar includes tabs for 'News', 'Tasks (2)', 'Records', 'Reports', and 'Actions'. The user 'Scott Berry' is logged in, with an 'Appian' logo next to their name. On the left sidebar, the IESO logo is visible along with a 'Save Changes' link. The main content area is titled 'Download Self Certification Submission' and contains the instruction: 'Download the PDF of your submission for your records. Once closed, this document will no longer be available.' Below this, a link for 'Self-Cert Request SC-2016-00521' is shown, accompanied by a red arrow pointing to it and a red text annotation: 'Select if you want to download a pdf copy of your submission'. A 'Close' button is located at the bottom of the content area.

MP PDF Download Example

- PDF will include a title page, details of your submission and a copy of the attachments included in your submission.



MP PDF Download Example Con't

- PDF will include a title page, details of your submission and a copy of the attachments included in your submission.

Attachments Included in this Submission

Guided Self-Certification Worksheet_Test_2016_08_16_Response



CONFIDENTIAL – Non-Public Information

Guided Self-Certification Worksheet

Standard: Test

Requirements: Test

Compliance Period: Jan 1 – Dec 31, 2015

SCOPE:

Provide summary of your compliance with the applicable Standard Requirements above.

Supporting Evidence and Documentation

Registered Entity Response:

Describe, in narrative form, how you meet (or do not meet) compliance with the Requirements.

Include a concluding statement stating the results of the self-certification.

Your narrative and concluding statement here.

Registered Entity Evidence:

Provide the following for all evidence submitted (Insert additional rows if necessary):

File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

Your Evidence references here

Submit your evidence with this attachment.

MP Self-Certification Record Storage

The image shows two screenshots of the IESO Records page. The top screenshot shows the 'Records' tab selected in the navigation bar, with a list of records including 'RCT MP Self Certifications'. A red arrow points from this record to the bottom screenshot. The bottom screenshot shows the 'RCT MP Self Certifications' page, displaying details for a specific record (SC-2016-00521). A red arrow points from the 'Select' label to the record details.

Top Screenshot: Records Page

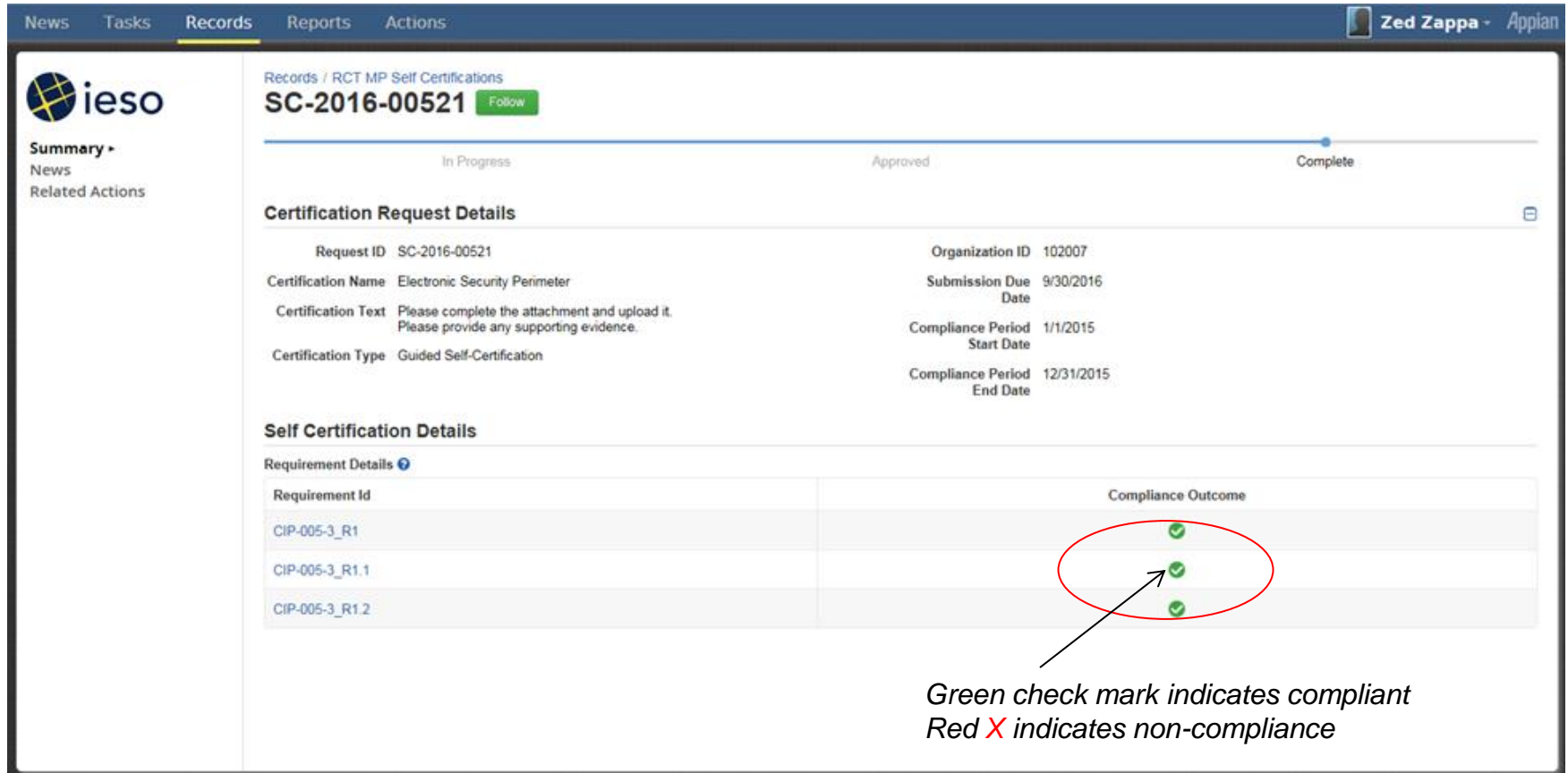
- Navigation: News, Tasks, **Records**, Reports, Actions
- User: Zed Zappa - Appian
- Records List:
 - RCT MP Potential Violations**
Provides details of all of your organization's reported potential violations
 - RCT MP Self Certifications**
Provides details of all of your organization's Self-Certification Requests
 - Users**
Directory of users

