talk with TEXAS RE

Self-Logging

Alex Petak
Enforcement Attorney

Mishani Tamayo
Enforcement Program Coordinator

March 2, 2023

TEXAS RE

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Upcoming Texas RE Events

March 9, 2023

APT Cyber Tools Targeting ICS/SCADA Devices

March 16, 2023

Cold Weather Standards

March 29, 2023

Women's Leadership in Grid Reliability and Security Conference

Upcoming ERO Events

March 20, 2023

Technical Talk with RF

March 21, 2023

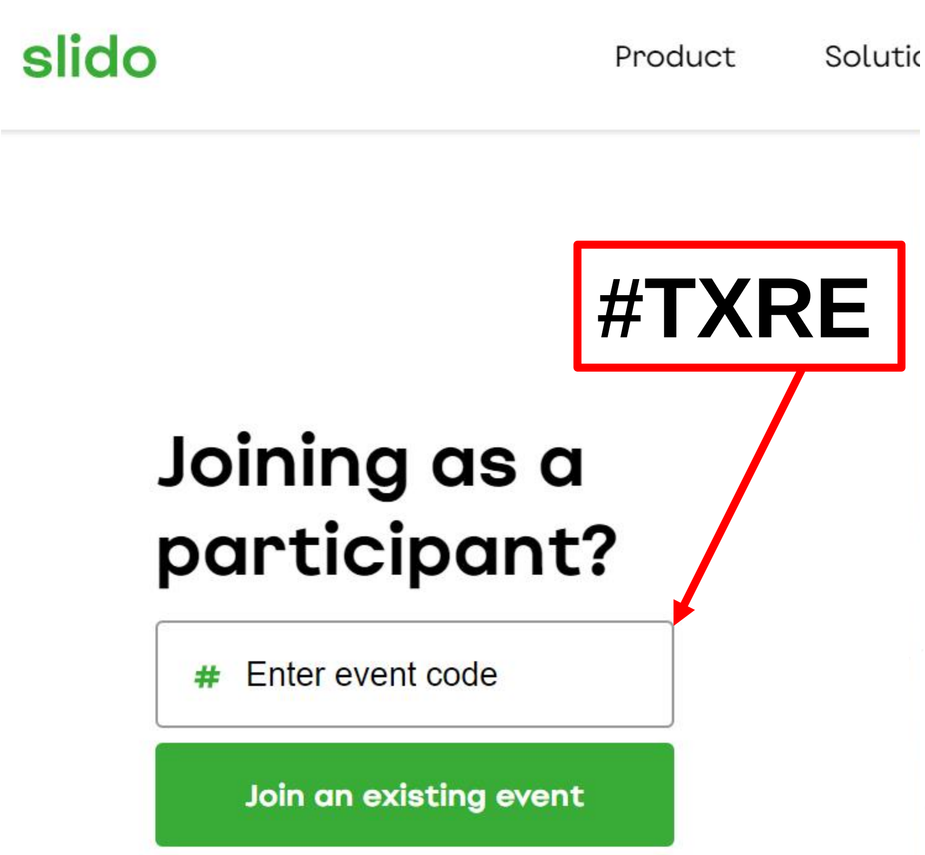
Spring Reliability and Security Virtual Workshop

March 22, 2023

MRO Hybrid RAM Conference

Sli.do

Who has heard of the Self-Logging program?



slido

#TXRE

Joining as a participant?

Agenda

Topics to Discuss Today:

1. What is the Self-Logging program?
2. Who is the program for?
3. Benefits of the Self-Logging program
4. How to join and submit logs
5. How to use the program effectively

What is Self-Logging?

An Alternative to Self-Reporting

Registered Entity Logs Minimal Risk Noncompliance

- Still contains essential parts
- Submitted to Regional Entity for review and approval at least once every six months
- Rebuttable presumption appropriate for compliance exception treatment

NERC Self-Logging User Guide

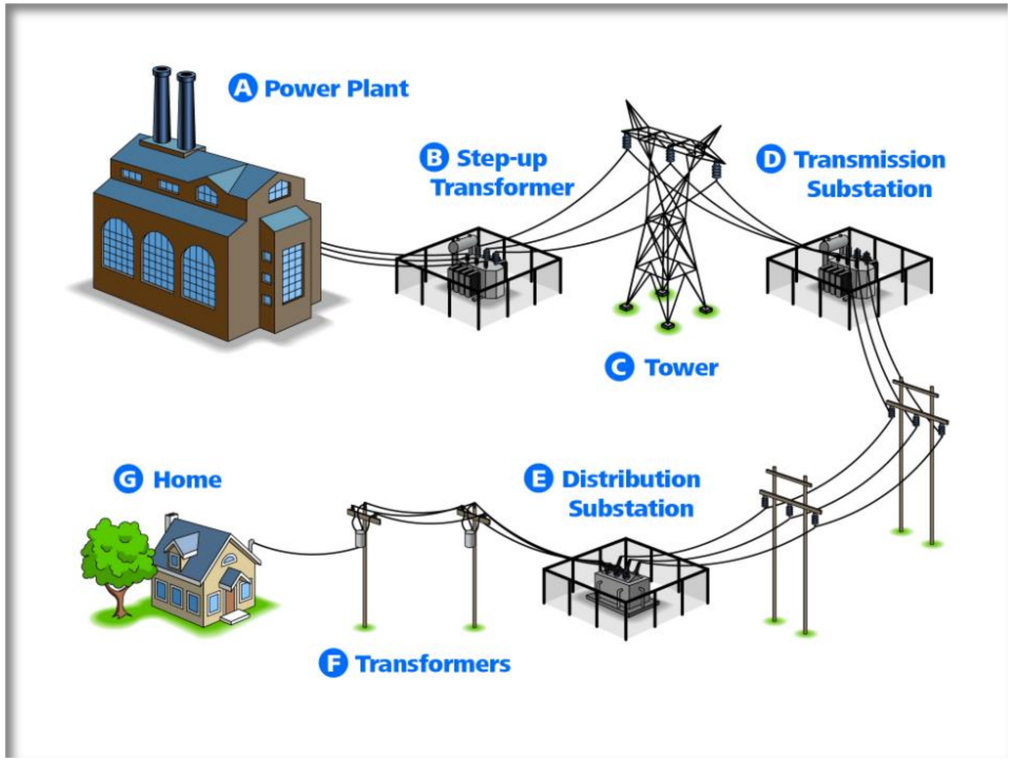
Who is the Program For?

EVERYONE
E
ESRB

All registered entities may apply

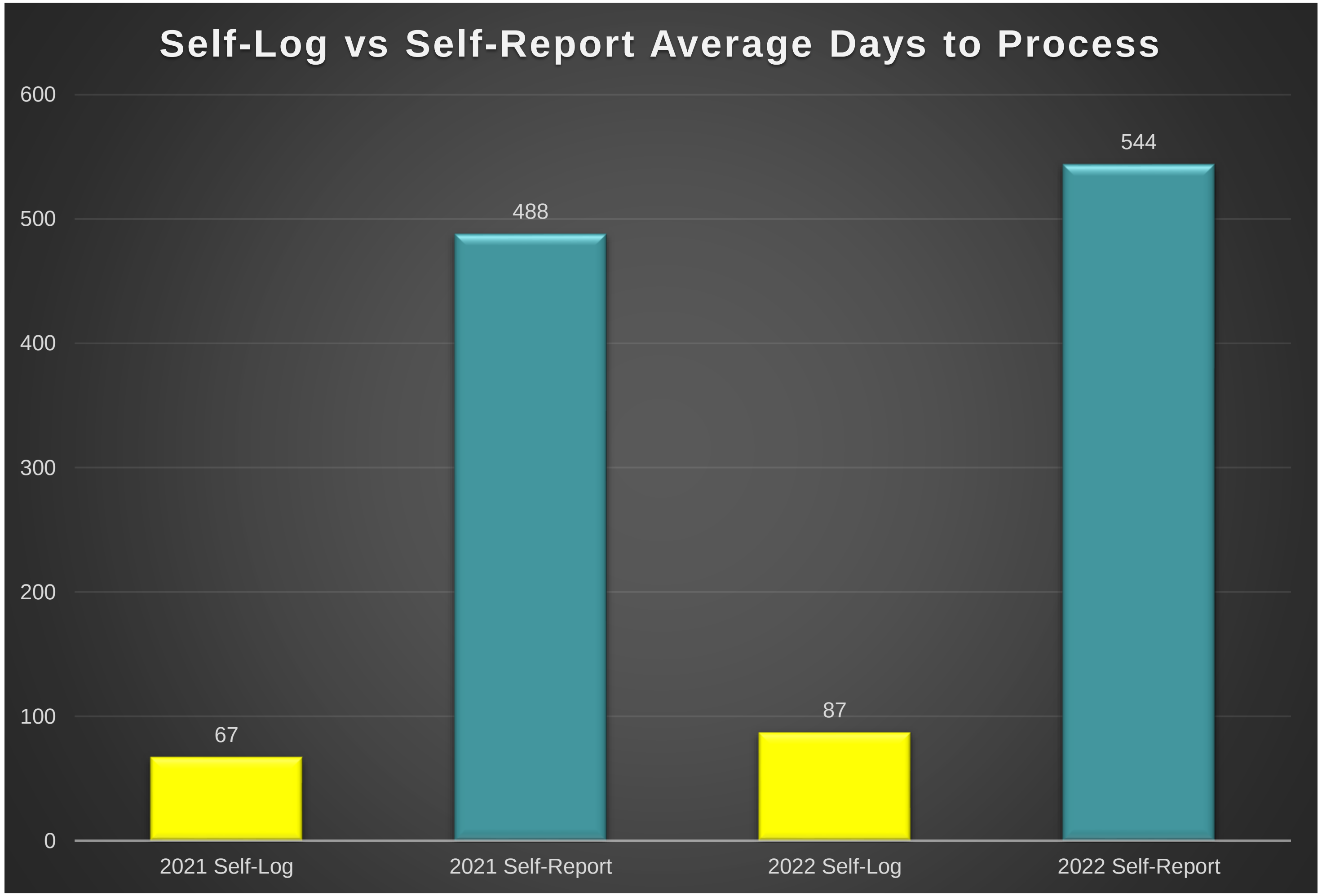
Eligibility based on robust Compliance Program

- Identification of PNCs
- Evaluation of PNCs
- Correction of PNCs



Benefits of the Program

- Presumption of compliance expectation (CE) treatment
- No need to develop a Self-Report for every issue
- Fewer (if any) requests for information (RFIs)
- No evidence submission required
- Faster processing



Benefits of the Program

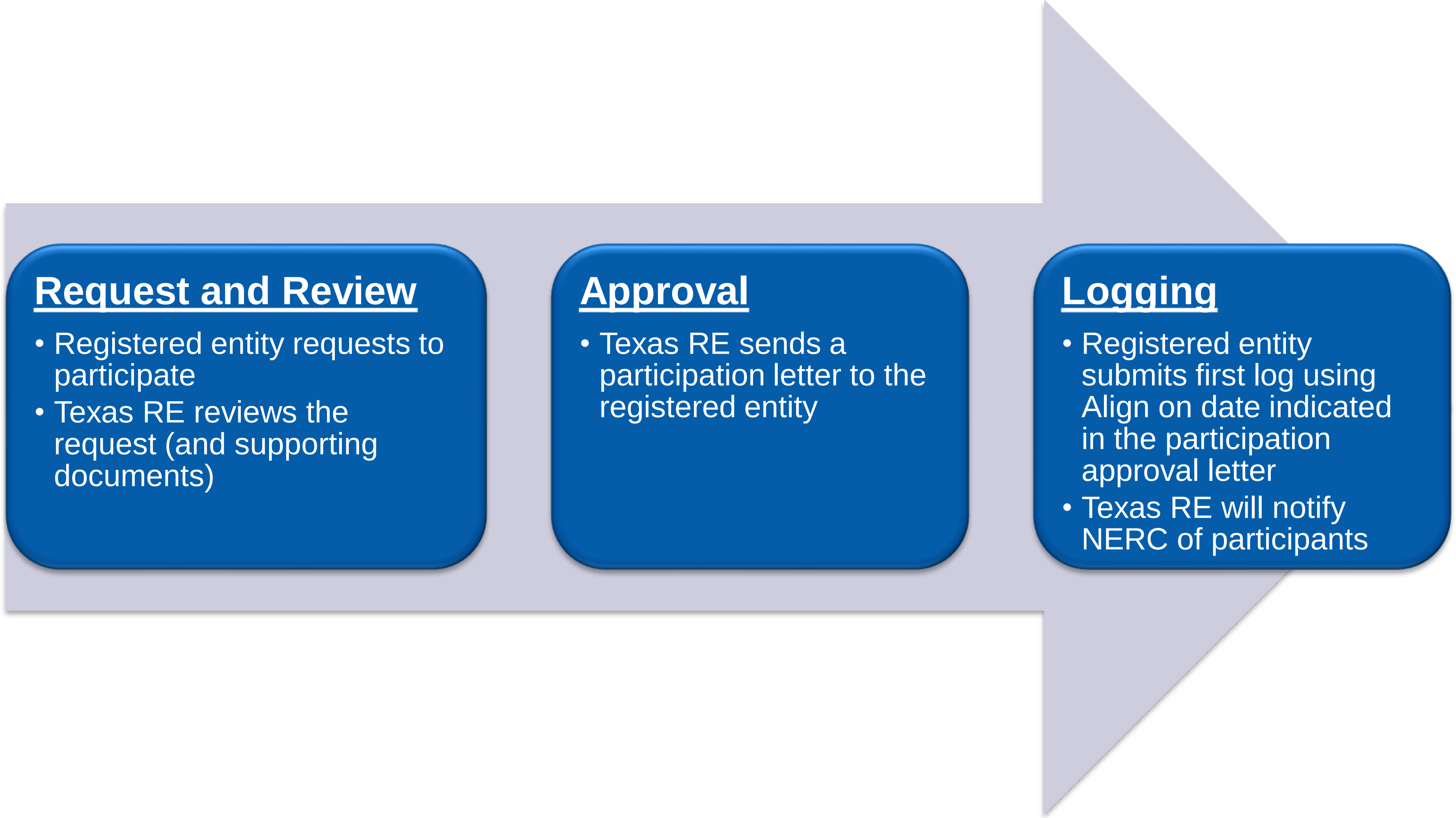
- Gives regulators confidence that the industry is monitoring and addressing their risks

- Can assist Regional Entities in trend spotting and further show a strong compliance culture

Slido Question

Who has submitted a self-log before?

