TIBCO LogLogic® Compliance Suite - NERC Edition
Guide

Software Release 3.9.0
November 2017
Document Updated: April 2018

Two-Second Advantage®

TIBCO®

Important Information

This document contains excerpted portions of the North American Electric Reliability Corporation ("NERC") standards (collectively, the "Regulatory Language"). The Regulatory Language is provided by TIBCO solely for your convenience and to provide context for certain functionality of the TIBCO LogLogic® products. The inclusion or omission by TIBCO of any Regulatory Language is in no way intended as legal advice regarding the NERC standards and does not constitute any representation or warranty that any TIBCO products comply with the terms contained in such Regulatory Language. If you have additional questions about the NERC standards, you should consult with an attorney for further legal guidance.

Contents

Figures

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

Product-Specific Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO LogLogic® Compliance Suite - NERC Guide*
- *TIBCO LogLogic® Compliance Suite - NERC Readme*
- *TIBCO LogLogic® Compliance Suite - NERC Release Notes*

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

NERC Background

The North American Electric Reliability Corporation (NERC) is a self-regulatory organization, subject to oversight by the US Federal Energy Regulatory Commission and governmental authorities in Canada. NERC was certified as the Electric Reliability Organization (ERO) on July 20, 2006, by Federal Electric Regulatory Commission. As of June 18, 2007, the US Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce reliability standards with all US users, owners, and operators of the bulk power system, and made compliance with those standards mandatory. Failure to meet the standards and implementation schedules set forth can result in significant financial penalties.

NERC Mission

NERC performs multiple functions.

Functions performed by NERC are as follows:

- Develops and enforces reliability standards
- Assesses adequacy annually via a 10-year forecast and winter and summer forecasts
- Monitors the Bulk Power System
- Educates, trains, and certifies industry personnel

NERC Standards

NERC Standard CIP-001 defines requirements for Sabotage Reporting, which is beyond the scope of this Guidebook. The NERC Standards CIP-002 through CIP-009, covered in this guide, provide a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Specifically, these standards include:

- **CIP-002 - Cyber Security - Critical Cyber Asset Identification:** Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.
- **CIP-003 - Cyber Security - Security Management Controls:** Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002.
- **CIP-004 - Cyber Security - Personnel & Training:** Requires personnel with access to critical cyber assets for identity verification and criminal checks. It also requires employee training.
- **CIP-005 - Cyber Security - Electronic Security Perimeters:** Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002.
- **CIP-006 - Cyber Security - Physical Security of Critical Cyber Assets:** Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.
- **CIP-007 - Cyber Security - Systems Security Management:** Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the noncritical cyber assets within an electronic security perimeter.

- **CIP-008 - Cyber Security - Incident Reporting and Response Planning:** Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.
- **CIP-009 - Cyber Security - Recovery Plans for Critical Cyber Assets:** Requires you to have in place business continuity and disaster recovery plans for critical cyber assets.

NERC states that the CIP reliability standards provide a comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks. They require Bulk-Power System users, owners, and operators to establish a risk-based vulnerability assessment methodology to identify and prioritize critical assets and critical cyber assets.

After the critical cyber assets are identified, the CIP reliability standards require, among other things, that the responsible entities establish plans, protocols, and controls to safeguard physical and electronic access; to train personnel on security matters; to report security incidents; and to be prepared for recovery actions.Standards is provided by TIBCO LogLogic.

The CIP requirements, sub-requirements, and measures outlined in this guidebook are summarized from FERC 18 CFR Part 40, Order No. 706, Mandatory Reliability Standards for Critical Infrastructure Protection and NERC Critical Infrastructure Protection Reliability Standards. The illustrative approaches described under each CIP Standard were obtained from FERC Order No. 706, NERC Security Guidelines for the Electricity Sector, and other resources of common IT risk management best practices. The TIBCO LogLogic solution information described in this guidebook that aligns with the CIP Standards is provided by TIBCO LogLogic.

The Compliance Suite - NERC Edition Guide Objectives

The objective of developing the TIBCO LogLogic Compliance Suite - NERC Edition Guidebook is to provide:

- The necessary background of the NERC CIP requirements and sub-requirements to the IT Network personnel with an illustrative approach
- The technology mapping from the TIBCO LogLogic Solutions to the NERC CIP requirements and sub-requirements in the form of LogLogic® Compliance Suite - NERC Edition

Each of the eight CIP standards addressed in this guide has a specific goal; and the requirements describe a prescriptive approach to be compliant with NERC standards at various levels.

The LogLogic® Compliance Suite - NERC Edition is designed to assist the Responsible Entities (RE) in compliance with these NERC CIP standards requirements by collecting and synthesizing the large amounts of user and system logs.

The Compliance Suite - NERC Edition Guidebook delivers approximately 373 out-of-the-box compliance reports and 140 out-of-the-box alerts with executive-level views.

The following sections of this guide list selected NERC Critical Infrastructure Protection (CIP) mandates and the TIBCO LogLogic reports that help achieve the appropriate compliance level.

TIBCO LogLogic Compliance Suite Setup

Setting up the LogLogic® Compliance Suite - NERC Edition comprises checking that all prerequisites are met before starting the installation process, installing the Compliance Suite file, and enabling the alerts.

See Installing the Compliance Suite and Enabling Compliance Suite Alerts for more details.

Installing the Compliance Suite

Setting up the TIBCO LogLogic Compliance Suite - NERC Edition comprises checking that all prerequisites are met before starting the installation process, installing the Compliance Suite file, and enabling the alerts.

Prerequisites

Before installing the LogLogic® Compliance Suite - NERC Edition, ensure that you have:

- TIBCO LogLogic LX or MX or ST Appliance running LogLogic LMI Release 5.7.x or higher
- TIBCO LogLogic® Log Source Package 32.1 or 33 installed

The Compliance Suite includes one file containing NERC filters, custom reports, and alerts.

- `NERC.xml` – NERC Reports, Search Filters, and Alerts

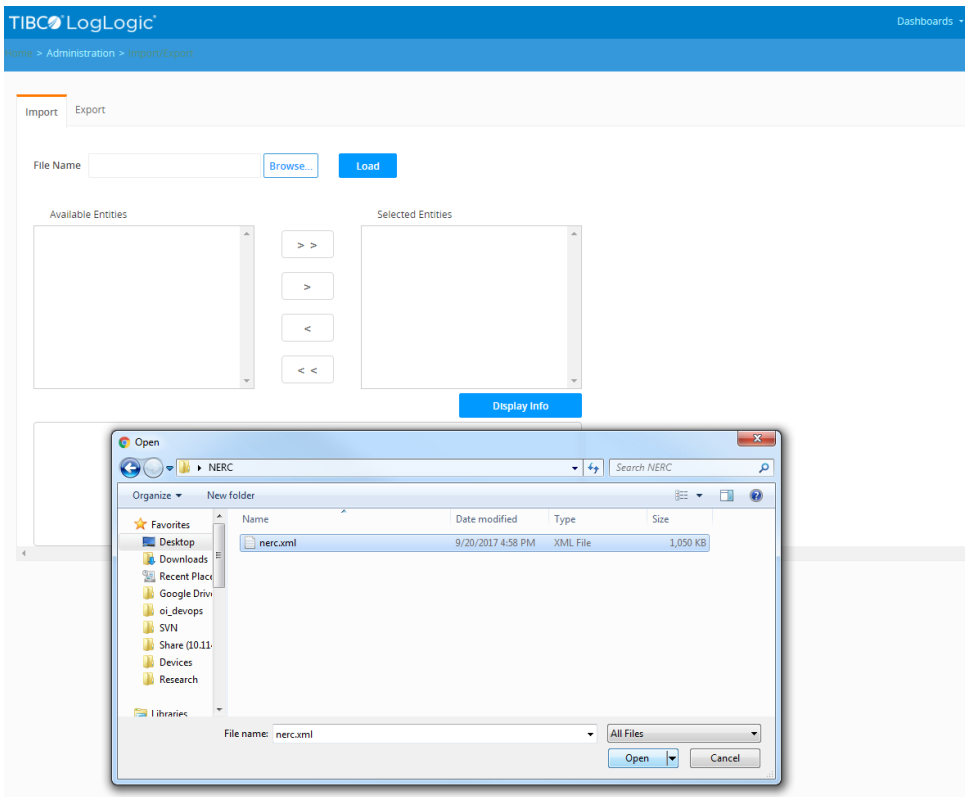
If you have previously imported any earlier versions of the Compliance Suite files, importing this version of the Compliance Suite will not overwrite the original files or any changes that have been made, unless you have saved the changes to the object using the default name.

If you have made any changes to base Compliance Suite alerts, search filters, or custom reports, TIBCO recommends saving these items with non-default names. This will help ensure that the latest Compliance Suite updates can be installed without any compatibility issues or naming conflicts.

Procedure

1. Log in to your TIBCO LogLogic LX or MX or ST appliance as an admin.
2. From the navigation menu, select **Administration** > **Import or Export**.
   The **Import** and **Export** tabs appear.
3. Load the Compliance Suite file by completing the following steps:
   a) On the **Import** tab, click **Browse**.
   b) In the File Upload window, select the appropriate XML file and click **Open**.
   The following figure shows the **File Upload** window that appears after clicking **Browse** on the **Import** tab.

Loading a Compliance Suite File



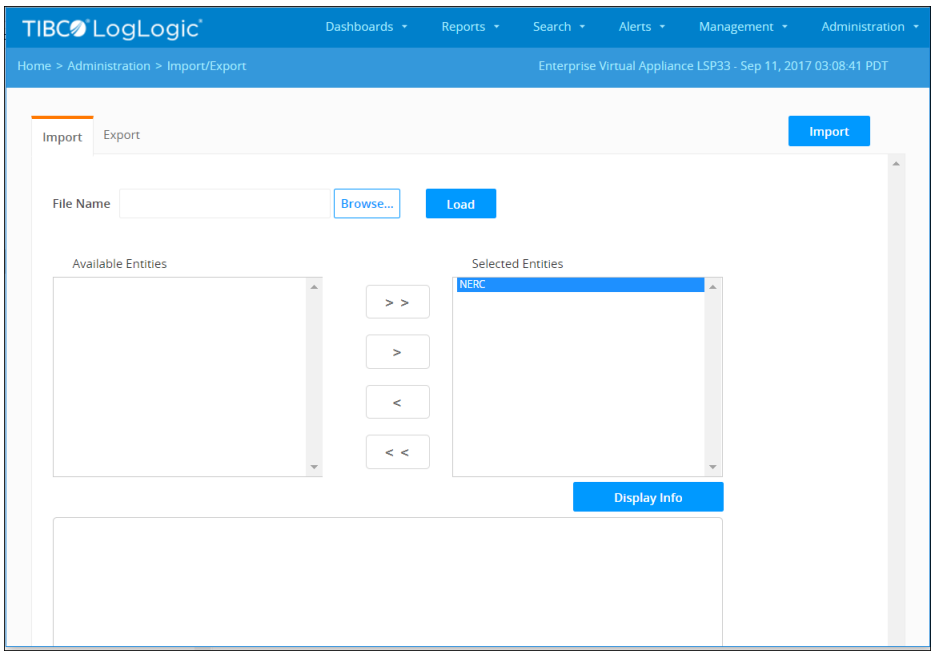
c) Click **Load**.
This loads the **Available Entities** from the XML file.

d) Click **Add All Entities**.