Select

Bottom Screenshot: RCT MP Self Certifications Page

- Navigation: News, Tasks, **Records**, Reports, Actions
- User: Zed Zappa - Appian
- Search: Search RCT MP Self Certif Q
- Left Sidebar:
 - All**
 - Status**
 - Approved
 - Completed
 - In-progress
 - Submission Due In**
 - Next 1 week
 - Next 1 month
 - Next 3 months
 - 3 months or more
- Record Details:
 - SC-2016-00521**
 - Request Type: Guided Self-Certification
 - Standard: CIP-005-3
 - Due Date: 9/30/2016
 - Created On: 8/16/2016 1:20 PM EST

MP Self-Certification Record Storage



News Tasks **Records** Reports Actions

ieso

Summary ▾
News
Related Actions

Records / RCT MP Self Certifications
SC-2016-00521 [Follow](#)

In Progress Approved Complete

Certification Request Details

Request ID SC-2016-00521 Organization ID 102007
Certification Name Electronic Security Perimeter Submission Due Date 9/30/2016
Certification Text Please complete the attachment and upload it.
Please provide any supporting evidence. Compliance Period Start Date 1/1/2015
Certification Type Guided Self-Certification Compliance Period End Date 12/31/2015

Self Certification Details

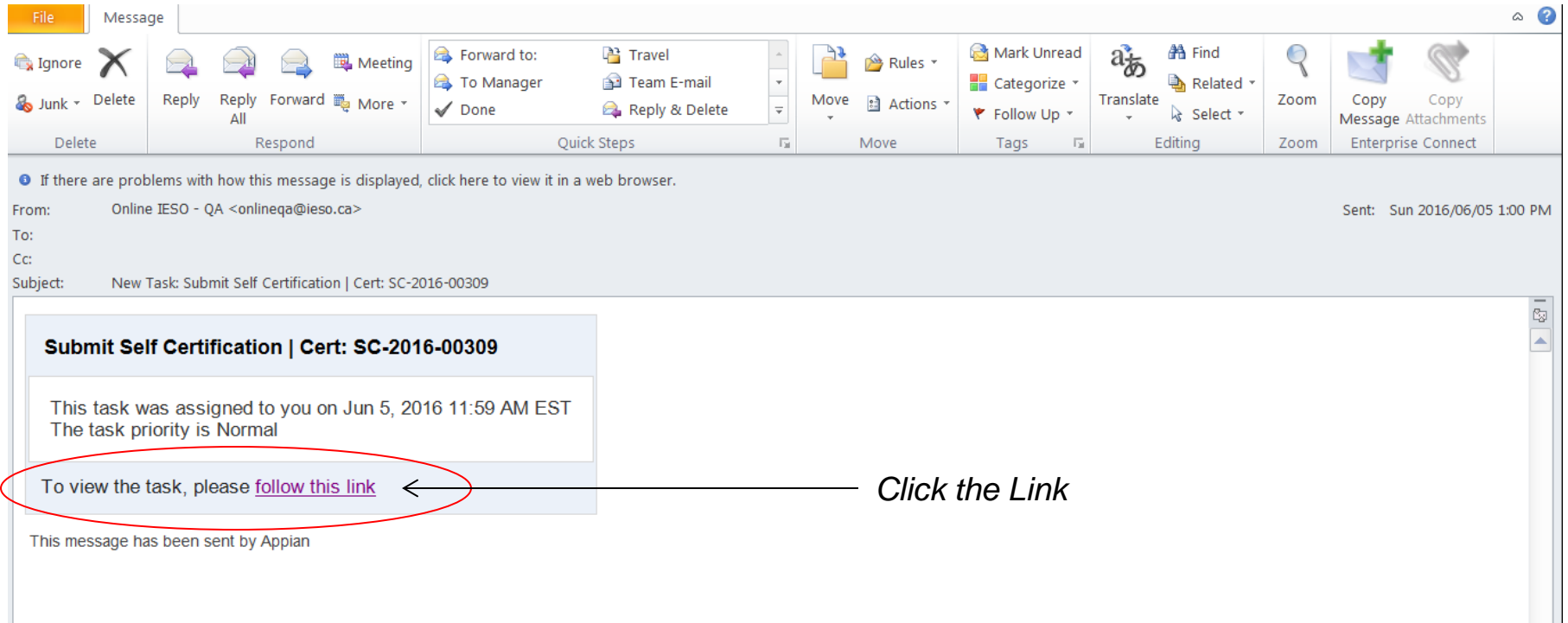
Requirement Details ⓘ

Requirement Id	Compliance Outcome
CIP-005-3_R1	✓
CIP-005-3_R1.1	✓
CIP-005-3_R1.2	✓

Green check mark indicates compliant
Red X indicates non-compliance

EPP/RPA Self-Certification Notification

- EPP/RPA Self-Certification: Similarly, MPs will receive an email notification with a link to the Self-Certification Task in their Online IESO account.



EPP/RPA Self Certification Form