Request to Participate in Self-Logging



Request and Review

- Registered entity requests to participate
- Texas RE reviews the request (and supporting documents)

Approval

- Texas RE sends a participation letter to the registered entity

Logging

- Registered entity submits first log using Align on date indicated in the participation approval letter
- Texas RE will notify NERC of participants

Request to Participate in Self-Logging

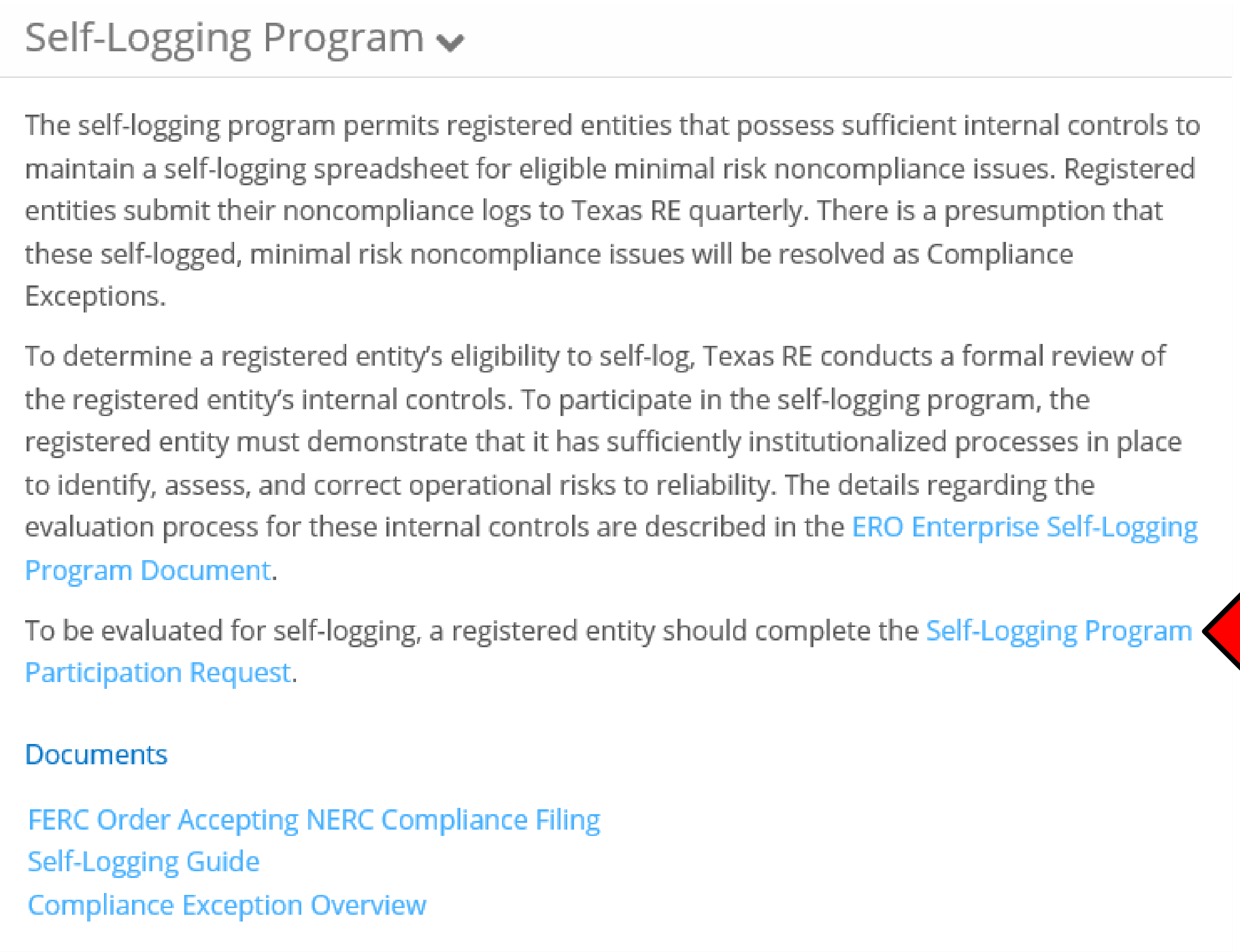
To Submit a Formal Request:

(1) Complete the Self-Logging Program Participation Request (Template)

(2) Include any documents (processes, etc.) describing your internal controls

(3) Email Texas RE at: enforcement@texasre.org with the subject line “Request for Evaluation – [Registered Entity Name]”

Self-Logging Webpage



Self-Logging Program

The self-logging program permits registered entities that possess sufficient internal controls to maintain a self-logging spreadsheet for eligible minimal risk noncompliance issues. Registered entities submit their noncompliance logs to Texas RE quarterly. There is a presumption that these self-logged, minimal risk noncompliance issues will be resolved as Compliance Exceptions.

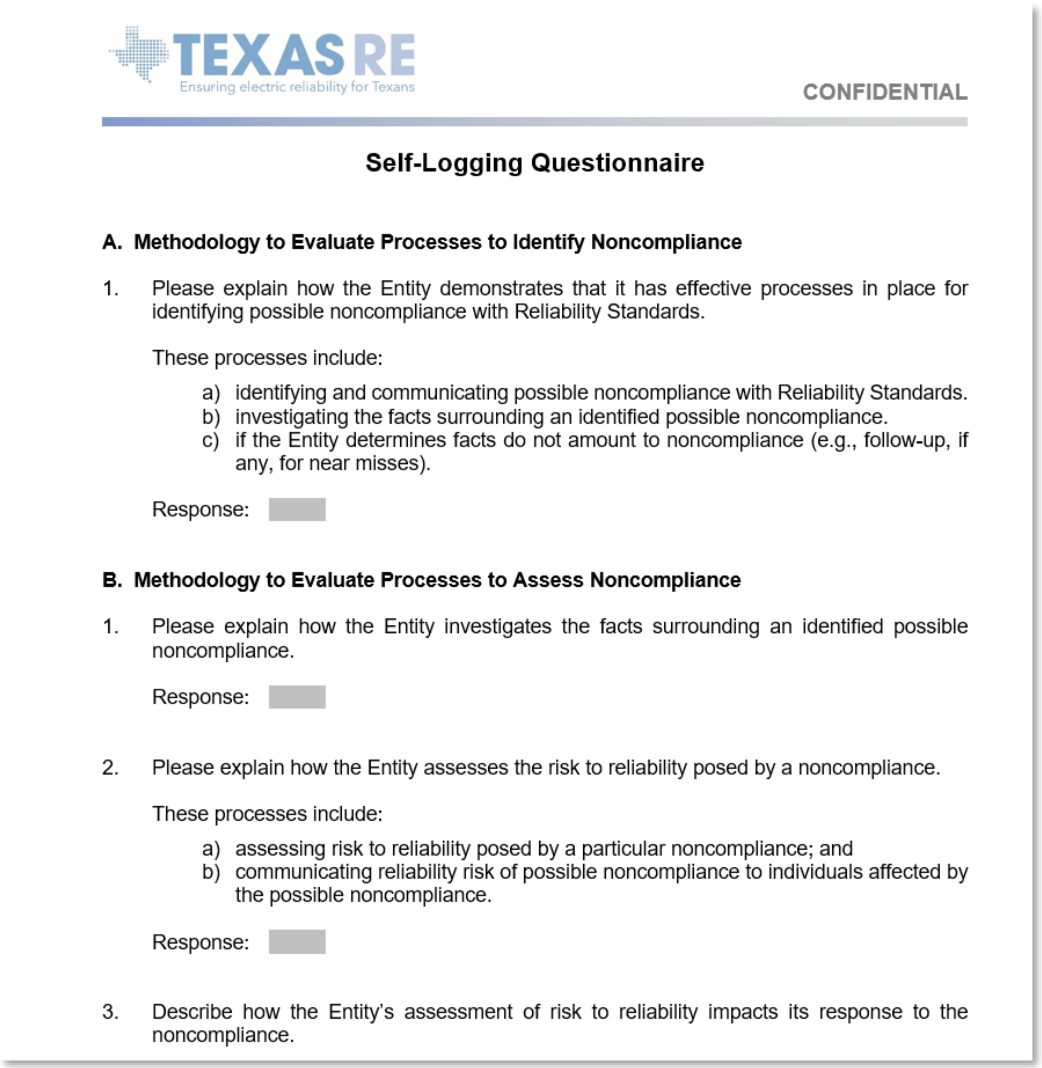
To determine a registered entity's eligibility to self-log, Texas RE conducts a formal review of the registered entity's internal controls. To participate in the self-logging program, the registered entity must demonstrate that it has sufficiently institutionalized processes in place to identify, assess, and correct operational risks to reliability. The details regarding the evaluation process for these internal controls are described in the ERO Enterprise Self-Logging Program Document.

To be evaluated for self-logging, a registered entity should complete the Self-Logging Program Participation Request.

Documents

FERC Order Accepting NERC Compliance Filing
Self-Logging Guide
Compliance Exception Overview

Self-Logging Program Participation Request Template



CONFIDENTIAL

Self-Logging Questionnaire

A. Methodology to Evaluate Processes to Identify Noncompliance

1. Please explain how the Entity demonstrates that it has effective processes in place for identifying possible noncompliance with Reliability Standards.

   These processes include:

   a) identifying and communicating possible noncompliance with Reliability Standards.
   b) investigating the facts surrounding an identified possible noncompliance.
   c) if the Entity determines facts do not amount to noncompliance (e.g., follow-up, if any, for near misses).

   Response:

B. Methodology to Evaluate Processes to Assess Noncompliance

1. Please explain how the Entity investigates the facts surrounding an identified possible noncompliance.

   Response:

2. Please explain how the Entity assesses the risk to reliability posed by a noncompliance.

   These processes include:

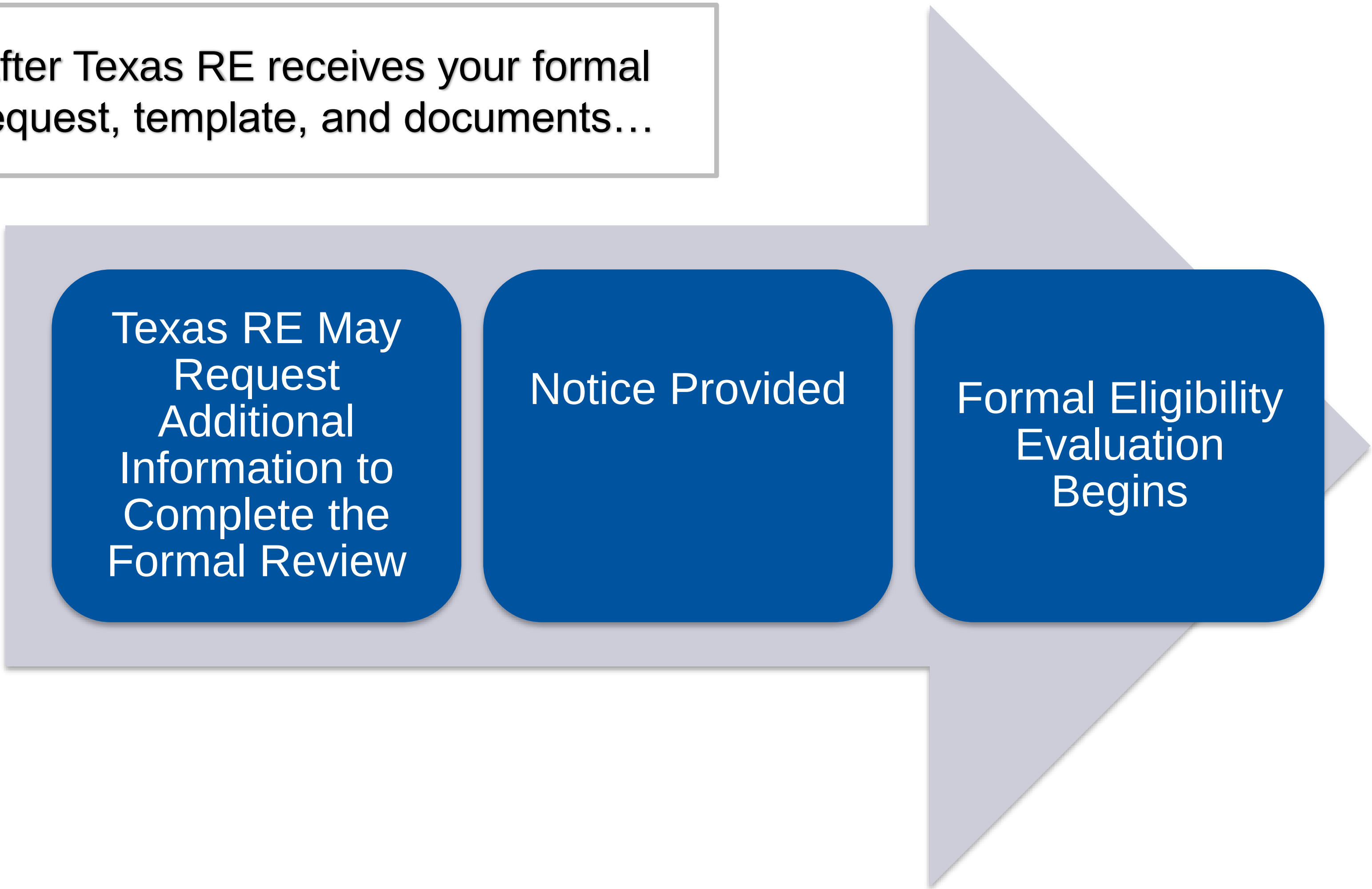
   a) assessing risk to reliability posed by a particular noncompliance; and
   b) communicating reliability risk of possible noncompliance to individuals affected by the possible noncompliance.