> You can also select specific NERC entities from the Available Entities text block, and then click **Add Selected Entities**.

The following figure shows an entity of the NERC XML file that was selected by clicking **Add All Entities**.

Selected Entities to be Imported



4. Click **Import**.
   A message appears above the **File Name** text field, informing that the import is successfully completed .

   Installation is complete after the XML file is imported successfully.

The Compliance Suite Usage

Once you have successfully installed the LogLogic® Compliance Suite - NERC Edition, you can begin using the custom reports and alerts.

You can view, test, and modify the packaged custom reports and alerts. See Viewing Compliance Suite Reports and Output Data and Customizing Compliance Suite Reports for more details. The custom reports and alerts were designed to run out of the box; however, TIBCO LogLogic enables you to perform further customization if necessary.

The Compliance Suite Reports

All LogLogic® Compliance Suite - NERC Edition reports are designed to run out of the box but are also sufficiently flexible if you need to make modifications based on your business needs.

For a description of all custom reports in this Compliance Suite, see TIBCO LogLogic Reports for NERC.

- To view the compliance suite reports and output data refer Viewing Compliance Suite Reports and Output Data
- To customize the compliance reports refer Customizing Compliance Suite Reports

Viewing Compliance Suite Reports and Output Data

Using TIBCO LogLogic LX or MX or ST Appliance, you can view all the Compliance Suite reports for the device and run them as well as view the output data.

Procedure

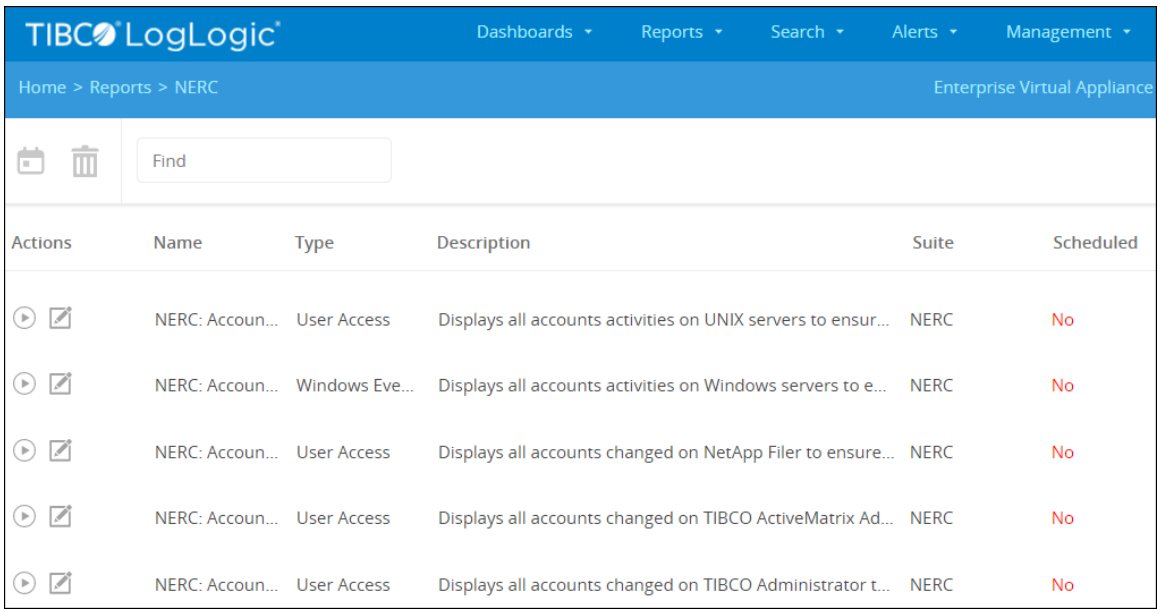
1. Log in to the TIBCO LogLogic LX or MX or ST Appliance as an admin.
2. From the navigation menu, select **Reports** > **NERC** .

   You can also access all of your custom reports on the Appliance, including the Compliance Suite reports you installed, by selecting **Reports** > **All Saved Reports** .
3. On the **Reports** page, you can see all of the custom reports you loaded during the installation process.

   The following figure shows a cropped list of the Compliance Suite reports loaded from the NERC XML file.

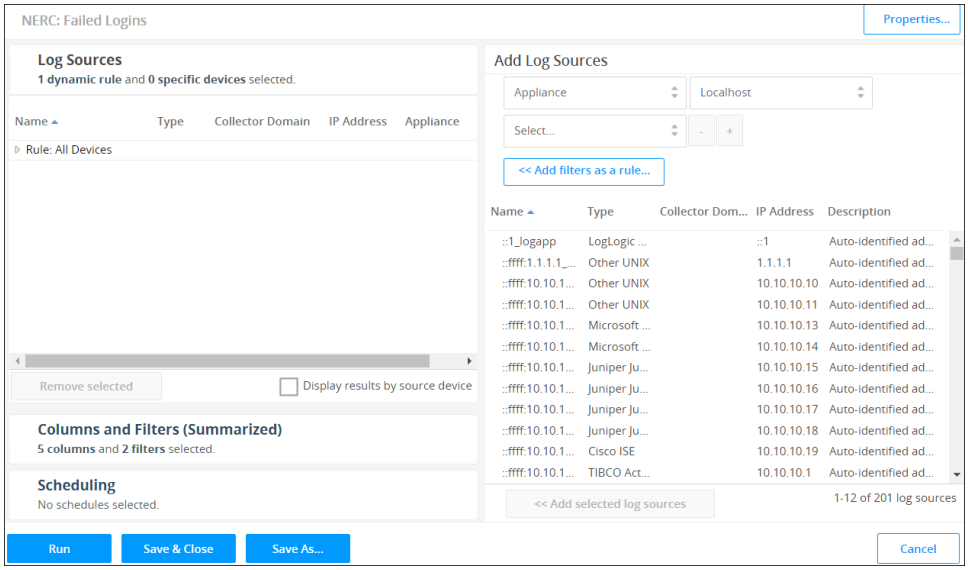
Compliance Suite Reports



4. Click the **Edit** button to see the details. Incorporate all the information in the following substeps:
   a) To view the filter parameters, click **Columns and Filters**.
   b) To view details about a report such as the report name and description, click **Properties**.

   The following figure shows the details of the **NERC: Failed Logins** report.

   Failed Logins Report Details



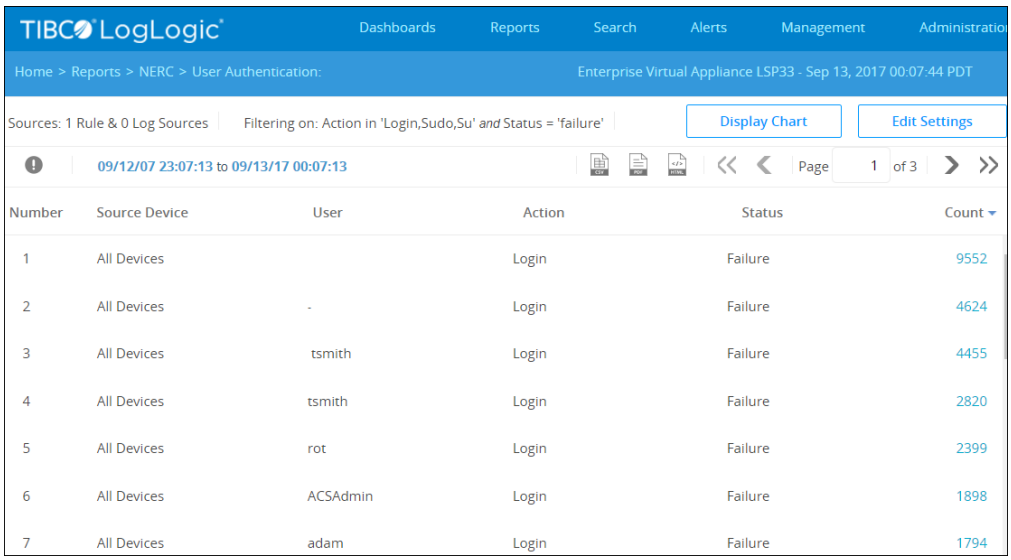
5. Run the report to view the report output data by completing the following steps:
   a) Click **Run**.

   The report runs and returns data based on the set parameters.
   b) To view detailed drill-down information, click the **Count** link.

   You can use the **Back to summarized results** button to return to the main data output view.

   The following figure shows sample results from the **NERC: Failed Logins** report.

Failed Logins Report Results



If you want to modify the main data output view, you can modify the report parameters and then run the report again.

Customizing Compliance Suite Reports

The LogLogic® Compliance Suite - NERC Edition reports are designed to run out of the box to meet specific compliance requirements. However, you may want to modify the reports to include additional information or devices, depending on your business needs.

For more information on how to use and modify custom reports, see to the *TIBCO LogLogic® Log Management Intelligence (LMI) User Guide*.

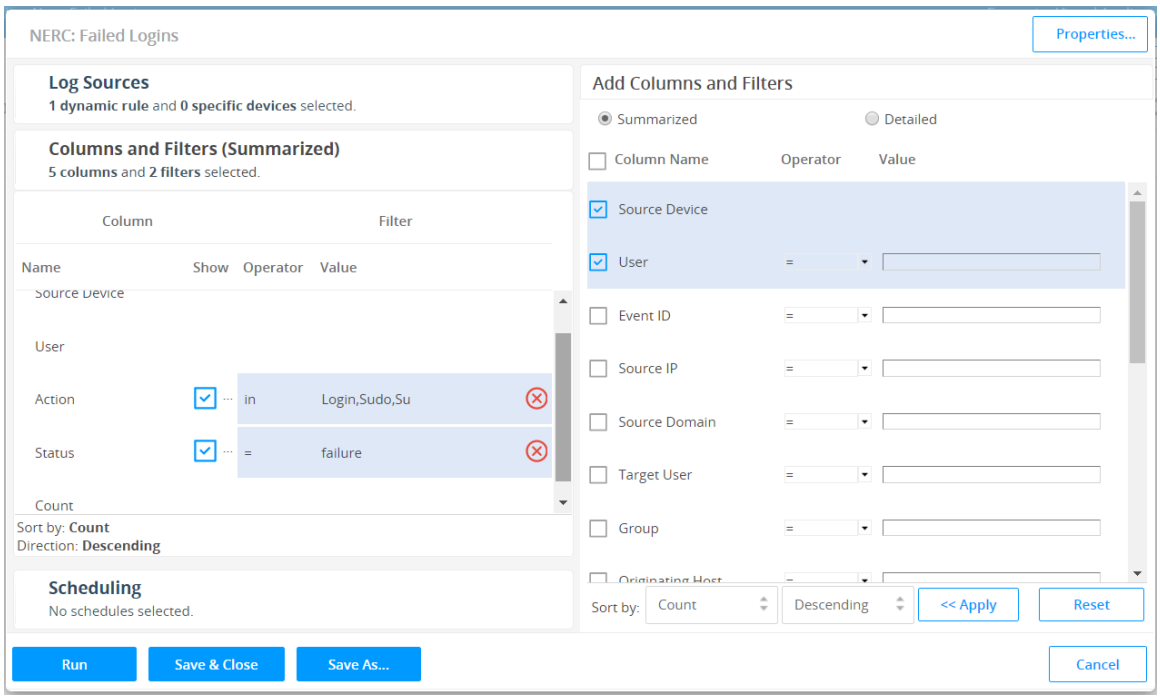
Procedure

1. Ensure that you are on the **Reports** page and click the **Edit** button of a report you want to modify.
2. Modify the report details (for example, name and description), filters, and parameters.