- MPs are asked to complete the attached forms and obtain the appropriate sign off before submitting

Submit Self-Certification Request

Certification Request Details

Request ID SC-2016-00306 Organization ID 102200

Certification Name Emergency Preparedness Plan Review Submission Due Date 6/6/2016

★ Certification Text Please complete the self certification form and the attachment and submit to the IESO. Please follow the instructions on the bottom of the attachment if you have not completed your EPP review for the compliance period. ★

Certification Type Emergency Preparedness Plan (EPP) Self-Certification

Compliance Result

☒ Compliant ☐ Non-Compliant

Comments

Plan Review undertaken in June 2015 as per OPG schedule. No changes to the current plan.

Certification Documents

Emergency Preparedness Plan (EPP) Self-Certification Worksheet
IESO_FORM_1608_v8.0

Upload Completed Worksheet and Supporting Document(s) as Needed *

EPP TEST_IESO_FORM_1608_v8.0_06032016.docx (64.57 KB) ×


Browse...

Submit Compliance

Optional PDF Download

NewsTasks (2)RecordsReportsActions

Scott BerryAppian


Save Changes

Download Self Certification Submission

If you need to download this document at a later time, it will be available in Records

Self-Cert Request SC-2016-00301 ← Select if you want to download a pdf copy of your submission

Close

PDF Downloadable Record



Self-Certification

SC-2016-00308
6/3/2016

Certification Request Details

Certification Request ID: SC-2016-00308

Certification Name: Restoration Plan Attachment Verification

Certification Text: Please complete the self certification form and the attachment and submit to the IESO.