   Response:

3. Describe how the Entity's assessment of risk to reliability impacts its response to the noncompliance.

Self-Logging Eligibility Review Process

After Texas RE receives your formal request, template, and documents…


Texas RE May Request Additional Information to Complete the Formal Review

Notice Provided

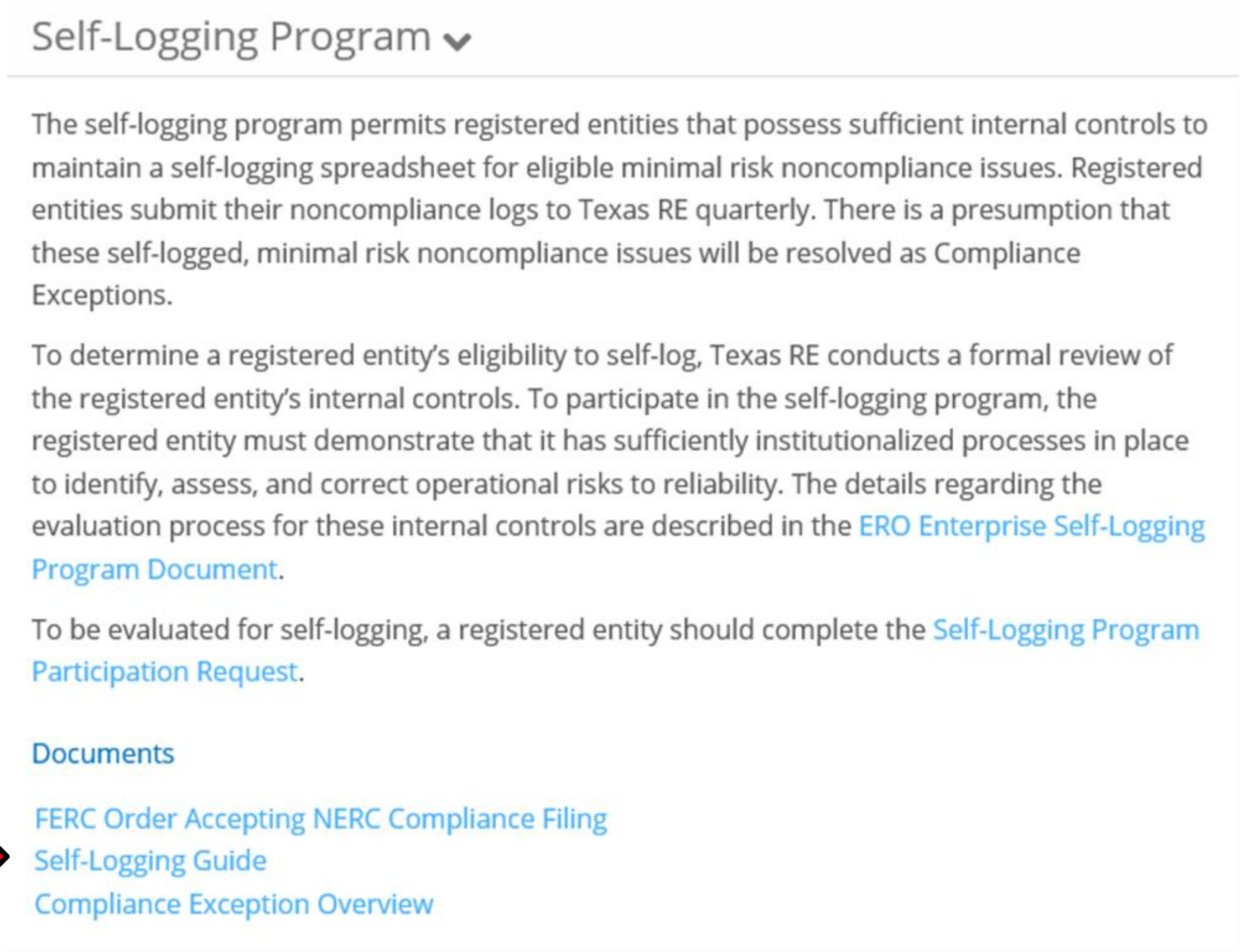
Formal Eligibility Evaluation Begins

Self-Logging Eligibility Criteria

<u>Texas RE Will Review Your Registered Entity’s</u>:

- History with Texas RE
  - Compliance history
  - Texas RE’s experience with your entity
- Evidence of effective processes for identifying possible noncompliance
- Timing and quality of self-reports
- Risk Assessment ability/quality
- Mitigation Performance
- Internal Compliance Program
- Inherent Risk Assessment
- Proposed Self-Logging procedure (optional)

Self-Logging User Guide



Self-Logging Program

The self-logging program permits registered entities that possess sufficient internal controls to maintain a self-logging spreadsheet for eligible minimal risk noncompliance issues. Registered entities submit their noncompliance logs to Texas RE quarterly. There is a presumption that these self-logged, minimal risk noncompliance issues will be resolved as Compliance Exceptions.

To determine a registered entity's eligibility to self-log, Texas RE conducts a formal review of the registered entity's internal controls. To participate in the self-logging program, the registered entity must demonstrate that it has sufficiently institutionalized processes in place to identify, assess, and correct operational risks to reliability. The details regarding the evaluation process for these internal controls are described in the ERO Enterprise Self-Logging Program Document.

To be evaluated for self-logging, a registered entity should complete the Self-Logging Program Participation Request.

Documents

FERC Order Accepting NERC Compliance Filing
Self-Logging Guide
Compliance Exception Overview

Eligibility Determination

Texas RE will provide formal, written notification of eligibility determination which will include:

- Whether the registered entity qualifies for Self-Logging
- The basis for Texas RE's decision
- The Reliability Standards for which the registered entity is eligible to Self-Log
- The date the first Self-Log is due

Self-Logging Process

Registered entity enters log using Align on or before submission due date

- ***No longer*** a process where Entity emails log to Texas RE

Texas RE Enforcement reviews the Self-Log to ensure that the logged instances of noncompliance are:

- Adequately identified and described
- Reasonably and justifiably assessed as minimal risk
- Adequately and appropriately corrected (i.e. mitigated)

Self-Logging Schedule

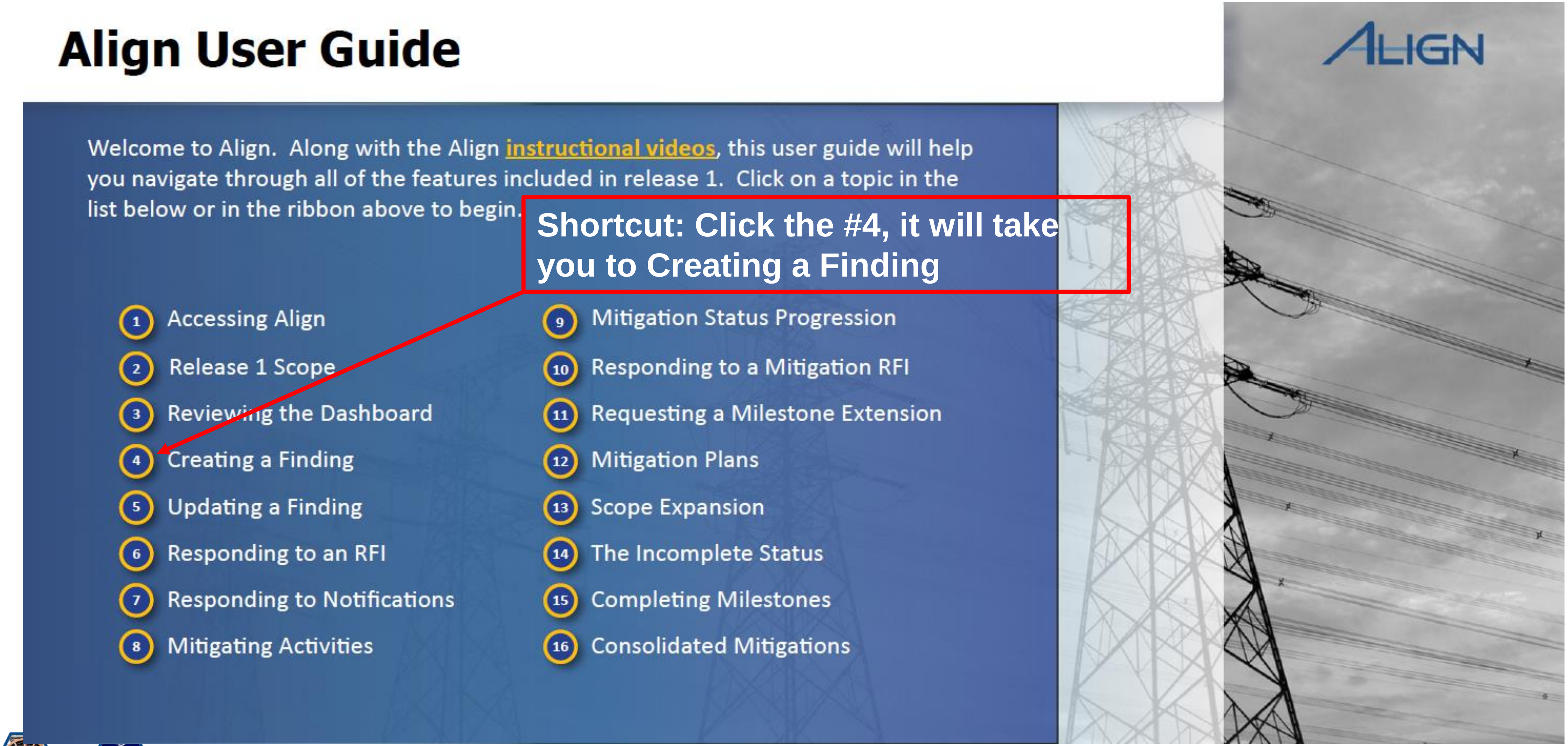
Self-Logs Must be Submitted Every Six Months

- Allowed to log anytime ***before*** your submission due date

Guidance for Drafting Self-Log

- CE Precedent located on the NERC Enforcement and Mitigation Page
- Align for Registered Entities (training videos for using Align)
- Registered Entity User Guide