   TIBCO LogLogic enables you to customize everything pertaining to the summarization and presentation of the reports. You can modify the device(s) on which the report runs, schedule when the report runs, and set specific report search filters.

   The following figure shows the report filters available under **Columns and Filters**.

Advanced Options and Update Saved Custom Report Views



It is a good practice to test your modifications to ensure that the report meets your business needs.

3. To test the report, click **Run**.

   The report runs and returns data based on the set parameters. Verify that the returned data is what you want. Continue modifying and testing the report as needed.

4. Save the report by completing the following steps:
   a) Click **Save As**.

      Make any necessary modifications to the report details (for example, **Report Name**, **Report Description**).
   b) Click **Save & Close**.

      A message appears, confirming that the report is saved. Your report is now modified. Consider testing the output of the report to ensure it contains all the data you need from this report.

The Compliance Suite Alerts

The LogLogic® Compliance Suite - NERC Edition alerts enable you to manage activities helping you to maintain NERC compliance. Activities can include detecting unusual traffic on your network or detecting Appliance system anomalies.

By default, the Compliance Suite alerts are disabled so that you can configure your environment with only those alerts that are necessary. For a description of all alerts in this Compliance Suite, see TIBCO LogLogic Alerts for NERC.

- For details on accessing compliance suite alerts, see Accessing Available Compliance Suite Alerts
- For details on the alerts, see Enabling Compliance Suite Alerts
- For details on viewing the alert results, see Viewing Compliance Suite Alert Results

Accessing Available Compliance Suite Alerts

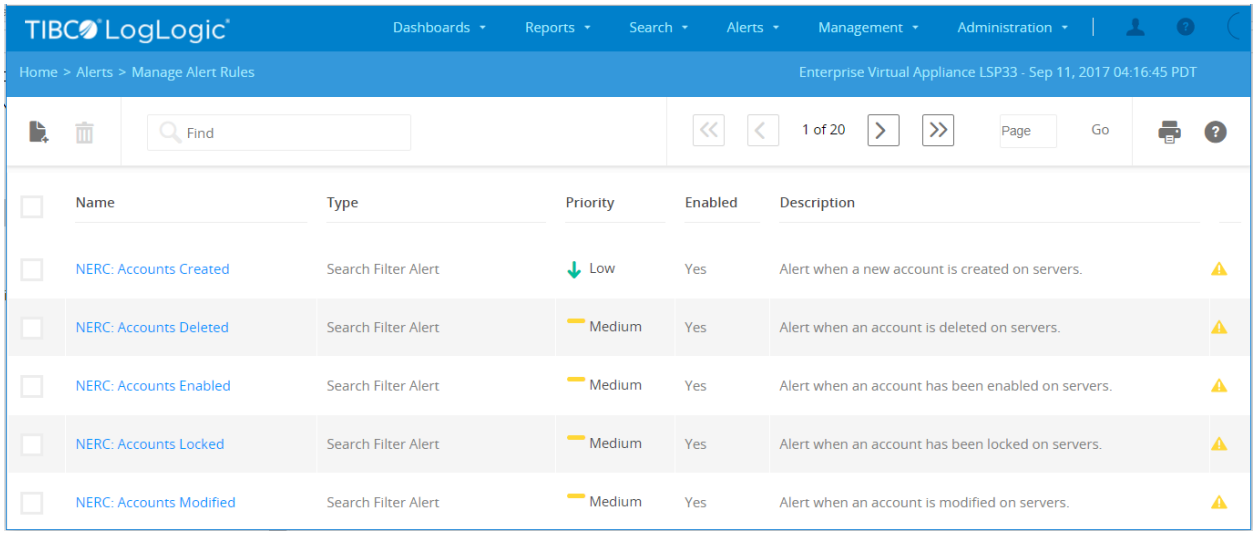
The Compliance Suite package contains a number of alerts that can be easily enabled and modified for your business needs.

Procedure

1. From the navigation menu, click **Alerts** > **Manage Alert Rules** .

   The following figure shows a cropped list of the Compliance Suite alerts loaded from the NERC XML file.

   Compliance Suite Alerts



2. To view details of a specific alert, click the **Name** of the alert.

   The **General** tab is selected by default, but each tab on the page contains information required to enable an alert.

3. Click each of the tabs to view the default entries.

   Make sure that you identify the default entries and areas that might need to be modified.

Enabling Compliance Suite Alerts

By default, the compliance suite alerts have pre-configured information to help you get started. In some instances, you can simply enable the alert because the default settings are aimed at capturing a broad range of alerts.

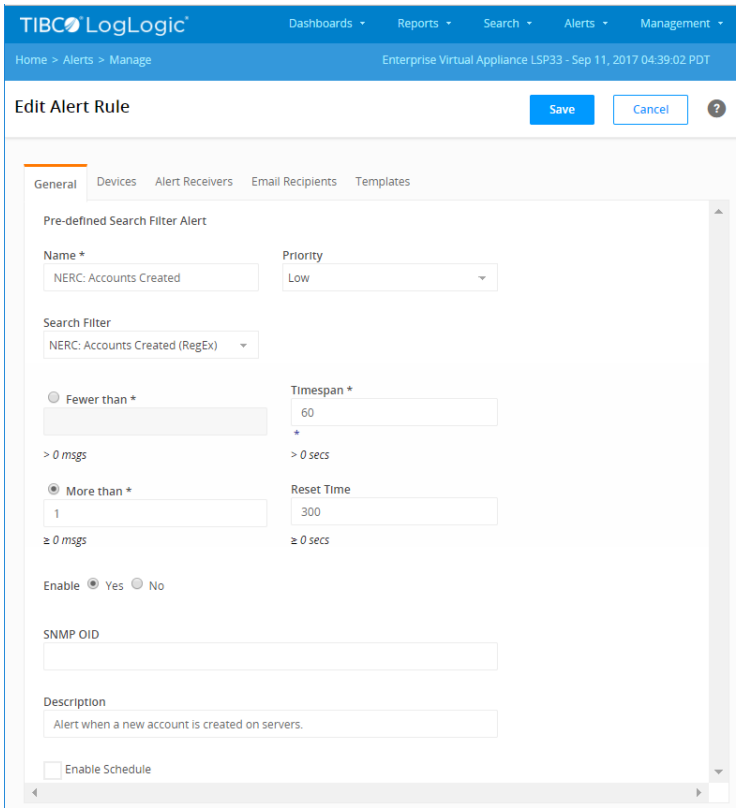
To enable alerts, you must set the device(s) to monitor, the SNMP trap receivers, as well as who receives an alert notification and how they receive it.

Procedure

1. From the navigation menu, select **Alerts** > **Manage Alert Rules** .
2. Click the **Name** of the alert.
3. On the **General** tab, for **Enable**, select the **Yes** radio button.

   The following figure shows the **General** tab for the **NERC: An Account Created** alert.

Account Created Alert



4. Select the device(s) to be alerted on by completing the following steps:

   You can define alerts for all devices, a selection of devices, or a single device.

   a) Select the **Devices** tab.

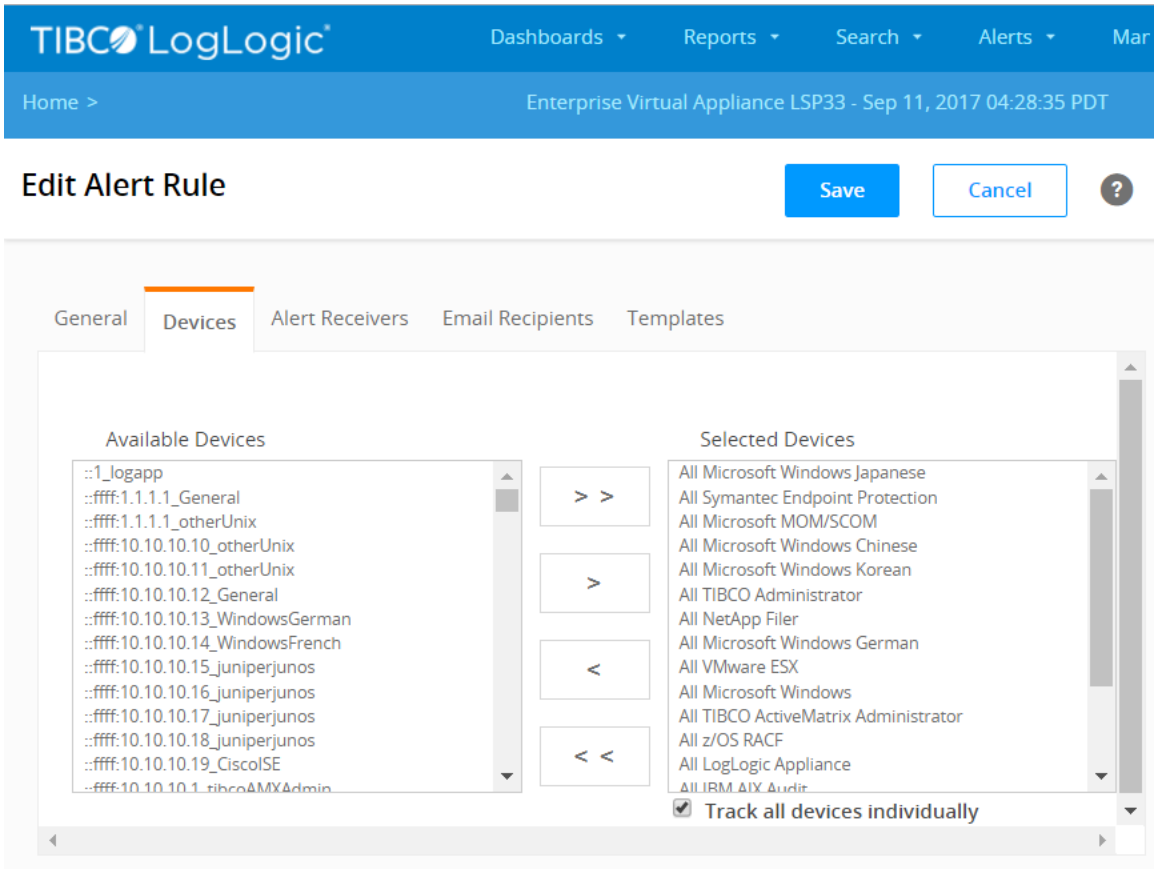
   b) In the **Available Devices** text block, select the appropriate log sources (i.e., devices) you want to monitor and be alerted on when an alert rule is triggered.