Please follow the instructions on the bottom of the attachment if you have not completed your RPA submission for the compliance period.

Organization ID: 102200

Submission Due Date: 6/6/2016

Compliance Result

Compliant: Y

Comment: No Changes were made to the RPA over the compliance period



Ontario Reliability Compliance Program Requirements Form EMERGENCY RESTORATION PLANNING

NOTICE TO MARKET PARTICIPANTS: The *market rules* require market participants to provide to the IESO such data as may be required and within the time prescribed by the IESO for reliability purposes and to enable the IESO to satisfy a request by a *compliance authority* (see Chapter 5, sections 14.1.3 and 14.1.4). The IESO has developed the Ontario Reliability Compliance Program (ORCP) to assist market participants in meeting these obligations. As part of the ORCP, market participants are required to submit to the IESO electronic certification forms using the IESO Reliability Compliance Tool accessed via the IESO Web Portal.

This requirements form does not replace the electronic certification forms. Rather, it is primarily intended for use by the IESO when the Reliability Compliance Tool becomes unavailable for use.

Terms and acronyms used in this Form that are italicized have the meanings ascribed thereto in Chapter 11 of the "Market Rules".

Part 1 – General Information

Market Participant Information:

Market Participant Name: OPG

Market Participant ID: 102200

Compliance Information:

Compliance Year: 2015

Reporting Period:

From: Jan 1, 2015 To: Dec 31, 2015

IESO FORM 1609 v10.0 Page 1 of 4
REV 15-03

Reference Document(s)

[Market Manual 7.8 – Ontario Power System Restoration Plan \(OPSRP\)](#)

[Market Rules Chapter 5 – Power System Reliability](#), Section 11.3

Signature

I have full authority to bind the *market participant*. I certify that all information set out or referred to in this form is true, accurate and complete as at the date of this certification. I further understand that this information is provided in accordance with the requirements of Chapter 5, Section 14.1.1 of the *market rules*. I understand that this information is subject to verification by the IESO and that such a review or audit will require all information set out or referred to in this form to be verified by appropriate documentation.

²
Certified by MPCC:

Robert Reliability

Please Print Name

Robert Reliability

Signature

Date of Certification: June 3, 2016

Part 2 – Market Participant Compliance Reporting

As an authorized representative of the *market participant*, I certify that the *market participant* was:

☒ **COMPLIANT** with the requirements of IESO-FORM-1609 stated below for the entire Reporting Period.

Did the review of your *restoration participant attachment* during the compliance reporting Period require any changes to be made? Please respond either "Yes" or "No" and include your comment, if any.

Please enter the last *restoration participant attachment* review date completed during the Reporting Period.

Comment: No, No changes were necessary to the RPA

☐ **NON-COMPLIANT** for a portion of or the entire Reporting Period with some or all requirement(s) of IESO-FORM-1609, but in compliance with all other applicable requirements of IESO-FORM-1609 for the entire Reporting Period, as indicated below.

☐ R1: All *restoration participants* must submit a *restoration participant attachment* to the IESO and must contain the following information:

☐ 1.1: Facilities:

☐ 1.1.1: All *facilities* covered by the attachment are identified.

☐ 1.1.2: All *directly-connected facilities*, including control centres, that are pre-wired to accept backup/parallel generation and loads that can be supplied from this source are identified.

☐ 1.6: *Restoration participants* must verify that they:

☐ 1.6.1: Deliver a training program to operators, which includes their restoration obligations and expected actions, and is based on the equipment and tools that they operate.

☐ 1.6.2: Provide two hours of restoration-related training every two calendar years to their field switching personnel that perform unique restoration-related tasks that are outside their normal tasks.

☐ 1.6.3: Have shown due diligence in preparing their operators to fulfill their restoration obligations by ensuring they have attended restoration training within the last three years.

☐ 1.6.4: Maintain operator training records.

☐ 1.6.5: *Restoration participants* that operate *certified black start facilities* must verify that they provide two hours of restoration-related training every two calendar years to any operating personnel responsible for performing startup of black start generation units and energization of the associated initial bus/circuit on the restoration path.

☐ 1.7: *Restoration participants* that use agents to fulfill any restoration-related operating obligations remain responsible for fulfilling those obligations, including training of the agents. In addition, the *restoration participant* must:

☐ 1.7.1: Identify that agents are used and the *facilities* they operate.