Creating a Self-Log Finding



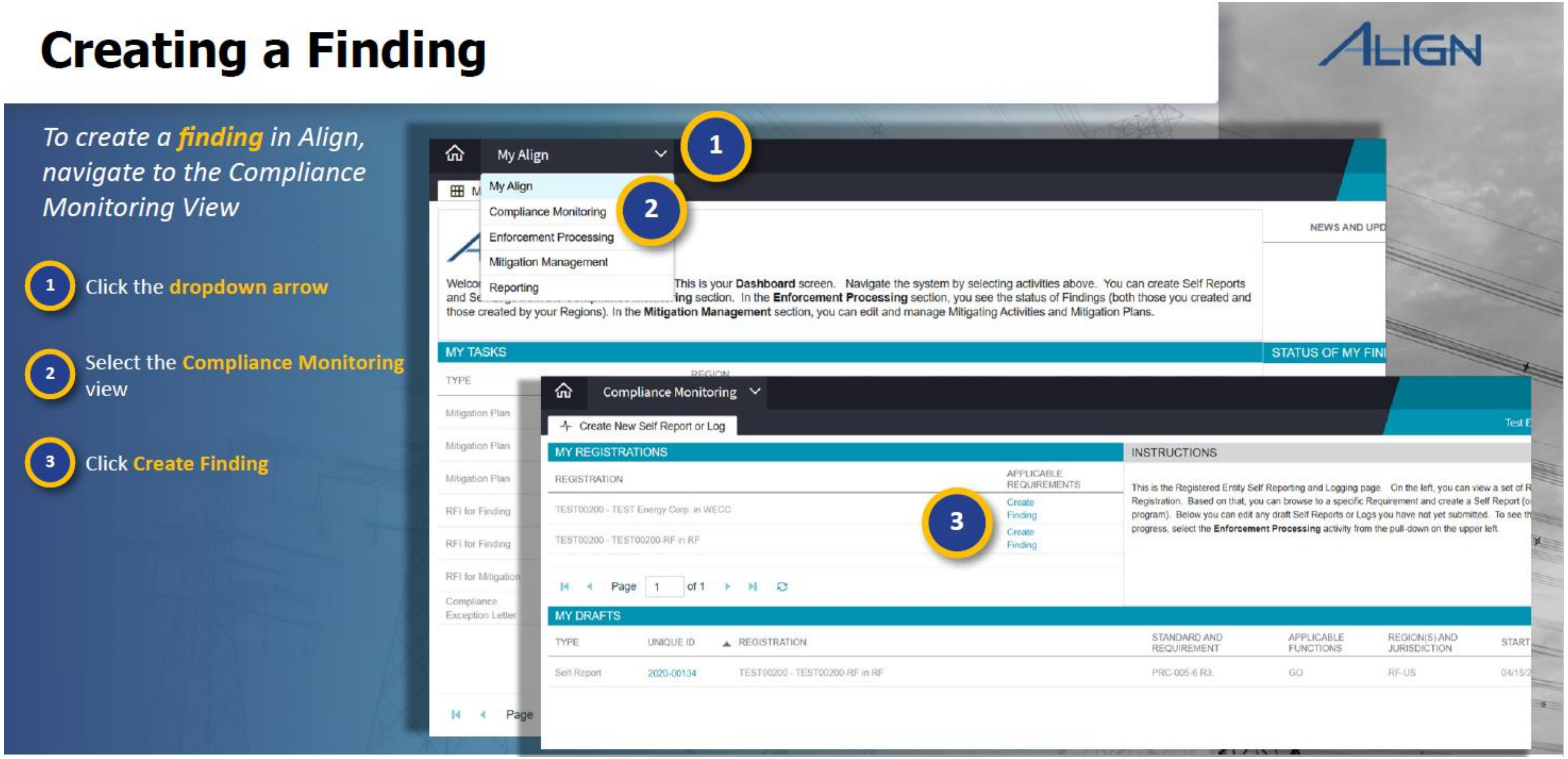
Align User Guide

Welcome to Align. Along with the Align instructional videos, this user guide will help you navigate through all of the features included in release 1. Click on a topic in the list below or in the ribbon above to begin.

1 Accessing Align
2 Release 1 Scope
3 Reviewing the Dashboard
4 Creating a Finding
5 Updating a Finding
6 Responding to an RFI
7 Responding to Notifications
8 Mitigating Activities
9 Mitigation Status Progression
10 Responding to a Mitigation RFI
11 Requesting a Milestone Extension
12 Mitigation Plans
13 Scope Expansion
14 The Incomplete Status
15 Completing Milestones
16 Consolidated Mitigations

Shortcut: Click the #4, it will take you to Creating a Finding

Creating a Self-Log Finding



Creating a Finding

*To create a **finding** in Align, navigate to the Compliance Monitoring View*

1. Click the **dropdown arrow**
2. Select the **Compliance Monitoring** view
3. Click **Create Finding**

Welco[...] This is your **Dashboard** screen. Navigate the system by selecting activities above. You can create Self Reports and Se[...]ing section. In the **Enforcement Processing** section, you see the status of Findings (both those you created and those created by your Regions). In the **Mitigation Management** section, you can edit and manage Mitigating Activities and Mitigation Plans.

MY TASKS

TYPE	REGION
Mitigation Plan	
Mitigation Plan	
Mitigation Plan	
RFI for Finding	
RFI for Finding	
RFI for Mitigation	
Compliance Exception Letter	

STATUS OF MY FINI

MY REGISTRATIONS

REGISTRATION	APPLICABLE REQUIREMENTS
TEST00200 - TEST Energy Corp. in WECC	Create Finding
TEST00200 - TEST00200-RF in RF	Create Finding

Page 1 of 1

INSTRUCTIONS

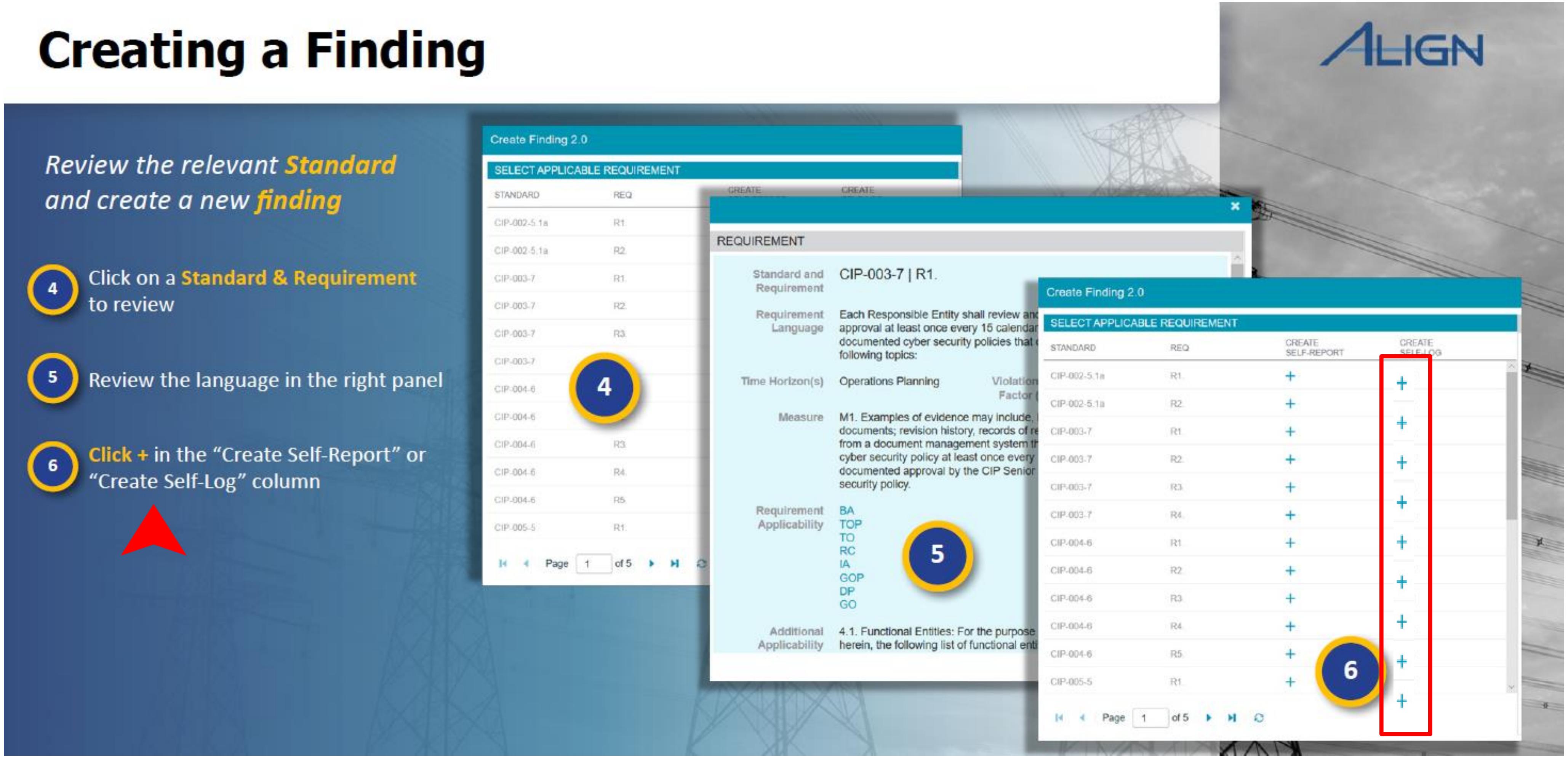
This is the Registered Entity Self Reporting and Logging page. On the left, you can view a set of R Registration. Based on that, you can browse to a specific Requirement and create a Self Report (o program). Below you can edit any draft Self Reports or Logs you have not yet submitted. To see th progress, select the **Enforcement Processing** activity from the pull-down on the upper left.

MY DRAFTS

TYPE	UNIQUE ID	REGISTRATION	STANDARD AND REQUIREMENT	APPLICABLE FUNCTIONS	REGION(S) AND JURISDICTION	START
Self-Report	2020-00134	TEST00200 - TEST00200-RF in RF	PRC-005-6 R3.	GO	RF-US	04/15/2

Page

Creating a Self-Log Finding



Creating a Finding

*Review the relevant **Standard** and create a new **finding***

4 Click on a **Standard & Requirement** to review

5 Review the language in the right panel

6 **Click +** in the "Create Self-Report" or "Create Self-Log" column

Create Finding 2.0

SELECT APPLICABLE REQUIREMENT

STANDARD	REQ	CREATE	CREATE
CIP-002-5.1a	R1.		
CIP-002-5.1a	R2.		
CIP-003-7	R1.		
CIP-003-7	R2.		
CIP-003-7	R3.		
CIP-003-7			
CIP-004-6			
CIP-004-6			
CIP-004-6	R3.		
CIP-004-6	R4.		
CIP-004-6	R5.		
CIP-005-5	R1.		

Page 1 of 5

REQUIREMENT

Standard and Requirement: CIP-003-7 | R1.

Requirement Language: Each Responsible Entity shall review and approval at least once every 15 calendar documented cyber security policies that following topics:

Time Horizon(s): Operations Planning

Violation Factor

Measure: M1. Examples of evidence may include, documents; revision history, records of re from a document management system th cyber security policy at least once every documented approval by the CIP Senior security policy.

Requirement Applicability: BA
TOP
TO
RC
IA
GOP
DP
GO

Additional Applicability: 4.1. Functional Entities: For the purpose herein, the following list of functional enti

Create Finding 2.0

SELECT APPLICABLE REQUIREMENT

STANDARD	REQ	CREATE SELF-REPORT	CREATE SELF-LOG
CIP-002-5.1a	R1.	+	+
CIP-002-5.1a	R2.	+	+
CIP-003-7	R1.	+	+
CIP-003-7	R2.	+	+
CIP-003-7	R3.	+	+
CIP-003-7	R4.	+	+
CIP-004-6	R1.	+	+
CIP-004-6	R2.	+	+
CIP-004-6	R3.	+	+
CIP-004-6	R4.	+	+
CIP-004-6	R5.	+	+
CIP-005-5	R1.	+	+

Page 1 of 5

Creating a Self-Log Finding

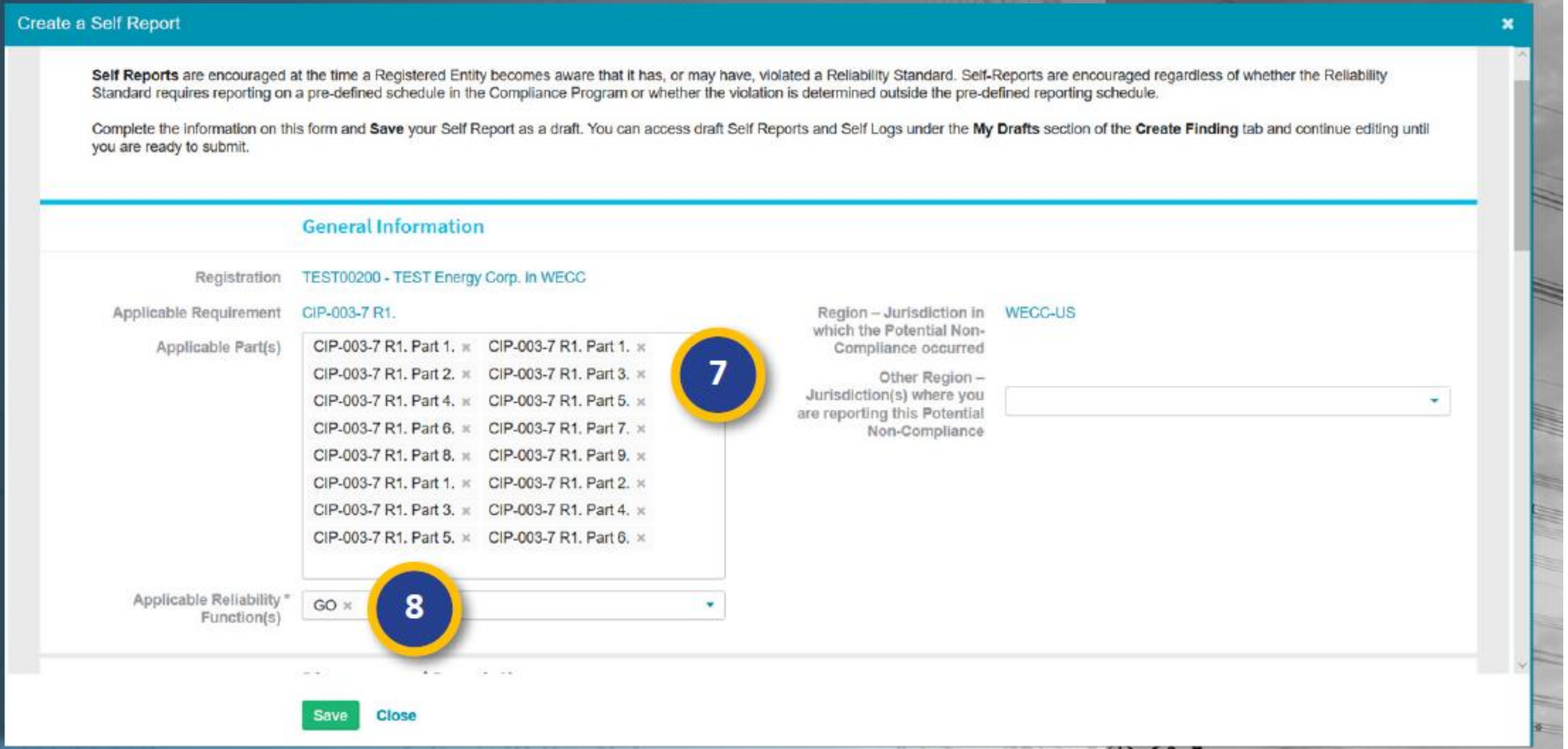
Creating a Finding

Ensure the ***Requirement Parts*** *and* ***Reliability Functions*** *are applicable for the Self-Report.*

Remove any Parts or Functions that do not apply.