   > If the **Show Only Device Groups** setting is enabled on the Appliance, then the **Available Devices** text block lists only device groups. To enable or disable this feature, go to **Administration** > **System Settings** > **General** tab, scroll down to the **System Performance Settings** section and modify the **Optimize Device Selection List** option.

   c) Click **Add All** or **Add Selected Device(s).**

   The following figure shows the **Devices** tab for the selected alert.

Available and Selected Devices



5. The Appliance has the ability to generate an SNMP trap that is sent to an SNMP trap receiver when an alert rule is triggered. Select the alert receivers available to your device(s) by completing the following steps:
   a) Select the **Alert Receivers** tab.
   b) In the **Available Alert Receivers** text block, select the appropriate alert receivers available for your device(s).
   c) Click **Add All** or **Add Selected Receiver(s)**.
6. Select the email recipients to be alerted with a notification email when an alert rule is triggered by completing the following steps:
   a) Select the **Email Recipients** tab.
   b) In the **Available Users** text block, select the appropriate email recipients.
   c) The **Available Users** text block lists all of the user accounts on the Appliance.
   d) Click **Add All** or **Add Selected User(s)**.
7. Click **Update**.

Viewing Compliance Suite Alert Results

After you have enabled at least one alert, and that alert is triggered, you can view the results.

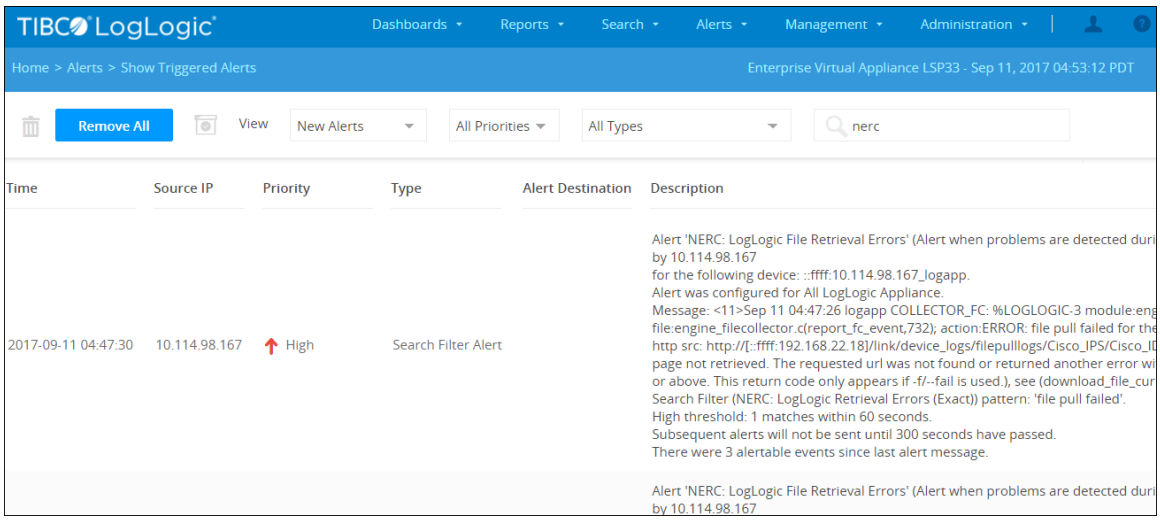
For more information on how to use and modify alerts, see to the *TIBCO LogLogic® Log Management Intelligence (LMI) User Guide*.

Procedure

1. In the navigation menu, select **Alerts** > **Show Triggered Alerts** .

   The following figure shows a cropped version of the **Show Triggered Alerts** page.

Aggregated Alert Log



2. From the **Show** menu, select the desired alert and priority filters to show only those alerts you want to display. The defaults are **New Alerts** and **All Priorities**.
3. (Management Station Appliances Only) From the **From Appliance** drop-down menu, select the Appliance from which you want to view the alerts.
   The results of your query are displayed. You can navigate through all of the data by using the page navigation buttons or page text field.
4. You can either acknowledge or remove an alert. Click the check box next to the alert name, then click **Acknowledge**, **Remove**, or **Remove All**.

   Each alert is triggered based on your set alert parameters, so care must be taken when acknowledging or removing the alert.

   For more information on how to use and modify alerts, see to the *TIBCO LogLogic® Log Management Intelligence (LMI) User Guide* .

NERC Critical Infrastructure Protection Standards

Using TIBCO LogLogic Compliance Suite you can implement NERC critical infrastructure protection standards objectives.

CIP-001: Sabotage Reporting

Sabotage Reporting is beyond the scope of this guide.

CIP-002: Cyber Security - Critical Cyber Asset Identification

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of risk-based assessment.

CIP-002: Cyber Security Requirements

- R1. Critical Asset Identification Method - The Responsible Entity must identify and document a risk-based assessment methodology to identify Critical Assets in the organization.
- R2. Critical Asset Identification - The Responsible Entity creates a list of Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity reviews this list at least annually and updates it as necessary.
- R3. Critical Cyber Asset Identification - Using the list of Critical Assets developed pursuant to R2, the Responsible Entity must develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.

  Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

  - The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter;
  - The Cyber Asset uses a routable protocol within a control center; or,
  - The Cyber Asset is dial-up accessible.
- R4. Annual Approval - The senior manager or delegate(s) shall approve annually the risk- based assessment methodology, the list of Critical Assets, and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets.

  The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets, and the list of Critical Cyber Assets (even if such lists are null.)

CIP-002: Cyber Security SubRequirements

- R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
- R1.2. The risk-based assessment shall consider the following assets:
  - R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

- R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.
- R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.
- R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.
- R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
- R1.2.6. Special Protection Systems that support reliable operation of the Bulk Electric System.
- R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

CIP-002: Cyber Security Measures

The following measures are used to demonstrate compliance:

- M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.
- M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.
- M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.
- M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

CIP-002: Cyber Security Illustrative Approach

An entity should first identify Cyber Assets associated with the operation of an identified Critical Asset. This is not intended to be a complete inventory of all Cyber Assets at the facility, but rather an evaluation and then identification of all Cyber Assets that may have direct or indirect impact on the essential function of a Critical Asset. However, a comprehensive Cyber Asset inventory would be helpful in supporting CIP-005-1.

Entities may want to perform complete inventories of Cyber Assets if there are questions about the nature of their impact on essential functions - this will ensure that all appropriate Cyber Assets have been considered in the assessment. A Cyber Asset is defined to be "Programmable electronic devices and communication networks including hardware, software and data." For the purposes of this guideline, software, data, and cabling are considered to exist within the framework of the Cyber Asset and not as separate Cyber Assets.

In general Cyber Assets are digital elements that are part of control systems, data acquisition systems, or the networking equipment used by a control or data acquisition system.

- Control systems comprise devices or sets of devices that act to manage, command, or regulate the behavior of processes, devices, or other systems.
- Data acquisition systems are a collection of sensors and communication links that act to sample, collect, and provide data regarding the plant systems to a centralized location for display, archiving, or further processing.
- Networking equipment includes devices such as routers, hubs, switches, firewalls, and modems.

When identifying Cyber Assets consider the different roles and functions of Cyber Assets that might directly or indirectly affect the essential functionality of a Critical Asset such as:

- Provides operation information in real time
- Controls parameters, manual or automated
- Calculates important parameters or limits

- Generates prompts or alarms
- Provides connectivity between Cyber Assets within the ESP
- Supports continuity of operations of the Critical Assets or local recovery plans

This approach assumes that the Responsible Entity has already identified its Critical Assets and has defined the essential functions of the Critical Assets. Defining the essential functions of the Critical Asset helps determine whether a particular Cyber Asset is essential to the operation of the Critical Asset. Cyber Assets that are connected to support systems (such as environmental and continuous power systems) that are indirectly essential to the operation of the Critical Asset could also be addressed. NERC recommends the following five steps:

Identify Cyber Assets associated with a Critical Asset.

Group Cyber Assets by application.

Identify Cyber Assets that support essential functions of Critical Assets.

Identify Cyber Assets with CIP-002 R3 qualifying characteristics.

Compile a list of Critical Cyber Assets.

Cyber Assets are considered essential to a Critical Asset if any one of the following criteria is met:

- The Cyber Asset is involved in, or is capable of, supervisory or autonomous control that supports an essential function of a Critical Asset.
- The Cyber Asset displays, transfers, or contains information used to make real time operational decisions that supports an essential function of a Critical Asset.
- The Cyber Asset if lost would degrade the essential function of a Critical Asset.
- The Cyber Asset if compromised could impact the essential function of a Critical Asset.

CIP-002 Reports and Alerts

There are no TIBCO LogLogic Compliance Suite Reports and Alerts for Critical Cyber Asset Identification.

CIP-003: Cyber Security - Security Management Controls

Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-003: Cyber Security Requirements

- R1. Cyber Security Policy - The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following requirements:
  - R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
  - R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retirement approved by FERC effective January 21, 2014.)
  - R1.3.The cyber security policy is annually reviewed and approved by the senior manager assigned pursuant to R2.
- R2. Leadership - The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

- R3. Exceptions - Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retirement approved by FERC effective January 21, 2014.)
- R4. Information Protection - The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
- R5. Access Control - The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
- R6. Change Control and Configuration Management - The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003: Cyber Security Sub-Requirements

- R2.1. The senior manager shall be identified by name, title, and date of designation.
- R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.
- R2.3. Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
- R2.4. The senior manager or delegate(s) shall authorize and document any exception from the requirements of the cyber security policy.
- R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retirement approved by FERC effective January 21, 2014.)
- R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and provide compensating measures. (Retirement approved by FERC effective January 21, 2014.)
- R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retirement approved by FERC effective January 21, 2014.)
- R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
- R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retirement approved by FERC effective January 21, 2014.)
- R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
- R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
  - R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

  - R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
- R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
- R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

CIP-003: Cyber Security Measures

- M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (Retirement approved by FERC effective January 21, 2014.)
- M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.
- M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retirement approved by FERC effective January 21, 2014.)
- M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.
- M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.
- M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

CIP-003: Cyber Security Illustrative Approach

Senior management should support ongoing security policy awareness and compliance. Management and employees must remain alert to operational changes that could affect security and actively communicate issues with security personnel. Business line managers are responsible and accountable for maintaining the security of his or her personnel, systems, facilities, and information. Everyone must be kept aware and educated, as the threats and vulnerabilities change that can affect the safe, sound, and secure day-to-day operations. Entities must monitor compliance with security policies and investigate security violations.

Before an effective information security program can be created, each agency must identify and list its critical assets and critical cyber assets through a risk-based assessment methodology as defined in CIP-002. This process involves the gathering of asset information from all business units within the entity. Each asset on this list must then be classified based on the magnitude of harm or inconvenience that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of the asset to the entity and the safety of its information. Typical classification levels used in describing cyber assets include:

- Public - Information that may be safely released to the general public. Examples include outage statistics and estimated restoration time. This level also includes information to be disclosed to the public, such as financial results.
- Proprietary - Information that may be obtained by an employee but should not be released to the public. Examples may include organization charts, telephone lists, or budget information.
- Sensitive - Information that may contribute to understanding or identifying an essential system. Examples may include operational procedures, lists of assets, network diagrams, floor plans, equipment layouts, and disaster recovery plans.
- Confidential - Information that significantly enhances the probability of a successful compromise of an essential system. Examples may include incident response plans, security configurations, password lists, and results of physical or cyber vulnerability assessments.