☐ 1.7.2: Identify the agreements that govern the use of their operating agents.

☐ 1.8: *Restoration participants* must provide the following contact information

Self-Certification submission reminders

- Notifications will be released via email according to the following timelines to Market Participants:
 - The Market Participant Compliance Contact (MPCC) will receive:
 1. The Initial Self Certification request
 2. Notification that the submission is due in 15 days
 3. Notification that the submission is due in 10 days
 - The Market Participant Escalation Contact (MPEC) will receive:
 4. Notification that the submission is due in 5 days
- Once the submission has been made by the Market Participant the notifications are cancelled.
- MACD will be notified if your submission is past due.

Copies of Self-Certifications to MACD records

- All Self-Certifications are sent to a MACD folder in the IESO Records Repository.
- Compliant Self- Certifications and evidence are stored for MACD review.
- Those Self Certifications marked as Non-Compliant are flagged for MACD review and follow-up

Self Reporting

- Self-reporting relies on the monitoring mechanisms of the market participant's internal compliance program to systematically review their compliance with reliability standards, and to detect potential non-compliance.
- If a market participant believes that they may have breached a reliability standard, they are strongly encouraged to take all reasonable steps to mitigate the impact that the breach may have caused on reliability and self-report the breach in a timely manner.


Self Reporting through the RCT

- MPs can initiate a standards self report via the Online IESO RCT Actions Tab.

The screenshot shows a web browser window with the URL <https://onlineqa.ieso.ca/suite/tempo/actions/view/all>. The browser's address bar includes search, lock, and refresh icons. The page features a navigation bar with tabs for News, Tasks, Records, Reports, and Actions (which is currently selected). On the right side of the navigation bar, there is a user profile for 'Robbie Reliability' and an 'Appian' logo. The main content area is divided into two sections. The left section contains the IESO logo, a list of filters including 'All' and 'Starred', and a section for 'Applications' with a link to 'Reliability Compliance Tool'. The right section is titled 'Report Potential Standards Violation (MP)' with a lightning bolt icon and a star icon, and it contains the text 'Report a Potential Standards Violation'.

Complete the Possible Violations Form

News Tasks (1) Records Reports Actions Zed Zappa - Applan



Save Changes

Submit Potential Standards Violation

Complete form and upload any mitigation plan documents below

Provide Details

Report Date Aug 17, 2016	Violation Start Date * <input type="text" value="M/d/yyyy"/>
Organization HYDRO ONE NETWORKS INC. (102007)	Violation End Date <input type="text" value="M/d/yyyy"/>
Detection Date * <input type="text" value="M/d/yyyy"/>	Leave blank if still in violation

Governing Body *
☐ NERC ☐ NPCC

Market Rules

Description Of Incident *

Details *

Summary *

Action taken to date *

Attach Documents

Upload Mitigation Plan Documents if Available

Comment History

Date	User	Comment
No items available		

[Add Comment](#)



ing Today.
Tomorrow.

Submit Possible Violation Form with relevant supporting attachments (part 1)

News Tasks (1) Records Reports Actions Zed Zappa - Applian

ieso
Save Changes

Submit Potential Standards Violation

Complete form and upload any mitigation plan documents below

Provide Details

Report Date
Aug 17, 2016

Organization
HYDRO ONE NETWORKS INC. (102007)

Detection Date
8/2/2016

Violation Start Date*
8/1/2016

Violation End Date
8/1/2016
Leave blank if still in violation

Governing Body*
☒ NERC ☐ NPCC

Select Standard*
CIP-004-5.1 : Cyber Security — PerSystem Operationsnel & Training

Standard Details

Standard ID	CIP-004-5.1	Governing Body	NERC
Standard Name	CIP	Standard Enforcement Date	
Standard Description	Cyber Security — PerSystem Operationsnel & Training		

Select Applicable Requirements

Req ID	Requirement
<input type="checkbox"/> CIP-004-5.1_R1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R1 – Security Awareness Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
<input checked="" type="checkbox"/> CIP-004-5.1_R2	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-5.1 Table R2 – Cyber Security Training Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
<input type="checkbox"/> CIP-004-5.1_R3	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]
<input type="checkbox"/> CIP-004-5.1_R4	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]
<input type="checkbox"/> CIP-004-5.1_R5	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R5 – Access Revocation. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]

1. Enter your violation dates

2. Choose NERC Std's or NPCC Criteria

3. Select the violated standard

4. Select the violated requirement(s)

Submit Possible Violation Form with relevant supporting attachments (part 2)

Market Rules

Description Of Incident *
On August 1, 2016 it was discovered that the Company failed to provide annual (within a 15 month time period) cyber security training to a subset of authorized contract personnel.