7 Click **X** to remove Applicable Parts

8 Click **X** to remove any Reliability Functions



Create a Self Report ✖

Self Reports are encouraged at the time a Registered Entity becomes aware that it has, or may have, violated a Reliability Standard. Self-Reports are encouraged regardless of whether the Reliability Standard requires reporting on a pre-defined schedule in the Compliance Program or whether the violation is determined outside the pre-defined reporting schedule.

Complete the information on this form and **Save** your Self Report as a draft. You can access draft Self Reports and Self Logs under the **My Drafts** section of the **Create Finding** tab and continue editing until you are ready to submit.

General Information

Registration: TEST00200 - TEST Energy Corp. in WECC

Applicable Requirement: CIP-003-7 R1.

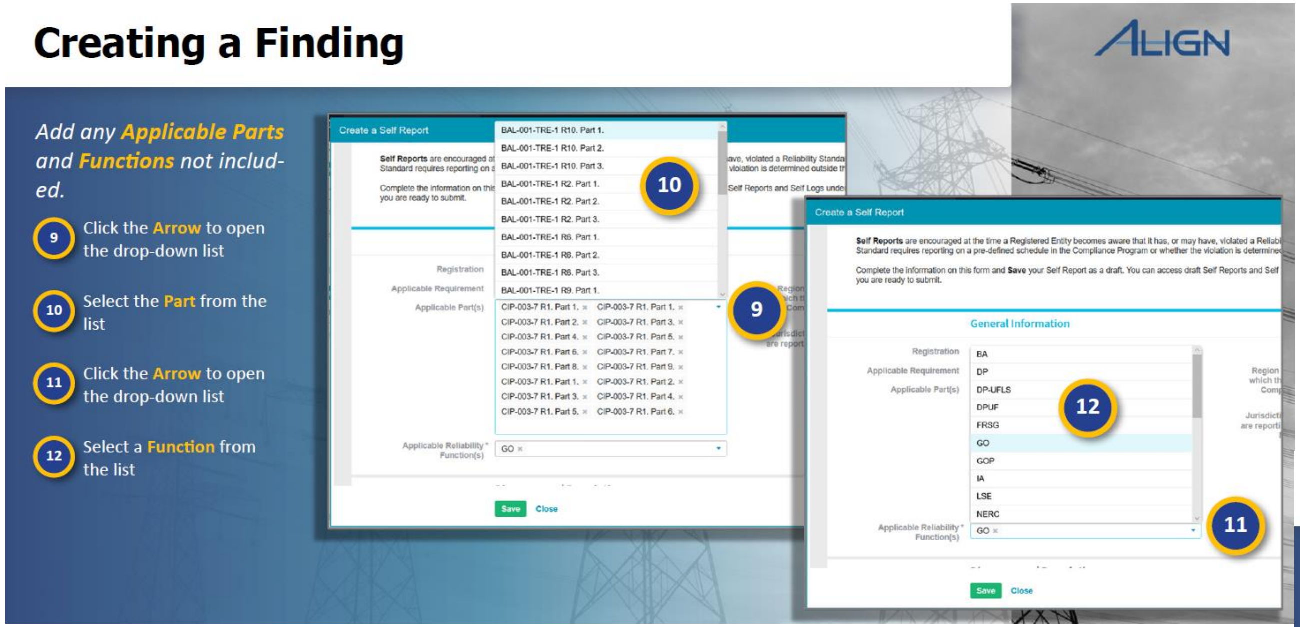
Applicable Part(s): CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 2. × CIP-003-7 R1. Part 3. × CIP-003-7 R1. Part 4. × CIP-003-7 R1. Part 5. × CIP-003-7 R1. Part 6. × CIP-003-7 R1. Part 7. × CIP-003-7 R1. Part 8. × CIP-003-7 R1. Part 9. × CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 2. × CIP-003-7 R1. Part 3. × CIP-003-7 R1. Part 4. × CIP-003-7 R1. Part 5. × CIP-003-7 R1. Part 6. ×

Applicable Reliability* Function(s): GO ×

Region – Jurisdiction in which the Potential Non-Compliance occurred: WECC-US

Other Region – Jurisdiction(s) where you are reporting this Potential Non-Compliance:

Creating a Self-Log Finding



Creating a Finding

*Add any **Applicable Parts** and **Functions** not included.*

9 Click the **Arrow** to open the drop-down list

10 Select the **Part** from the list

11 Click the **Arrow** to open the drop-down list

12 Select a **Function** from the list

Create a Self Report

Self Reports are encouraged at … ave, violated a Reliability Standa… Standard requires reporting on a … violation is determined outside th…

Complete the information on this … Self Reports and Self Logs unde… you are ready to submit.

Registration

Applicable Requirement

Applicable Part(s): CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 2. × CIP-003-7 R1. Part 3. × CIP-003-7 R1. Part 4. × CIP-003-7 R1. Part 5. × CIP-003-7 R1. Part 6. × CIP-003-7 R1. Part 7. × CIP-003-7 R1. Part 8. × CIP-003-7 R1. Part 9. × CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 2. × CIP-003-7 R1. Part 3. × CIP-003-7 R1. Part 4. × CIP-003-7 R1. Part 5. × CIP-003-7 R1. Part 6. ×

Applicable Reliability * Function(s): GO ×

BAL-001-TRE-1 R10. Part 1.
BAL-001-TRE-1 R10. Part 2.
BAL-001-TRE-1 R10. Part 3.
BAL-001-TRE-1 R2. Part 1.
BAL-001-TRE-1 R2. Part 2.
BAL-001-TRE-1 R2. Part 3.
BAL-001-TRE-1 R6. Part 1.
BAL-001-TRE-1 R6. Part 2.
BAL-001-TRE-1 R6. Part 3.
BAL-001-TRE-1 R9. Part 1.

Save Close

Create a Self Report

Self Reports are encouraged at the time a Registered Entity becomes aware that it has, or may have, violated a Reliabi… Standard requires reporting on a pre-defined schedule in the Compliance Program or whether the violation is determine…

Complete the information on this form and **Save** your Self Report as a draft. You can access draft Self Reports and Self … you are ready to submit.

General Information

Registration

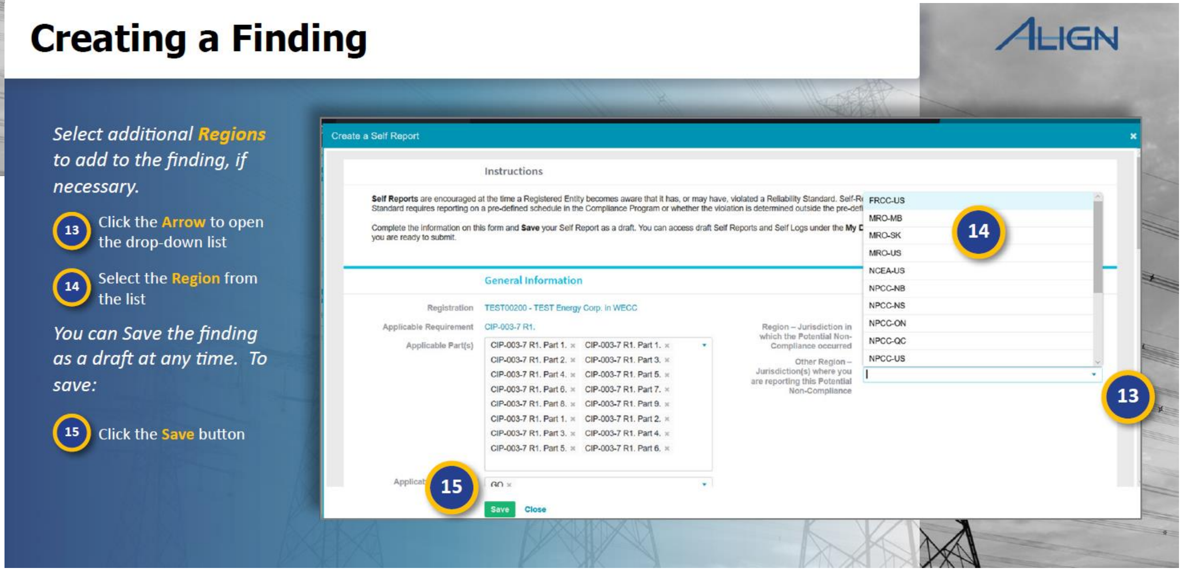
Applicable Requirement

Applicable Part(s)

BA
DP
DP-UFLS
DPUF
FRSG
GO
GOP
IA
LSE
NERC

Applicable Reliability * Function(s): GO ×

Save Close



Creating a Finding

*Select additional **Regions** to add to the finding, if necessary.*

13 Click the **Arrow** to open the drop-down list

14 Select the **Region** from the list

You can Save the finding as a draft at any time. To save:

15 Click the **Save** button

Create a Self Report ×

Instructions

Self Reports are encouraged at the time a Registered Entity becomes aware that it has, or may have, violated a Reliability Standard. Self-R… Standard requires reporting on a pre-defined schedule in the Compliance Program or whether the violation is determined outside the pre-def…

Complete the information on this form and **Save** your Self Report as a draft. You can access draft Self Reports and Self Logs under the **My D…** you are ready to submit.

General Information

Registration: TEST00200 - TEST Energy Corp. in WECC

Applicable Requirement: CIP-003-7 R1.

Applicable Part(s): CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 2. × CIP-003-7 R1. Part 3. × CIP-003-7 R1. Part 4. × CIP-003-7 R1. Part 5. × CIP-003-7 R1. Part 6. × CIP-003-7 R1. Part 7. × CIP-003-7 R1. Part 8. × CIP-003-7 R1. Part 9. × CIP-003-7 R1. Part 1. × CIP-003-7 R1. Part 2. × CIP-003-7 R1. Part 3. × CIP-003-7 R1. Part 4. × CIP-003-7 R1. Part 5. × CIP-003-7 R1. Part 6. ×

Applicab…: GO ×

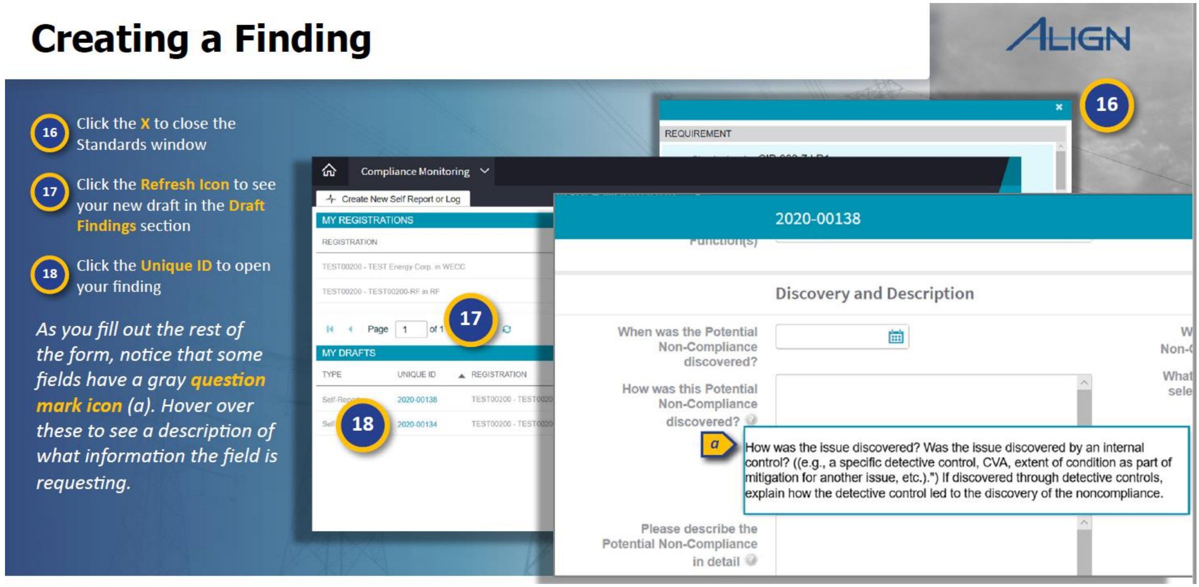
Region – Jurisdiction in which the Potential Non-Compliance occurred

Other Region – Jurisdiction(s) where you are reporting this Potential Non-Compliance

FRCC-US
MRO-MB
MRO-SK
MRO-US
NCEA-US
NPCC-NB
NPCC-NS
NPCC-ON
NPCC-QC
NPCC-US

Save Close

Creating a Self-Log Finding



Creating a Finding

16 Click the X to close the Standards window

17 Click the Refresh Icon to see your new draft in the Draft Findings section

18 Click the Unique ID to open your finding

As you fill out the rest of the form, notice that some fields have a gray question mark icon (a). Hover over these to see a description of what information the field is requesting.