After all cyber assets are identified and classified, the agency must identify and prioritize all known and unknown threats and vulnerabilities that pose information security risks and could affect its cyber assets. Then (and only then) can the entity create, monitor, and enforce adequate policies, procedures and controls that cost-effectively reduce information security risks to an acceptable level throughout the entity's networks, facilities, and the life cycle of each information system or groups of information systems, as appropriate.

Examples for such security policies and controls include access controls and change management controls.

- Access Controls – Each entity should control access to protected information. The access restrictions should be consistent with the asset classification levels that are established, for example, public, proprietary, sensitive, or confidential. The following list describes some commonly used access levels:
  - Public access level allows read-only access. Write permissions should only be granted to those authorized to modify information.
  - Proprietary access level restricts access to employees only. Access to contractors and third parties is permitted only under a signed nondisclosure agreement (NDA).
  - Sensitive access level enables you to grant access to employees, contractors with an NDA, and third parties with NCA may be granted access. Access may be granted to groups of sensitive documents or to all sensitive documents.
  - Confidential access must be given only to personnel with a need-to-know requirement. Contractors or third parties with need for confidential information should be granted access only after legal review of the NDA to ensure that NDA is sufficient for this level of access. Access should be granted only to individual applications, databases, or files for a defined time period. When the time period expires, the access privileged should be reviewed and renewed only if still needed.
- Change Control and Configuration Management – These controls ensure that only authorized and fully tested software is placed in operation. They also limit and monitor access to powerful programs and sensitive files associated with computer operations. They are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. This includes patch management to mitigate the risks of software vulnerabilities.

Policy monitoring is accomplished by implementing system or security software that provides an audit trail with logs of all system activity. Done properly, entities should configure their software to collect and maintain audit trails that are sufficient to track all security-relevant events.

The security risk management practices must include the following automated capabilities:

- Asset identification and classification
- Risk assessment
- Risk-based policy and procedure implementation
- Cost-effective implementation of risk-based controls
- Real-time vulnerability assessment, monitoring, and alert generation

Security risk management and CIP compliance are business problem that needs to be addressed by an enterprise-wide methodology that leverages the right people, practices, and technology on a continuous basis – not a limited point-in-time project basis. A static and incomplete security program provides a false sense of security and is increasingly ineffective over time. Monitoring and updating the security program is an important part of the ongoing cyclical security process. Entities should continuously gather and analyze information regarding: critical cyber assets; new threats and vulnerabilities; actual attacks on the organization, its assets, and its interlinked business partners; and the effectiveness of the existing security controls.

Deploying a series of diverse security technologies at multiple layers helps to mitigate the risk of successful cyber attacks. Technology solutions can add significant value in jumpstarting successful information security risk management best practice initiatives.

CIP-003 Reports and Alerts

- CIP-003-1 R3.2
- CIP-003-1 R5.2
- CIP-003-1 R5.3

CIP-004: Cyber Security - Personnel and Training

To minimize the risk of misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by providing an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

CIP-004: Cyber Security Requirements

- R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using the following mechanisms:
  - Direct communications (for example, emails, memos, computer based training)
  - Indirect communications (for example, posters, intranet, brochures)
  - Management support and reinforcement for example, presentations, meetings)
- R2. 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.
- R3. Personnel Risk Assessment - The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:
  - R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (for example, Social Security Number verification in the US) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending on the criticality of the position.
  - R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
  - R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.
- R4. Access - The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

CIP-004: Cyber Security Sub-Requirements

- R2.1. This training program must ensure that all personnel with access to Critical Cyber Assets, including contractors and service vendors, are trained before they are granted access except in specified circumstances such as an emergency.
- R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004 and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
  - R2.2.1. The proper use of Critical Cyber Assets
  - R2.2.2. Physical and electronic access controls to Critical Cyber Assets
  - R2.2.3. The proper handling of Critical Cyber Asset information
  - R2.2.4. Action plans and procedures to recover or reestablish Critical Cyber Assets and access then after following a Cyber Security Incident
- R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
- R4.1. The Responsible Entity shall review the list(s) of its personnel who have access to Critical Cyber Assets quarterly and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
- R4.2. The Responsible Entity shall revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004: Cyber Security Measures

- M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.
- M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.
- M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.
- M4. The Responsible Entity shall make available documentation of the lists, list review and update, and access revocation as needed as specified in Requirement R4.

CIP-004: Cyber Security Illustrative Approach

Entities need to educate users regarding policies and their security roles and responsibilities. Training should support security awareness and strengthen compliance with security policies and procedures. Ultimately, the behavior and priorities of senior management heavily influence the level of employee awareness and policy compliance, so training and the commitment to security should start with senior management.

Cyber security training programs should encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets. Cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities.

Personnel training should be appropriate for an employee's duties, functions, experience, or access level. Any training information that concerns vulnerabilities should be revealed on a need-to-know basis and not universally.

Newly hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. Current employees and vendors with existing contractual relationships with the entity should have an initial personnel risk assessment completed as soon as reasonably possible, for example, before they are to be auditably compliant with this Requirement.

Timely system updates to access rights are important because access to critical cyber assets by employees, contractors, or vendors represents a gap in security when such access is no longer needed.

When an employee, contractor, or vendor no longer performs a function that requires authorized physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement or termination), their access privileges should be revoked immediately. Need for a brief lag in revoking such privileges, must be documented for audit purposes. There may be operational reasons that justify retention of privileges after an employee transfers, but the default procedure should be to cancel access privileges at transfer.

In addition, unescorted physical access should be denied to individuals that are not identified on the authorization list.

CIP-004 Reports and Alerts

There are no TIBCO LogLogic Compliance Suite Reports and Alerts for Personnel and Training.

CIP-005: Cyber Security — Electronic Security Perimeter(s)

Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-005: Cyber Security Requirements

- 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).
- R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
- R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
- R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
  - R4.1. A document identifying the vulnerability assessment process;
  - R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
  - R4.3. The discovery of all access points to the Electronic Security Perimeter;
  - R4.4. A review of controls for default accounts, passwords, and network management community strings;
  - R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

- R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

CIP-005: Cyber Security Sub-Requirements

- 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).
- R1.2. For a dial-up accessible Critical Cyber Asset that uses a nonroutable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
- R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
- R1.4. Any noncritical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.
- R1.5. Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003; Standard CIP-004 Requirement R3; Standard CIP-005 Requirements R2 and R3; Standard CIP-006 Requirement R3; Standard CIP-007 Requirements R1 and R3 through R9; Standard CIP-008; and Standard CIP-009.
- R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.
- R2.1. The entity's electronic access control processes and mechanisms shall use an access control model that denies access by default, unless explicit access permissions are specified.
- R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
- R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
- R2.4. Where external interactive access to the Electronic Security Perimeter is enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
- R2.5. The required documentation must, at least, identify and describe:
  - R2.5.1. The processes for access request and authorization.
  - R2.5.2. The authentication methods.
  - R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.
  - R2.5.4. The controls used to secure dial-up accessible connections.
- R2.6. Appropriate Use Banner - Where technically feasible, electronic access control devices shall display an appropriate usage banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
- R3.1. For dial-up accessible Critical Cyber Assets that use nonroutable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
- R3.2. Where technically feasible, the security monitoring process(es) shall detect and generate alert for attempts at or actual unauthorized access. These alerts are used to send appropriate notifications

to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

- R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP- 005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.
- R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
- R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents must meet with the requirements of Standard CIP-008.

CIP-005: Cyber Security Measures

- M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.
- M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.
- M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.
- M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.
- M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

CIP-005: Cyber Security Illustrative Approach

Electronic access controls include those related to boundary protection, user identification and authentication, authorization, encryption, logging, auditing, and monitoring. Agencies must protect the security boundaries and all access points that are identified as critical cyber assets through its risk assessment methodology.

Multiple electronic security perimeters may be required; for example, one may be needed around a control room, while another may be established around a substation. For any electronic security perimeter established, the responsible entity must develop mechanisms to control and monitor electronic access to all electronic access points. In addition the mechanism, must assess the electronic security perimeter's cyber vulnerability and test every electronic access point at least annually.

The Federal Energy Regulatory Commission (FERC) has instructed the NERC to issue specific supplemental guidance on the identification and protection of electronic security perimeters. NERC will issue additional guidance on:

- Adequacy of electronic security perimeters – While the electronic security perimeter constitutes a first line of defense, the effectiveness of any one defensive measure depends on the quality of active human maintenance. Also, there is no one perfect defensive measure that will guarantee the protection of the Bulk-Power System. Therefore, when constructing an electronic security perimeter, each entity should implement a defensive security approach including two or more defensive measures in a defense in depth poster, if technically feasible. However, there may be instances in which certain facilities cannot implement defense in depth or where such an approach would harm reliability rather than enhance it. In such instances, the responsible entity should implement electronic defense in depth measures or justify why it is not technical feasible.
- Protecting access points and controls – Examples of strong verification and authentication technologies for protecting access points under Requirement R2.4 include digital certificates and two-factor authentication. FERC has instructed NERC to identify additional examples of specific verification technologies and other technically equivalent measures or technologies.

- Monitoring access logs – Automated and manual log reviews are important. Automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches. Supplemental periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. In addition, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. For example, if a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For entities without automated log review and alerts, performing a manual review is even more important because this is the only review of the logs.

  Each entity should designate individual assets as "readily accessible" or "not readily accessible." Readily available logs, such as those from within a control room setting, should be reviewed at least weekly. Logs that are not readily available, such as those located at a remote substation, are less accessible and therefore can be read less frequently. Any attempt, however, to differentiate the required frequency of review of these logs must be balanced against the criticality of the facilities; it is not acceptable to dismiss a critical facility from timely review simply because it is remote.
- Vulnerability assessments – Annual vulnerability assessments are sufficient when no significant modifications have been made to the electronic access points of the electronic security perimeter. When the electronic security perimeter or another measure in a defense in depth strategy is significantly modified, it is not acceptable to wait a year to test modifications. In such instances, a vulnerability assessment of the electronic access points as part of, or contemporaneously with, any modifications to the electronic security perimeter or defense in depth strategy should be conducted. For example, updating an attack signature file on the electronic access point might not require an active vulnerability assessment, but replacing the devices that comprise the electronic access point could require a vulnerability assessment.

  In addition to the annual vulnerability assessment, each entity should conduct an active vulnerability assessment at least once every three years, with annual paper assessments allowable in the intervening years. If an active vulnerability assessment is not "technically feasible," then a responsible entity may apply to be excused from full compliance to the NERC Regional Entity, fully documenting the necessary interim actions, milestone schedule, and mitigation plan.