Details *
CIP004-5.1 R2 states: Training —The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.
R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.
Upon discovery the contractors were immediately provided with the Training package

Summary *
On August 1, 2016 it was discovered that the Company failed to provide annual (within a 15 month time period) cyber security training to a subset of authorized contract personnel

Action taken to date *
- Training was provided to the contractors on August 1 upon discovery that they had not been trained.
- Review of training requirements has been assigned to Dept X for annual maintenance and provision
- Protocols have been put in place to ensure all contractors are provided cyber security training before physical access to the property is permitted.

Attach Documents
Upload Mitigation Plan Documents if Available

Comment History

Date	User	Comment
No items available		

← Add any comments you feel are necessary

5. Provide as many details of the violation as possible in the areas provided.

6. Provide any evidence you feel supports your position. Provide a Mitigation Plan if available.

7. Press submit


Processing the Possible Violation submission

- Market Participant Possible Violation submissions will be sent to Compliance Assurance for initial triage before they are forwarded to the MACD folder in the IESO's records repository.
- If the submission is incomplete or does not have required information it will be returned to the MP for rework
- If the submission is satisfactory it will be sent to the MACD folder and MACD will be notified via email that a submission has been made. All attachments will accompany the submission into the folder.

Self Report MP Record

- Go to Records


NewsTasksRecordsReportsActions



Search RCT MP Potential

All ▶
Status
Complete
In Progress

RCT MP Potential Violations



[SR-2016-00508](#) ←
Standard: CIP-004-5.1
Requirements: CIP-006-5_R2; CIP-004-5.1_R2
Status: In Progress
Potential Violation Detection Date: 8/2/2016

Click on the Report number you wish to see

Self Report MP Record


News

Tasks

Records

Reports

Actions



Summary ▾

News

Related Actions

Records / RCT MP Potential Violations

SR-2016-00508 Follow

Cancelled

In Progress

Complete

All Active Tasks

Task Name	Assigned To	Status	Started on
Review MP PV Submission	IESO Compliance Assurance SME	Assigned	8/17/2016 12:18 PM EST

Submission Details

Potential Violation Request ID

PV-2016-00517

Report Date

Aug 17, 2016

Detection Date

Aug 2, 2016

Org ID

102007

Org Name

HYDRO ONE NETWORKS INC.

Standard Details

Standard ID

CIP-004-5.1

Standard Name

CIP

Standard Description

Cyber Security — PerSystem Operationsnnel & Training

Governing Body

NERC

Standard Enforcement Date

Requirements Assessed for Potential Violation

Req ID	Requirement
CIP-006-5_R2	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in CIP0065 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]

Details of Potential Violation

Description Of Incident

On August 1, 2016 it was discovered that the Company failed to provide annual (within a 15 month time period) cyber security training to a subset of authorized contract personnel.

Details

CIP004-5.1 R2 states: Training —The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary. R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency. Upon discovery the contractors were immediately provided with the Training package

Summary

On August 1, 2016 it was discovered that the Company failed to provide annual (within a 15 month time period) cyber security training to a subset of authorized contract personnel

Action taken to date

- Training was provided to the contractors on August 1 upon discovery that they had not been trained.

- Review of training requirements has been assigned to Dept X for annual maintenance and provision

- Protocols have been put in place to ensure all contractors are provided cyber security training before physical access to the property is permitted.

The Report provides the same information as was submitted on the Form

Communicating RCT Issues

- The following Communication channels are available to participants if you run into issues with the tool:
 - IESO IT Helpdesk: it.servicedesk@IESO.ca or 905-855-6200
 - Email: orcp@ieso.ca
 - System access: customer.relations@ieso.ca
- Postings on the website: [Reliability Compliance Tool](#)

Thank you for participating

Q&A