TEST00200 - TEST Energy Corp. in WECC

TEST00200 - TEST00200-RF in RF

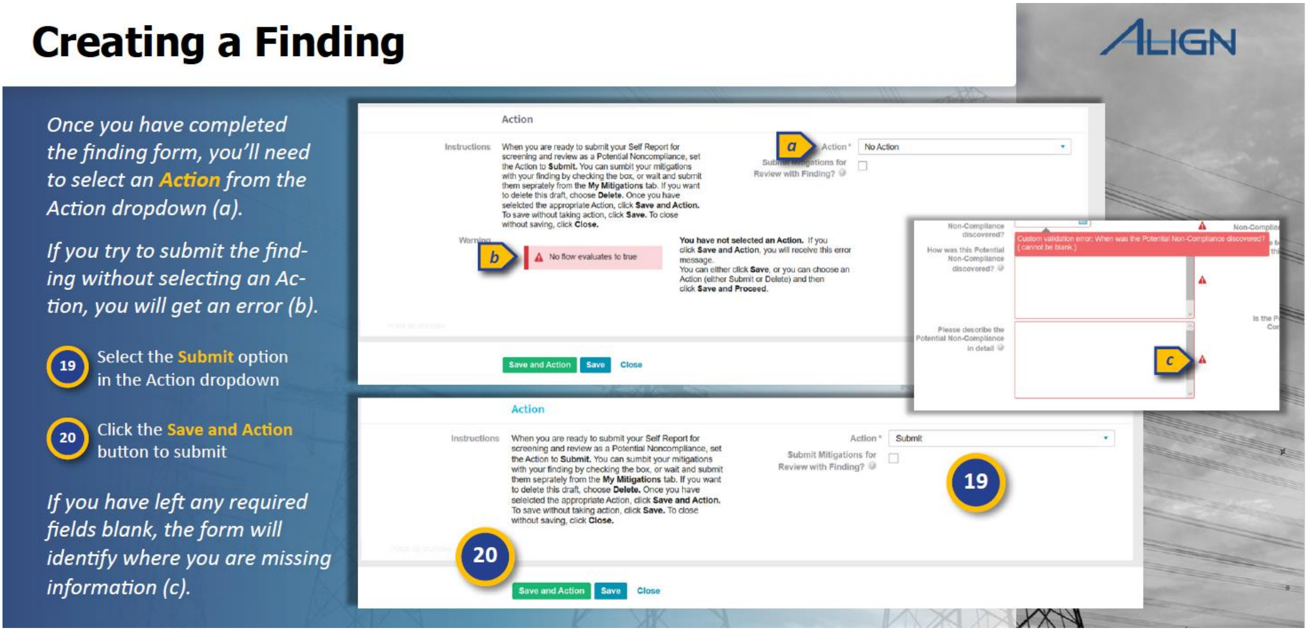
TYPE	UNIQUE ID	REGISTRATION
Self-Rep	2020-00138	TEST00200 - TEST0020
Self	2020-00134	TEST00200 - TEST0020

When was the Potential Non-Compliance discovered?

How was this Potential Non-Compliance discovered?

How was the issue discovered? Was the issue discovered by an internal control? ((e.g., a specific detective control, CVA, extent of condition as part of mitigation for another issue, etc.).") If discovered through detective controls, explain how the detective control led to the discovery of the noncompliance.

Please describe the Potential Non-Compliance in detail



Creating a Finding

Once you have completed the finding form, you'll need to select an Action from the Action dropdown (a).

If you try to submit the finding without selecting an Action, you will get an error (b).

19 Select the Submit option in the Action dropdown

20 Click the Save and Action button to submit

If you have left any required fields blank, the form will identify where you are missing information (c).

Instructions: When you are ready to submit your Self Report for screening and review as a Potential Noncompliance, set the Action to **Submit.** You can sumbit your mitigations with your finding by checking the box, or wait and submit them seprately from the **My Mitigations** tab. If you want to delete this draft, choose **Delete.** Once you have seleicted the appropriate Action, click **Save and Action.** To save without taking action, click **Save.** To close without saving, click **Close.**

Action*: No Action

Submit Mitigations for Review with Finding? □

Warning: No flow evaluates to true

You have not selected an Action. If you click **Save and Action**, you will receive this error message.
You can either click **Save**, or you can choose an Action (either Submit or Delete) and then click **Save and Proceed.**

Non-Compliance discovered?

Custom validation error: When was the Potential Non-Compliance discovered? (cannot be blank)

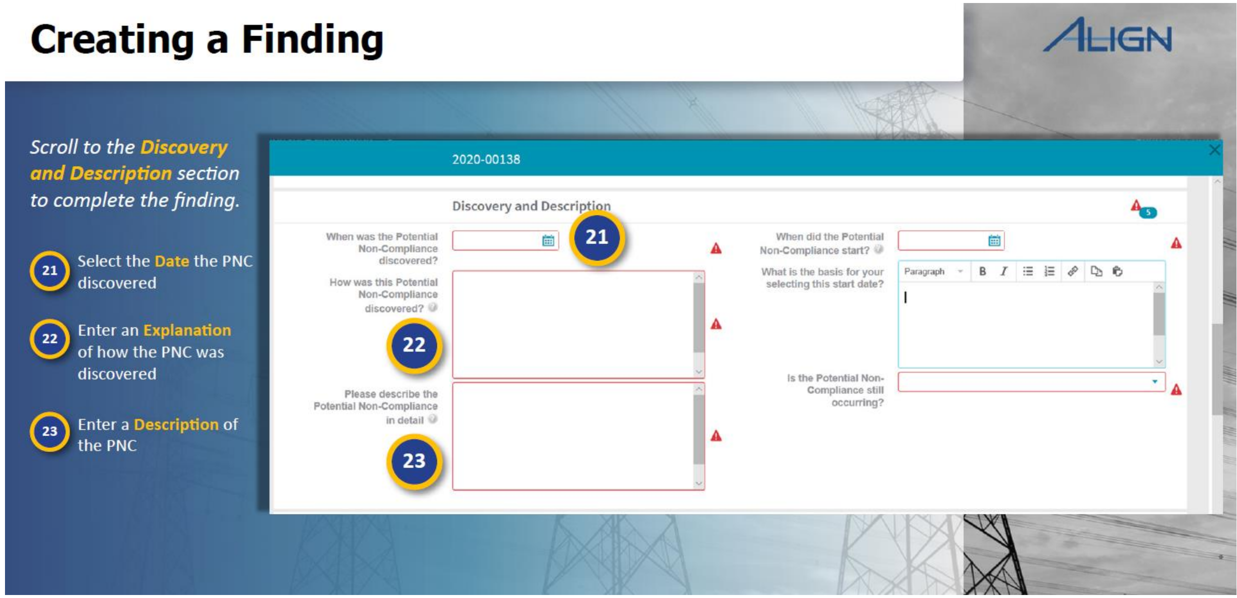
How was this Potential Non-Compliance discovered?

Please describe the Potential Non-Compliance in detail

Action*: Submit

Submit Mitigations for Review with Finding? □

Creating a Self-Log Finding



Creating a Finding

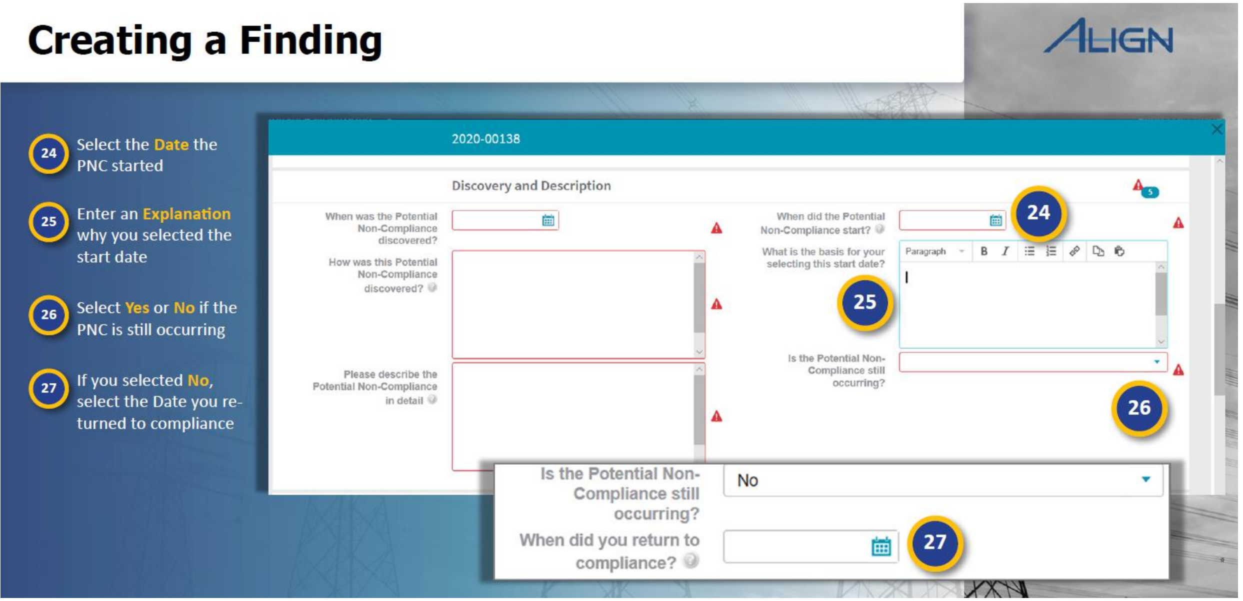
*Scroll to the **Discovery and Description** section to complete the finding.*

21 Select the **Date** the PNC discovered

22 Enter an **Explanation** of how the PNC was discovered

23 Enter a **Description** of the PNC

ALIGN
2020-00138
Discovery and Description
When was the Potential Non-Compliance discovered?
21
How was this Potential Non-Compliance discovered?
22
Please describe the Potential Non-Compliance in detail
23
When did the Potential Non-Compliance start?
What is the basis for your selecting this start date?
Paragraph
B
I
Is the Potential Non-Compliance still occurring?
5



Creating a Finding

24 Select the **Date** the PNC started

25 Enter an **Explanation** why you selected the start date

26 Select **Yes** or **No** if the PNC is still occurring

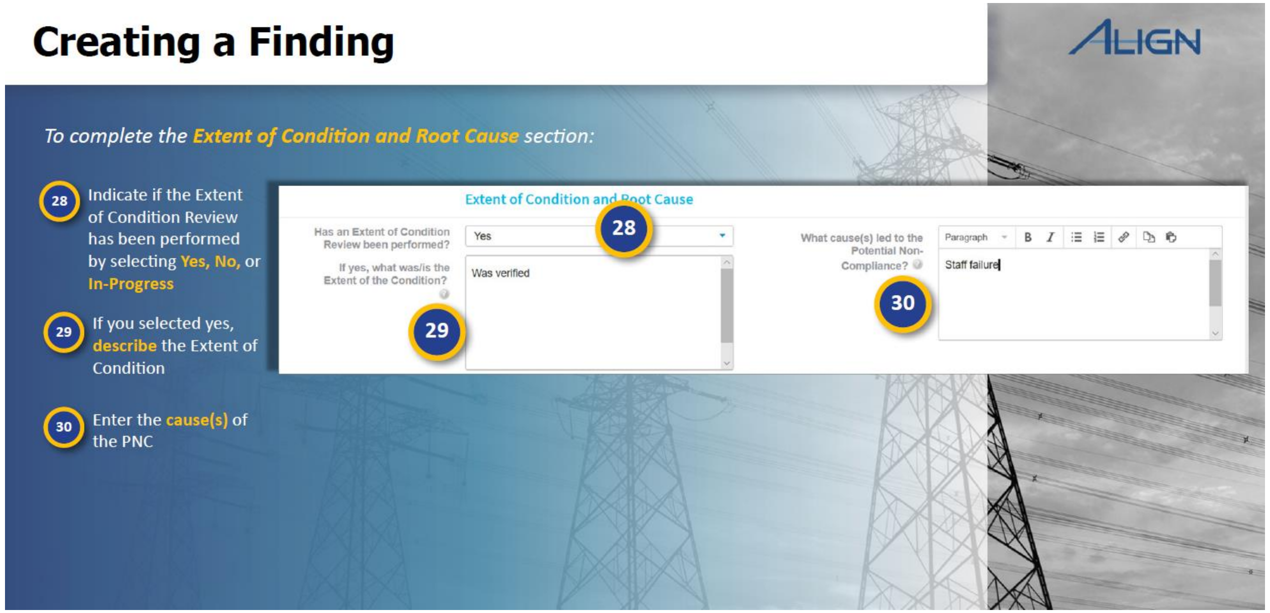
27 If you selected **No**, select the Date you re-turned to compliance

Is the Potential Non-Compliance still occurring? No

When did you return to compliance?