  Active vulnerability testing should be conducted on test systems. Test systems do not need to exactly match or mirror the operational system. However, to perform active vulnerability assessments, the responsible entities should create a representative system, that is, one that replicates the actual system as closely as possible. The active vulnerability assessment should be carried out on this representative system. The responsible entity should also document the differences between the operational and representative system for the auditors. As part of this documentation, the responsible entity should also document how test results on the representative system might differ from the operational system and how the responsible entity accounts for such differences in operating the system. In short, the responsible entity should ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.

CIP-005 Reports and Alerts

Use the following links/references to see the CIP-005 reports and alerts:

- CIP-005-1 R1.6
- CIP-005-1 R2.2
- CIP-005-1 R2.3
- CIP-005-1 R2.4
- CIP-005-1 R3
- CIP-005-1 R3.1
- CIP-005-1 R3.2

- CIP-005-1 R1.4
- CIP-005-1 R4.2
- CIP-005-1 R4.4

CIP-006: Cyber Security – Physical Security of Critical Cyber Assets

Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002-2 through CIP-009-2 using reasonable business judgment.

CIP-006: Cyber Security Requirements and Sub-Requirements

- R1. Physical Security Plan - The Responsible Entity shall document, implement, and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
  - R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
  - R1.2. Identification of all access points through each Physical Security Perimeter and measures to control entry at the access points.
  - R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
  - R1.4. Appropriate use of physical access controls as described in Requirement R4, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
  - R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
  - R1.6. Continuous escorted access within the physical security perimeter of personnel not authorized for unescorted access.
  - R1.7. Update of the physical security plan within 30 calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
  - R1.8. Annual review of the physical security plan.
- R2. Protection of Physical Access Control Systems - Cyber Assets that authorize or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
  - R2.1. Be protected from unauthorized physical access.
  - R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.
  - R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
  - R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
- R3. Protection of Electronic Access Control Systems - Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

- R4. Physical Access Controls - The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
  - R4.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
  - R4.2. Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “mantrap” systems.
  - R4.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
  - R4.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
- R5. Monitoring Physical Access - The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:
  - R5.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
  - R5.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.
- R6. Logging Physical Access - Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
  - R6.1. Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.
  - R6.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.
  - R6.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
- R7. Access Log Retention - The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents must meet with the requirements of Standard CIP-008-2.
- R8. Maintenance and Testing - The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:
  - R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
  - R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.
  - R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

CIP-006: Cyber Security Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

- M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.
- M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.
- M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.
- M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.
- M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.
- M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.
- M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.
- M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

CIP-006: Cyber Security Illustrative Approach

While this standard emphasizes requirements for establishing a Physical Security Perimeter within a "six-wall" border, it also allows for alternative measures to control physical access to cyber assets that do not reside within such a border. In today's distributed network environment, cyber assets are increasingly likely to exist outside the "six-wall" border. In addressing alternative measures to establish physical security practices outside the "six-wall" border, responsible entities should define physical security zones and implement appropriate preventive and detective controls in each zone to protect against the risks of:

- Physical penetration by malicious or unauthorized people,
- Damage from environmental contaminants, and
- Electronic penetration through active or passive electronic emissions.

Risk-based Security Zones – Zones are physical areas with differing physical security requirements. The security requirements of each zone are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone. For instance, data centers that would typically reside within a "six-wall" border may be in the highest security zone. Staff offices may be in a much lower security zone. Different security zones can exist within the same structure. Routers and servers in an office, for instance, may be protected to a greater degree than password protected dumb terminals. Computers and telecommunications equipment within an operations center will have a higher security zone than input or output operations, with the media used by that equipment stored at an even higher zone.

The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but not be limited to, the following threats:

- Aircraft crashes
- Chemical effects
- Dust

- Electrical supply interference
- Electromagnetic radiation
- Explosives
- Fire
- Smoke
- Theft/Destruction
- Vibration/Earthquake
- Water
- Criminals
- Terrorism
- Political issues (e.g. strikes, disruptions)
- Any other threats applicable based on the entity's unique geographical location, building configuration, neighboring entities, etc.

Alternative Measures – Alternative physical security measures are needed where cyber assets such as hardware and software exist in a distributed IT environment, e.g., in a user department that may be less secure than a "six-wall" location such as a data center or a computer room. Distributed hardware and software environments (e.g., local area networks or LANs) that offer a full range of applications are commonly housed throughout the organization. In such situations, physical security precautions are often less sophisticated than those found in large data centers, and overall building security becomes more important. Internal control procedures are necessary for all hardware and software deployed in distributed, and less secure, environments.

The level of security surrounding any hardware and software should depend on the sensitivity of the data that can be accessed, the significance of applications processed, the cost of the equipment, and the availability of backup equipment. For example, because of their portability and location in distributed environments, personal computers (PCs) and other portable devices such as laptops often are prime targets for theft and misuse. The location of these portable devices and the sensitivity of the data and systems they access determine the extent of physical security required. For example, entities should consider securing PCs to workstations, locking or removing disk drives and unnecessary physical ports, and using screensaver passwords or automatic timeouts. Employees also should have only the access to PCs and data they need to perform their job. The sensitivity of the data processed or accessed by the computer usually dictates the level of control required. The effectiveness of security measures depends on employee awareness and enforcement of these controls.

Physical security for distributed IT, particularly LANs that are usually PC-based, is slightly different than for mainframe platforms. With a network there is often no centralized computer room. In addition, a network often extends beyond the local premises. There are certain components that need physical security. These include the hardware devices and the software and data that may be stored on the file servers, PCs, or removable media (tapes and disks). As with more secure IT environments, physical network security should prevent unauthorized personnel from accessing LAN devices or the transmission of data. In the case of wire-transfer clients, more extensive physical security is required.

An advantage of PCs is that they can operate in an office environment, providing flexible and informal operations. However, as with larger systems, PCs and other portable devices are sensitive to environmental factors such as smoke, dust, heat, humidity, food particles, and liquids. Because they are not usually located within a secure area, policies should be adapted to provide protection from ordinary contaminants. Other environmental problems to guard against include electrical power surges and static electricity.

The electrical power supply in an office environment is sufficient for PC requirements. However, periodic fluctuations in power (surges) can cause equipment damage or loss of data. PCs in environments that generate static electricity are susceptible to static electrical discharges that can cause damage to PC components or memory.

Network wiring also requires some form of protection because the data it carries can be revealed or contaminated even with slight physical contact with the wiring. Examples of controls include using a conduit to encase the wiring, avoiding routing through publicly accessible areas, and avoiding routing networking cables in close proximity to power cables. The type of wiring can also provide a degree of protection; signals over fiber cables, for instance, are less susceptible to interception than signals over copper cable.

Network security also can be compromised through the capture of radio frequency emissions. Frequency emissions are of two types, intentional and unintentional. Intentional emissions are broadcast, for instance, by a wireless network. Unintentional emissions are the normally occurring radiation from monitors, keyboards, disk drives, and other devices. Shielding is a primary control over emissions. The goal of shielding is to confine a signal to a defined area. An example of shielding is the use of foil-backed wallboard and window treatments. Once a signal is confined to a defined area, additional controls can be implemented in that area to further minimize the risk that the signal will be intercepted or changed.

Physical security devices frequently need preventive maintenance to function properly.

Maintenance logs are one control the entity can use to determine whether the devices are appropriately maintained. Periodic testing of the devices provides assurance that they are operating correctly.

Security guards should be properly instructed about their duties. The employees who access secured areas should have proper identification and authorization to enter the area. All visitors should sign in and wear proper IDs so that they can be identified easily. Security guards should be trained to restrict the removal of assets from the premises and to record the identity of anyone removing assets. Consideration should be given to implementing a specific and formal authorization process for the removal of hardware and software from premises.

CIP-006 Reports and Alerts

Use the following links/references to see the CIP-006 reports and alerts:

- CIP-006-1 R4
- CIP-006-1 R5

CIP-007: Cyber Security — Systems Security Management

Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing systems that are determined to be Critical Cyber Assets, as well as the other (noncritical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-007: Cyber Security Requirements

- R1. Test Procedures - The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
- R2. Ports and Services - The Responsible Entity shall establish, document and implement a process to ensure that only the ports and services required for normal and emergency operations are enabled.
- R3. Security Patch Management - The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

- R4. Malicious Software Prevention - The Responsible Entity shall use antivirus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
- R5. Account Management - The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

  Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R5.
- R6. Security Status Monitoring - The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
- R7. Disposal or Redeployment - The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
- R8. Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
  - R8.1. A document identifying the vulnerability assessment process;
  - R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
  - R8.3. A review of controls for default accounts; and,
  - R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R9. Documentation Review and Maintenance - The Responsible Entity shall review an update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

CIP-007: Cyber Security Requirements (Update:v5 Rev.3 09/11/12)

- R1. Ports and Services - Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R1. (Maps to Prior Requirement R2)
- R2. Security Patch Management - Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R2. (Maps to Prior Requirement R3)
- R3. Malicious Software Prevention - Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R3. (Maps to Prior Requirement 4)
- R4. Security Event Monitoring - Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R4. (Maps to Prior Requirement R6)
- R5. System Access Controls - Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R5. (Maps to Prior Requirement R5)

CIP-007: Cyber Security Sub-Requirements

- R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures ensuring minimal adverse effects on the production system or its operation.
- R1.2. The Responsible Entity shall document testing procedures to reflect the production environment.
- R1.3. The Responsible Entity shall document test results.
- R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
- R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
- R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
- R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
- R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
- R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
- R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installation of the signatures.
- R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to the work functions performed.
- R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.
- R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
- R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
- R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
  - R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
  - R5.2.2. The Responsible Entity shall identify the individuals with access to shared accounts.
  - R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
- R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, depending on feasibility:

  - R5.3.1. Each password shall be a minimum of six characters.
  - R5.3.2. Each password shall consist of a combination of alphanumeric, and “special” characters.
  - R5.3.3. Each password shall be changed at least annually or more frequently based on the risk.
- R6.1. The Responsible Entity shall implement and document the organizational processes, and technical and procedural mechanisms for monitoring security events on all Cyber Assets within the Electronic Security Perimeter.
- R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
- R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
- R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
- R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.
- R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

CIP-007: Cyber Security Sub-Requirements (Update: v5 Rev.3.09 09/11/12)

- R1.1. Where technically feasible, enable only logical network accessible ports that the Responsible Entity needs, including port ranges or services to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device, the open ports are deemed needed.
- R1.2. Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.
- R2.1. A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
- R2.2. At least once every 35 calendar days, evaluate applicability of security patches that have been released since the last evaluation. use the source or sources identified in Part 2.1 for evaluation.
- R2.3. For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, perform one of the following actions:
  - Apply the applicable patches
  - Create a dated mitigation plan
  - Revise an existing mitigation plan

  Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.
- R2.4. For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.
- R3.1. Deploy method(s) to deter, detect, or prevent malicious code.
- R3.2. Mitigate the threat of identified malicious code.

- R3.3 For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.
- R4.1. Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents, which includes, as a minimum, each of the following types of events:
  - 4.1.1. Detected successful login attempts
  - 4.1.2. Detected failed access attempts and failed login attempts
  - 4.1.3. Detected malicious code
- R4.2. Generate alerts for security events that need an alert, which includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):
  - 4.2.1. Detected malicious code from Part 4.1
  - 4.2.2. Detected failure of Part 4.1 event logging
- R4.3 Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, except under CIP Exceptional Circumstances.
- R4.4 Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents.
- R5.1. Have a method(s) to enforce authentication of interactive user access, where technically feasible.
- R5.2. Identify and inventory all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
- R5.3. Identify individuals who have authorized access to shared accounts.
- R5.4. Change known default passwords, per Cyber Asset capability.
- R5.5. For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:
  - 5.5.1. Password length that is, at least, less than eight characters or the maximum length supported by the Cyber Asset; and
  - 5.5.2. Minimum password complexity that is less than three or more different types of characters (for example, uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.
- R5.6. Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.
- R5.7. Where technically feasible:
  - Limit the number of unsuccessful authentication attempts; or
  - Generate alerts after a threshold of unsuccessful authentication attempts.

CIP-007: Cyber Security Measures

- M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.
- M2. The Responsible Entity shall make available documentation as specified in Requirement R2.
- M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

- M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.
- M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.
- M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.
- M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.
- M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.
- M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

CIP-007: Cyber Security Measures (Update: v5 Rev.3 09/11/12)

- M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R1. - Ports and Services
- M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R2. - Security Patch Management
- M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R3. - Malicious Code
- M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in CIP-007-5 R4. - Security Event Monitoring
- M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-007-5. - System Access Controls

CIP-007: Cyber Security Illustrative Approach

While these system security management requirements are more prescriptive in nature than the other CIP Requirements, the Federal Energy Regulatory Commission (FERC) has instructed the NERC to issue specific supplemental guidance on the appropriate methods, processes, and procedures for securing critical and non-critical cyber assets within the electronic security perimeters. NERC will issue additional guidance on:

- Test procedures – Similar to the active vulnerability testing procedures defined under the electronic security perimeter requirements, test systems do not need to match or mirror production systems. However, to perform active testing, the responsible entities should create a representative system, that is, one that replicates the actual system as closely as possible. The Responsible Entity should also document the differences between the operational and representative system for the auditors. As part of this documentation, the Responsible Entity should also document how test results on the representative system might differ from the operational system and how the Responsible Entity accounts for such differences in operating the system. In short, the Responsible Entity should ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.
- Malicious software prevention – Entities should establish safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means.
- While every system in an electronic security perimeter does not need antivirus software, critical cyber assets must be protected, regardless of the operating system being used. Any network infrastructure devices that are not directly targeted can be affected as collateral damage. Computer virus technology changes every day. Therefore, entities should protect all cyber assets within an electronic security perimeter, regardless of the operating system being used.

- Security status monitoring – Among other things, a Responsible Entity must maintain logs of system events related to cyber security, where technically feasible, to support security incident response as required in CIP-008, Incident Reporting and Response Planning. Logs must be retained for 90 calendar days, and the Responsible Entity must review logs of system events related to cyber security and maintain records documenting review of logs. A sampling of logs should be reviewed at least weekly. Log sampling procedures should be defined in the entity's cyber security policy. The review process should be rigorous enough to enable the entity to detect intrusions by attackers. Examples of information that should be contained in logs include:
  - Identification of the information affected
  - Type of activity
  - Date and time of activity
  - Individual performing the activity
  - Individual approving the activity
- Disposal or redeployment – Each entity should assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. In general, there are three methods for disposing of computer data:
  - Clear: Overwriting the media with random content.
  - Purge: Degaussing the media with a strong magnetic field. High-quality degaussing can adequately protect media from unauthorized access. Degaussing, however, is not the sole means for achieving this goal.
  - Destroy: Methods include disintegration, pulverization, melting, and incineration.
- Cyber vulnerability assessment – Vulnerability testing is a valuable tool in determining whether actions that were taken to support the security posture of the electronic security perimeter and other areas of responsibility are in fact adequate. Each entity's vulnerability testing should take into account emerging and diverse technologies and newly discovered vulnerabilities as they emerge. The FERC has directed the ERO and NERC to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments.
- Documentation review and maintenance – Establishing and maintaining correct documentation of methods, processes and procedures for securing a Responsible Entity's system is necessary. If an event occurred before documentation was updated, an operator may not know of a change and could operate the system relying on out-of-date information. Such an event would put reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk.

CIP-007 Reports and Alerts

Use the following links/references to see the CIP-007 reports and alerts:

- CIP-007 R4
- CIP-007-5 R1.1
- CIP-007-5 R1.2
- CIP-007-5 R2
- CIP-007-5 R2.1
- CIP-007-5 R3
- CIP-007 R5
- CIP-007 R5.1.1

- CIP-007 R5.1.2 / CIP-007-5 R4.1
- CIP-007 R5.2 / CIP-007-5 R5.3
- CIP-007 R5.3.3 / CIP-007-5 R5.6
- CIP-007 R6.2 / CIP-007-5 R4.2
- CIP-007 R6.5 / CIP-007-5 R4.4

CIP-008: Cyber Security — Incident Reporting and Response Planning

Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered as CIP-002 through CIP-009.

CIP-008: Cyber Security Requirements

- R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:
  - R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
  - R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.
  - R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.
  - R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.
  - R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
  - R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can be a paper drill or a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.
- R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

CIP-008: Cyber Security Measures

- M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.
- M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

CIP-008: Cyber Security Illustrative Approach

An internal cyber security response center serves as a central location for the analysis and investigation of potential security incidents. In that role, the cyber security response center should consider, evaluate, and respond to both external threats and internal vulnerabilities.

Sources of external threat information include industry information sharing and analysis centers such as Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Infraguard, mailing lists, and commercial reporting services.

Internal vulnerability information is available from condition reporting and activity monitoring. Cyber security response teams should be able to access all relevant internal vulnerability information in a

read-only format. Such data may reside in centralized log repositories, on the devices that perform the logging, and in results of self-assessments and independent tests. Security response centers also should have available tools to analyze the logs and to perform ad hoc activity monitoring. Other additional and useful data sources are reports of anomalies in both network and host performance and the end-user experience.

Because the identification of incidents requires monitoring and management, response teams frequently use security information management (SIM) tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents.

The cyber security response team should be governed by policies and procedures that address security incidents:

- M1. Monitoring policies should enable adequate continual and ad hoc monitoring of communications and the use of the results of monitoring in subsequent legal procedures. The responsibility and authority of security personnel and system administrators for monitoring should be established, and the tools used should be reviewed and approved by appropriate management with appropriate conditions for use.
- M2. Classification policies should be sufficiently clear to enable timely classification of incidents into different levels of severity. Response and reporting levels should be commensurate with the severity levels.
- M3. Escalation policies should address when different personnel within the organization will be contacted about the incident and the responsibility those personnel have in incident analysis and response.
- M4. Reporting policies should address internal and external reporting, including coordination with service providers and reporting to ES-ISAC.

In addition, a policy should address who is empowered to declare an incident to be an intrusion.

At a minimum, each entity should tests its incident response plan at least annually. Such testing should validate that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. Employees should take what action would be required under the response plan, given the hypothetical incident. When reviewing actual incidents or testing the incident response plan, the entity should document lessons learned and incorporate appropriate changes to the plan, as needed.

The effectiveness of a cyber security incident response team also is a function of the training and expertise of the security analysts. An entity should ensure that its analysts are sufficiently trained to appropriately analyze network and host activity and to use the monitoring and analysis tools made available to them.

CIP-008 Reports and Alerts

There are no TIBCO LogLogic Compliance Suite Reports and Alerts for Incident Reporting and Response Planning.

CIP-009: Cyber Security — Recovery Plans for BES Cyber Systems

To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

CIP-009: Cyber Security Requirements

- R1. Recovery Plans - The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
  - R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

  - R1.2. Define the roles and responsibilities of responders.
- R2. Exercises - The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.
- R3. Change Control - Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days after the change is carried out.
- R4. Backup and Restore - The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, and tape backup.
- R5. Testing Backup Media - Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off-site.

CIP-009: Cyber Security Measures

- M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.
- M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.
- M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.
- M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.
- M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

CIP-009: Cyber Security Illustrative Approach

Entities should ensure that recovery plans for critical cyber assets follow established business continuity and disaster recovery techniques and practices. The recovery of critical cyber assets and the Bulk-Power System is of short-term critical importance. The Bulk-Power System and its critical cyber assets play a crucial role in the overall economy and our critical infrastructure. Disruptions in service should be minimized to maintain public trust and confidence in the power system. As such, responsible entities should incorporate business continuity considerations into the overall design of their business model to proactively mitigate the risk of service disruptions and recovery as quickly as possible, if disruptions occur.

Changes in business processes and technology, increased terrorism concerns, catastrophic natural disasters, and the threat of a pandemic have focussed even greater attention on the need for effective business continuity planning. Consequently, these issues should be given greater consideration in the business continuity planning process.

Responsible entities should consider the potential for area-wide disasters that could affect an entire region and result in significant loss of service to the Bulk-Power System. The business continuity planning process should address interdependencies, both market-based and geographic, among system participants and infrastructure service providers. In most cases, recovery time objectives (RTOs) are now much shorter than they were in years past, and for most entities RTOs are based on hours, minutes, and even seconds. Ultimately, all entities should anticipate and plan for the unexpected and ensure that their recovery and business continuity planning process appropriately addresses the lessons they have learned from past incidents and disasters.

Events that trigger the implementation of a business continuity plan may also have significant security implications. Depending on the event, some or all of the elements of the security environment may

change. Different people may be involved in operations, at different physical locations, using similar but different machines and software, which may communicate over different communications lines. Different trade-offs may exist between availability, integrity, confidentiality, and accountability, with a different appetite for risk on the part of management.

Recovery and business continuity plans should be reviewed as an integral part of the security process. For example, risk assessments should consider the changing risks that appear in business continuity scenarios and the different security posture that may be established. Strategies should consider the different risk environment and the degree of risk mitigation necessary to protect the entity and its critical cyber assets in the event the continuity plans must be implemented. The implementation should consider the training of appropriate personnel in their security roles, and the implementation and updating of technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of business continuity plan implementations.

A responsible entities recovery and business continuity planning process should reflect the following objectives:

- The business continuity planning process should include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components;
- Business continuity planning involves the development of an enterprise-wide business continuity planning and the prioritization of business objectives and critical operations that are essential for recovery;
- Recovery and business continuity planning should include regular updates based on changes in business processes, audit recommendations, and lessons learned from testing; and
- Business continuity planning represents a cyclical, process-oriented approach that includes business impact analysis (BIA), risk assessment, risk management, and risk monitoring and testing.

The following additional practices are commonly used to maintain a recovery and business continuity plan:

- Integrating business continuity planning into every business decision
- Incorporating business continuity planning maintenance responsibilities in applicable employee job descriptions and personnel evaluations
- Assigning the responsibility for periodic review of the business continuity planning to a planning coordinator, department, group, or committee
- Performing regular audits and annual, or more frequent, tests of the recovery and business continuity planning

CIP-009 Reports and Alerts

There are no TIBCO LogLogic Compliance Suite Reports and Alerts for Recovery Plans for Critical Cyber Assets.