ALIGN
2020-00138
Discovery and Description
When was the Potential Non-Compliance discovered?
How was this Potential Non-Compliance discovered?
Please describe the Potential Non-Compliance in detail
When did the Potential Non-Compliance start?
24
What is the basis for your selecting this start date?
Paragraph
B
I
25
Is the Potential Non-Compliance still occurring?
26
27
5

Creating a Self-Log Finding



Creating a Finding

*To complete the **Extent of Condition and Root Cause** section:*

28 Indicate if the Extent of Condition Review has been performed by selecting **Yes**, **No**, or **In-Progress**

29 If you selected yes, **describe** the Extent of Condition

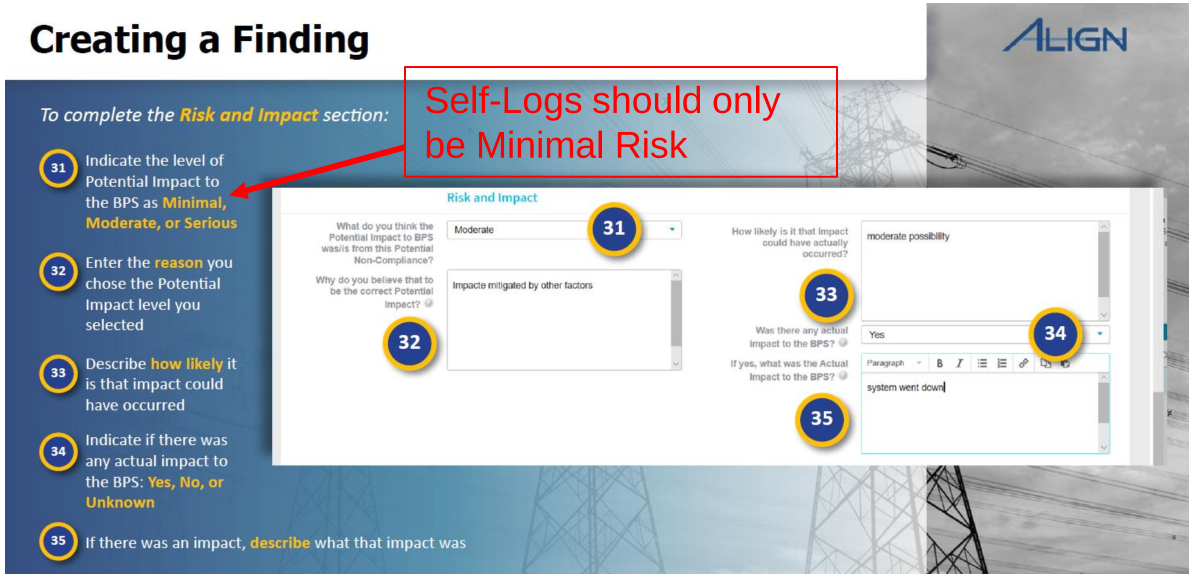
30 Enter the **cause(s)** of the PNC

Extent of Condition and Root Cause

Has an Extent of Condition Review been performed? Yes (28)

If yes, what was/is the Extent of the Condition? Was verified (29)

What cause(s) led to the Potential Non-Compliance? Staff failure (30)



Creating a Finding

*To complete the **Risk and Impact** section:*

Self-Logs should only be Minimal Risk

31 Indicate the level of Potential Impact to the BPS as **Minimal, Moderate, or Serious**

32 Enter the **reason** you chose the Potential Impact level you selected

33 Describe **how likely** it is that impact could have occurred

34 Indicate if there was any actual impact to the BPS: **Yes, No, or Unknown**

35 If there was an impact, **describe** what that impact was

Risk and Impact

What do you think the Potential Impact to BPS was/is from this Potential Non-Compliance? Moderate (31)

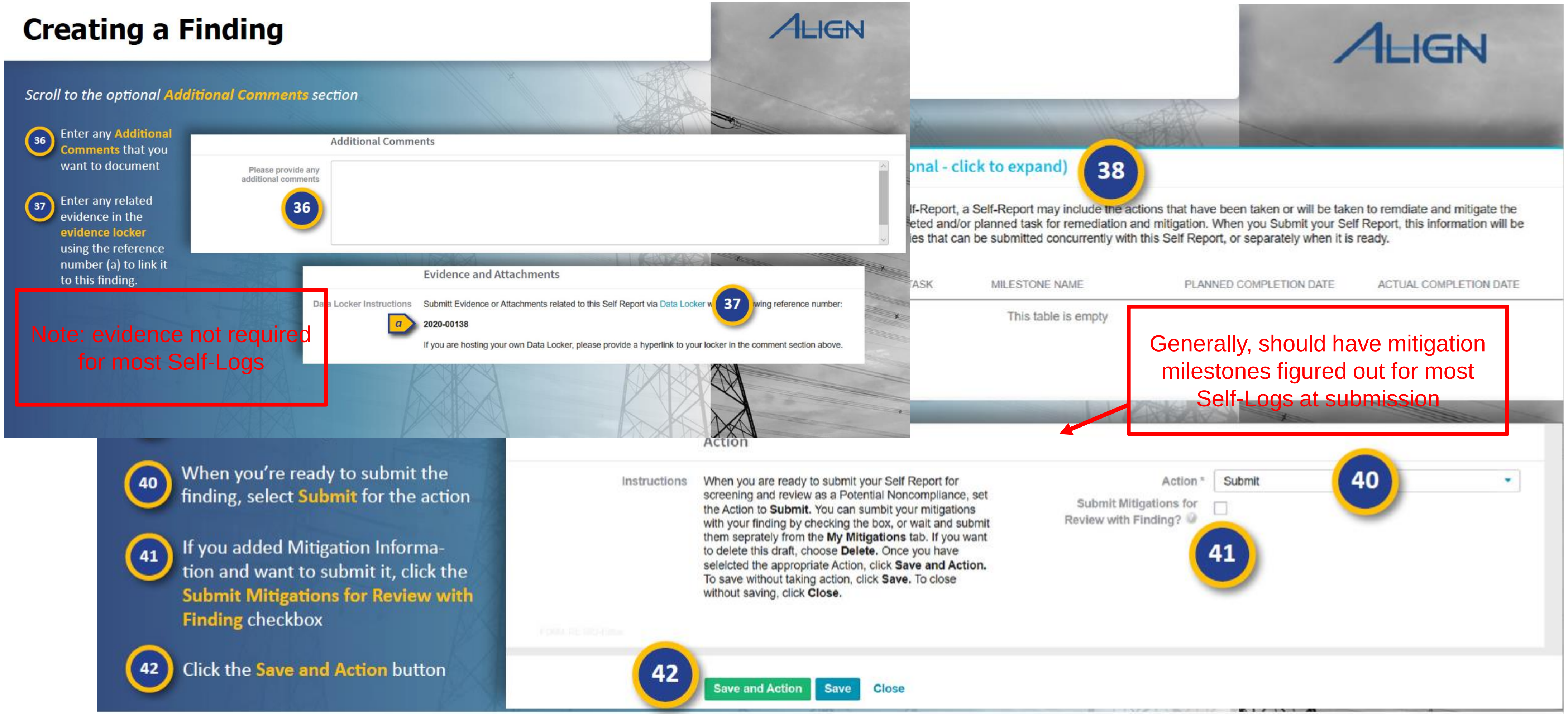
Why do you believe that to be the correct Potential Impact? Impacte mitigated by other factors (32)

How likely is it that Impact could have actually occurred? moderate possibility (33)

Was there any actual impact to the BPS? Yes (34)

If yes, what was the Actual Impact to the BPS? system went down (35)

Creating a Self-Log Finding



Creating a Finding

*Scroll to the optional **Additional Comments** section*

36 Enter any **Additional Comments** that you want to document

37 Enter any related evidence in the **evidence locker** using the reference number (a) to link it to this finding.

Note: evidence not required for most Self-Logs

Additional Comments

Please provide any additional comments

Evidence and Attachments

Da a Locker Instructions

Submitt Evidence or Attachments related to this Self Report via Data Locker w wing reference number:

a 2020-00138

If you are hosting your own Data Locker, please provide a hyperlink to your locker in the comment section above.

onal - click to expand) 38

lf-Report, a Self-Report may include the actions that have been taken or will be taken to remdiate and mitigate the eted and/or planned task for remediation and mitigation. When you Submit your Self Report, this information will be es that can be submitted concurrently with this Self Report, or separately when it is ready.

ASK	MILESTONE NAME	PLANNED COMPLETION DATE	ACTUAL COMPLETION DATE
	This table is empty		

Generally, should have mitigation milestones figured out for most Self-Logs at submission

40 When you're ready to submit the finding, select **Submit** for the action

41 If you added Mitigation Information and want to submit it, click the **Submit Mitigations for Review with Finding** checkbox

42 Click the **Save and Action** button

Action

Instructions: When you are ready to submit your Self Report for screening and review as a Potential Noncompliance, set the Action to **Submit.** You can sumbit your mitigations with your finding by checking the box, or wait and submit them seprately from the **My Mitigations** tab. If you want to delete this draft, choose **Delete.** Once you have seleicted the appropriate Action, click **Save and Action.** To save without taking action, click **Save.** To close without saving, click **Close.**

Action *: Submit

Submit Mitigations for Review with Finding? □

How to Use the Program Effectively

Enter each instance into log when identified

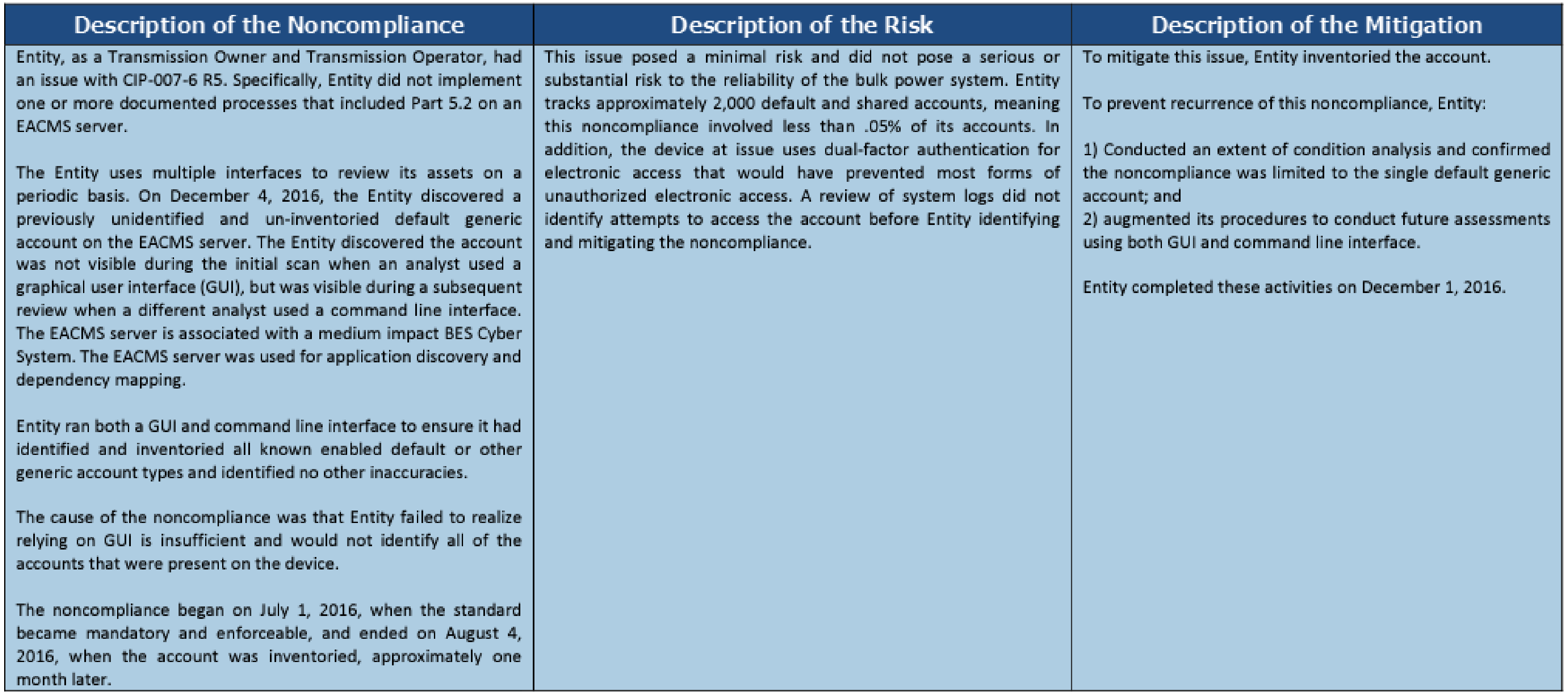
- If multiple instances of same standard over time, possible to consolidate when processed for CE treatment
- Too many similar instances in a small amount of time may reduce chances of eligibility

Log should tell a complete story

Direct relationship between cause, minimal risk, and mitigating activities

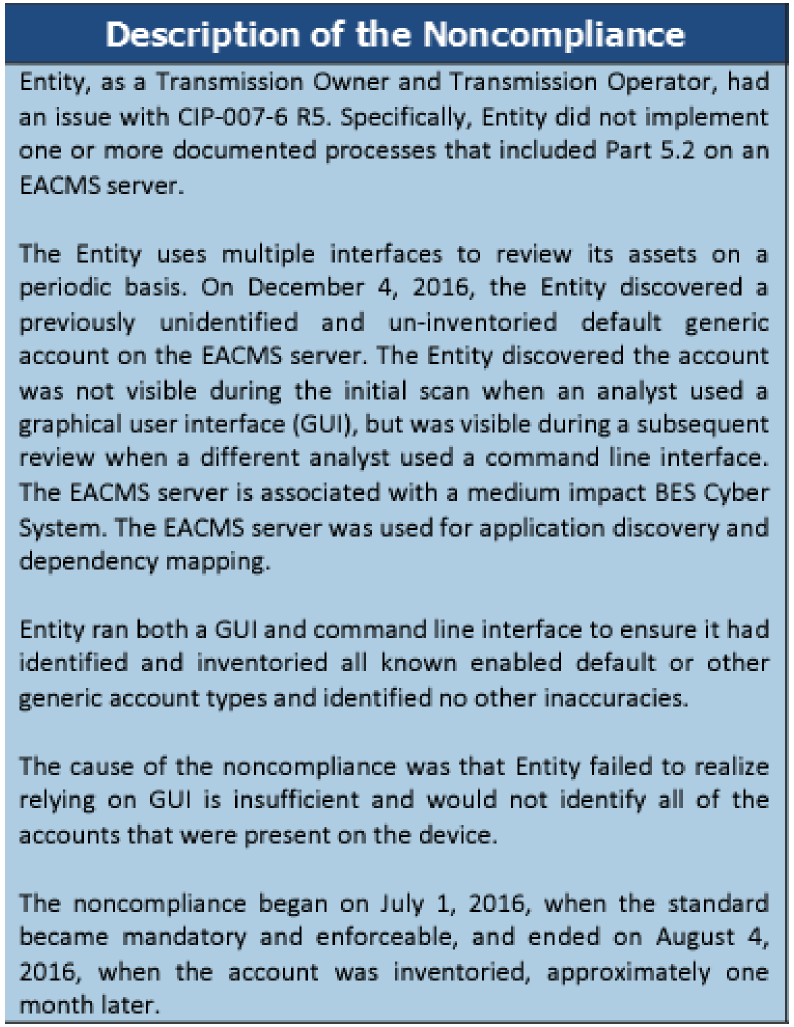
Ideally, minimal review and editing of material needed before posting as a CE

Submission Example



Description of the Noncompliance	Description of the Risk	Description of the Mitigation
Entity, as a Transmission Owner and Transmission Operator, had an issue with CIP-007-6 R5. Specifically, Entity did not implement one or more documented processes that included Part 5.2 on an EACMS server. The Entity uses multiple interfaces to review its assets on a periodic basis. On December 4, 2016, the Entity discovered a previously unidentified and un-inventoried default generic account on the EACMS server. The Entity discovered the account was not visible during the initial scan when an analyst used a graphical user interface (GUI), but was visible during a subsequent review when a different analyst used a command line interface. The EACMS server is associated with a medium impact BES Cyber System. The EACMS server was used for application discovery and dependency mapping. Entity ran both a GUI and command line interface to ensure it had identified and inventoried all known enabled default or other generic account types and identified no other inaccuracies. The cause of the noncompliance was that Entity failed to realize relying on GUI is insufficient and would not identify all of the accounts that were present on the device. The noncompliance began on July 1, 2016, when the standard became mandatory and enforceable, and ended on August 4, 2016, when the account was inventoried, approximately one month later.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Entity tracks approximately 2,000 default and shared accounts, meaning this noncompliance involved less than .05% of its accounts. In addition, the device at issue uses dual-factor authentication for electronic access that would have prevented most forms of unauthorized electronic access. A review of system logs did not identify attempts to access the account before Entity identifying and mitigating the noncompliance.	To mitigate this issue, Entity inventoried the account. To prevent recurrence of this noncompliance, Entity: 1) Conducted an extent of condition analysis and confirmed the noncompliance was limited to the single default generic account; and 2) augmented its procedures to conduct future assessments using both GUI and command line interface. Entity completed these activities on December 1, 2016.

How to Use the Program Effectively



Description of the Noncompliance

Entity, as a Transmission Owner and Transmission Operator, had an issue with CIP-007-6 R5. Specifically, Entity did not implement one or more documented processes that included Part 5.2 on an EACMS server.

The Entity uses multiple interfaces to review its assets on a periodic basis. On December 4, 2016, the Entity discovered a previously unidentified and un-inventoried default generic account on the EACMS server. The Entity discovered the account was not visible during the initial scan when an analyst used a graphical user interface (GUI), but was visible during a subsequent review when a different analyst used a command line interface. The EACMS server is associated with a medium impact BES Cyber System. The EACMS server was used for application discovery and dependency mapping.

Entity ran both a GUI and command line interface to ensure it had identified and inventoried all known enabled default or other generic account types and identified no other inaccuracies.

The cause of the noncompliance was that Entity failed to realize relying on GUI is insufficient and would not identify all of the accounts that were present on the device.

The noncompliance began on July 1, 2016, when the standard became mandatory and enforceable, and ended on August 4, 2016, when the account was inventoried, approximately one month later.

Standard at issue

Discovery, description of issue

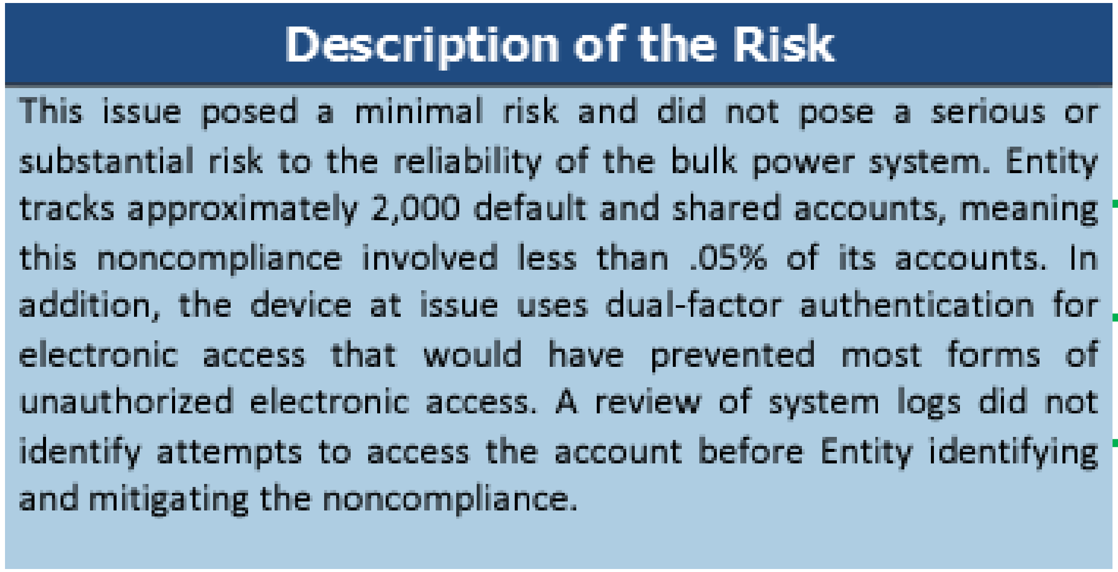
Description of asset at issue

Extent of Condition

Root Cause

Description of start and end dates

How to Use the Program Effectively



Description of the Risk

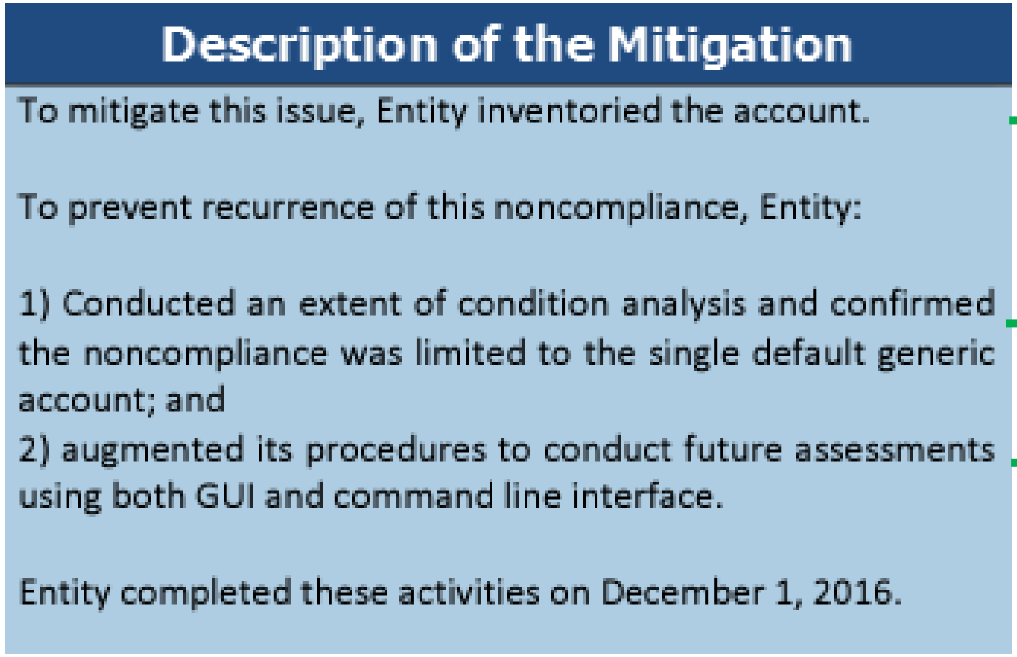
This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Entity tracks approximately 2,000 default and shared accounts, meaning this noncompliance involved less than .05% of its accounts. In addition, the device at issue uses dual-factor authentication for electronic access that would have prevented most forms of unauthorized electronic access. A review of system logs did not identify attempts to access the account before Entity identifying and mitigating the noncompliance.

Scope

Mitigating Factors

No actual harm

How to Use the Program Effectively



Description of the Mitigation

To mitigate this issue, Entity inventoried the account.

To prevent recurrence of this noncompliance, Entity:

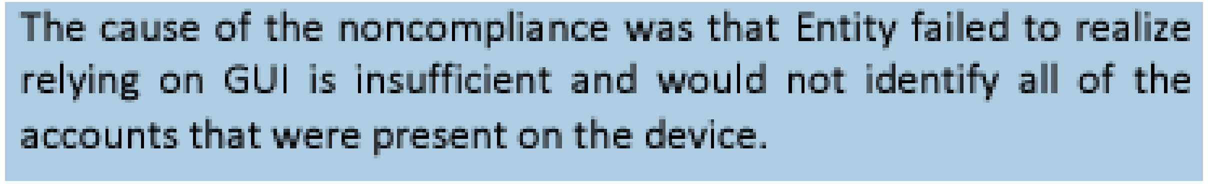
1) Conducted an extent of condition analysis and confirmed the noncompliance was limited to the single default generic account; and
2) augmented its procedures to conduct future assessments using both GUI and command line interface.

Entity completed these activities on December 1, 2016.

Fixed noncompliance issue

Ensured no other similar issues currently exist

Steps taken to ensure same issue doesn't happen again - corrects root cause



The cause of the noncompliance was that Entity failed to realize relying on GUI is insufficient and would not identify all of the accounts that were present on the device.

What Not to Log

Examples of What Cannot Be Logged:

- Noncompliance posing moderate or greater risk
- Loss of load
- Instability to the BPS
- Uncontrolled separation
- Cascading blackouts
- Vegetation contacts causing extended outages
- Systemic or significant performance failures
- Intentional or willful acts/omissions
- Gross negligence

What Not to Log

More *Nuanced* Examples of What Cannot Be Logged:

- If reasonable experts could disagree on the risk

- If there is a compliance history *with the same root cause where previous mitigation should have prevented reoccurrence*

Self-Logging Challenges

Examples of Challenges with Self-Logs:

No preventative mitigation activities

Only listing “human error” as a root cause

Lack of discovery information

Too many similar cases filed in a short period

Contact

Alex Petak
alex.petak@texasre.org
(512) 583-4913

Mishani Tamayo
mishani.tamayo@texasre.org
(512) 583-4993

Questions?

TEXAS RE

Ensuring electric reliability for Texans