TIBCO LogLogic Reports and Alerts for NERC

The Compliance Suite - NERC Edition is delivered as an XML file that is imported into the appliance by the user. The Compliance Suite - NERC Edition uses the existing TIBCO LogLogic Search Framework.

TIBCO LogLogic Reports for NERC

The following table lists the reports included in the LogLogic® Compliance Suite - NERC Edition.

Serial Number	TIBCO LogLogic Report	Description
1	NERC: Account Activities on UNIX Servers	Displays all account activities on UNIX servers to ensure authorized and appropriate access.
2	NERC: Account Activities on Windows Servers	Displays all account activities on Windows servers to ensure authorized and appropriate access.
3	NERC: Accounts Changed on NetApp Filer	Displays all accounts changed on NetApp Filer to ensure authorized and appropriate access.
4	NERC: Accounts Changed on TIBCO Administrator	Displays all accounts changed on TIBCO Administrator to ensure authorized and appropriate access.
5	NERC: Accounts Changed on TIBCO ActiveMatrix Administrator	Displays all accounts changed on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
6	NERC: Accounts Changed on UNIX Servers	Displays all accounts changed on UNIX servers to ensure authorized and appropriate access.
7	NERC: Accounts Changed on Windows Servers	Displays all accounts changed on Windows servers to ensure authorized and appropriate access.
8	NERC: Accounts Created on NetApp Filer	Displays all accounts created on NetApp Filer to ensure authorized and appropriate access.
9	NERC: Accounts Created on NetApp Filer Audit	Displays all accounts created on NetApp Filer Audit to ensure authorized and appropriate access.
10	NERC: Accounts Created on Symantec Endpoint Protection	Displays all accounts created on Symantec Endpoint Protection to ensure authorized and appropriate access.
11	NERC: Accounts Created on TIBCO Administrator	Displays all accounts created on TIBCO Administrator to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
12	NERC: Accounts Created on TIBCO ActiveMatrix Administrator	Displays all accounts created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
13	NERC: Accounts Created on Sidewinder	Displays all accounts created on Sidewinder to ensure authorized and appropriate access.
14	NERC: Accounts Created on UNIX Servers	Displays all accounts created on UNIX servers to ensure authorized and appropriate access.
15	NERC: Accounts Created on Windows Servers	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
16	NERC: Accounts Deleted on NetApp Filer	Displays all accounts deleted on NetApp Filer to ensure authorized and appropriate access.
17	NERC: Accounts Deleted on NetApp Filer Audit	Displays all accounts deleted on NetApp Filer Audit to ensure authorized and appropriate access.
18	NERC: Accounts Deleted on Sidewinder	Displays all accounts deleted on Sidewinder to ensure authorized and appropriate access.
19	NERC: Accounts Deleted on Symantec Endpoint Protection	Displays all accounts deleted on Symantec Endpoint Protection to ensure authorized and appropriate access.
20	NERC: Accounts Deleted on TIBCO Administrator	Displays all accounts deleted on TIBCO Administrator to ensure authorized and appropriate access.
21	NERC: Accounts Deleted on TIBCO ActiveMatrix Administrator	Displays all accounts deleted on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
22	NERC: Accounts Deleted on UNIX Servers	Displays all accounts deleted on UNIX servers to ensure authorized and appropriate access.
23	NERC: Accounts Deleted on Windows Servers	Displays all accounts deleted on Windows servers to ensure authorized and appropriate access.
24	NERC: Active Connections for Cisco ASA	Displays all currently active firewall connections for Cisco ASA.
25	NERC: Active Connections for Cisco FWSM	Displays all currently active firewall connections for Cisco FWSM.
26	NERC: Active Connections for Cisco PIX	Displays all currently active firewall connections for Cisco PIX.
27	NERC: Active Directory System Changes	Displays changes made within Active Directory.

Serial Number	TIBCO LogLogic Report	Description
28	NERC: Active VPN Connections for Cisco VPN Concentrators	Displays all currently active VPN connections for Cisco VPN Concentrators.
29	NERC: Active VPN Connections for Nortel Contivity	Displays all currently active VPN connections for Nortel Contivity VPN devices.
30	NERC: Active VPN Connections for RADIUS	Displays all currently active VPN connections for RADIUS Acct Client.
31	NERC: Administrator Logins on Windows Servers	Displays all logins with the administrator account on Windows servers.
32	NERC: Allowed URLs by Source IPs	Displays successful access to URLs by source IP addresses.
33	NERC: Allowed URLs by Source IPs - F5 BIG-IP TMOS	Displays successful access to URLs by source IP addresses on F5 BIG-IP TMOS.
34	NERC: Allowed URLs by Source IPs - Microsoft IIS	Displays successful access to URLs by source IP addresses on Microsoft IIS.
35	NERC: Allowed URLs by Source Users - F5 BIG-IP TMOS	Displays successful access to URLs by source users on F5 BIG-IP TMOS.
36	NERC: Allowed URLs by Source Users - Microsoft IIS	Displays successful access to URLs by source users on Microsoft IIS.
37	NERC: Allowed URLs by Source Users	Displays successful access to URLs by source users.
38	NERC: Attackers by Service	Displays all attack source IP address and service ports.
39	NERC: Attackers by Service - Cisco IOS	Displays all attack source IP address and service ports by Cisco IOS.
40	NERC: Attackers by Service - FireEye MPS	Displays all attack source IP address and service ports by FireEye MPS.
41	NERC: Attackers by Service - ISS SiteProtector	Displays all attack source IP address and service ports by ISS SiteProtector.
42	NERC: Attackers by Service - SiteProtector	Displays all attack source IP address and service ports by SiteProtector.
43	NERC: Attackers by Service - Sourcefire Defense Center	Displays all attack source IP address and service ports by Sourcefire Defense Center.

Serial Number	TIBCO LogLogic Report	Description
44	NERC: Attackers by Signature - ISS SiteProtector	Displays all attack source IP address and signatures by ISS SiteProtector.
45	NERC: Attackers by Signature - SiteProtector	Displays all attack source IP address and signatures by SiteProtector.
46	NERC: Attackers by Signature	Displays all attack source IP address and signatures.
47	NERC: Attackers by Signature - Cisco IOS	Displays all attack source IP address and signatures by Cisco IOS.
48	NERC: Attackers by Signature - Sourcefire Defense Center	Displays all attack source IP address and signatures by Sourcefire Defense Center.
49	NERC: Attackers by Signature - FireEye MPS	Displays all attack source IP address and signatures by FireEye MPS.
50	NERC: Attacks Detected	Displays all IDS attacks detected against servers and applications.
51	NERC: Attacks Detected - Cisco IOS	Displays all IDS attacks detected against servers and applications by Cisco IOS.
52	NERC: Attacks Detected - HIPS	Displays all IPS attacks detected against servers and applications.
53	NERC: Attacks Detected - ISS SiteProtector	Displays all IDS attacks detected against servers and applications by ISS SiteProtector.
54	NERC: Attacks Detected - SiteProtector	Displays all IDS attacks detected against servers and applications by SiteProtector.
55	NERC: Attacks Detected - Sourcefire Defense Center	Displays all IDS attacks detected against servers and applications by Sourcefire Defense Center.
56	NERC: Bandwidth Usage by User	Displays users who are using the most bandwidth.
57	NERC: Blocked URLs by Source IPs	Displays URLs that have been blocked by source IP addresses.
58	NERC: Blocked URLs by Source IPs - F5 BIG-IP TMOS	Displays URLs that have been blocked by source IP addresses on F5 BIG-IP TMOS.
59	NERC: Blocked URLs by Source IPs - Microsoft IIS	Displays URLs that have been blocked by source IP addresses on Microsoft IIS.
60	NERC: Blocked URLs by Source Users	Displays URLs that have been blocked by source users.

Serial Number	TIBCO LogLogic Report	Description
61	NERC: Blocked URLs by Source Users - F5 BIG-IP TMOS	Displays URLs that have been blocked by source users on F5 BIG-IP TMOS.
62	NERC: Blocked URLs by Source Users - Microsoft IIS	Displays URLs that have been blocked by source users on Microsoft IIS.
63	NERC: Check Point Configuration Changes	Displays all Check Point audit events related to configuration changes.
64	NERC: Cisco ESA: Attacks by Event ID	Displays Cisco ESA attacks by Event ID.
65	NERC: Cisco ESA: Attacks Detected	Displays attacks detected by Cisco ESA.
66	NERC: Cisco ESA: Attacks by Threat Name	Displays Cisco ESA Attacks by threat name.
67	NERC: Cisco ESA: Scans	Displays scans using Cisco ESA.
68	NERC: Cisco ESA: Updated	Displays updates to Cisco ESA.
69	NERC: Cisco ISE, ACS Accounts Created	Displays all accounts created on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
70	NERC: Cisco ISE, ACS Accounts Removed	Displays all accounts removed on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
71	NERC: Cisco ISE, ACS Configuration Changes	Displays Cisco ISE and Cisco SecureACS configuration changes.
72	NERC: Cisco ISE, ACS Password Changes	Displays all password change activities on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
73	NERC: Cisco PIX, ASA, FWSM Policy Changed	Displays all configuration changes made to the Cisco PIX, ASA, and FWSM devices.
74	NERC: Cisco PIX, ASA, FWSM Failover Disabled	Displays all logs related to disabling Cisco PIX, ASA, and FWSM failover capability.
75	NERC: Cisco PIX, ASA, FWSM Failover Performed	Displays all logs related to performing a Cisco PIX, ASA, or FWSM failover.
76	NERC: Cisco PIX, ASA, FWSM Restarted	Displays all Cisco PIX, ASA, or FWSM restart activities to detect unusual activities.
77	NERC: Cisco Switch Policy Changes	Displays all configuration changes to the Cisco router and switch policies.

Serial Number	TIBCO LogLogic Report	Description
78	NERC: DB2 Database Configuration Changes	Displays DB2 database configuration changes.
79	NERC: DB2 Database Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
80	NERC: DB2 Database Successful Logins	Displays successful DB2 database logins.
81	NERC: DB2 Database User Additions and Deletions	Displays IBM DB2 Database events related to creation and deletion of database users.
82	NERC: Denied Connections by IP Addresses	Displays remote IP addresses with the most denied connections.
83	NERC: Denied Connections - Cisco IOS	Displays all connections that have been denied by the Cisco IOS devices.
84	NERC: Denied Connections - Cisco NXOS	Displays all connections that have been denied by the Cisco NXOS devices.
85	NERC: Denied Connections - F5 BIG-IP TMOS	Displays all connections that have been denied by the F5 BIG-IP TMOS devices.
86	NERC: Denied Connections - Cisco Router	Displays all connections that have been denied by the Cisco Router devices.
87	NERC: Denied Connections - Sidewinder	Displays all connections that have been denied by the Sidewinder devices.
88	NERC: Denied Connections - VMware vShield	Displays all connections that have been denied by the VMware vShield devices.
89	NERC: Denied Inbound Connections - Check Point	Displays all inbound connections that have been denied by the Check Point devices.
90	NERC: Denied Inbound Connections - Cisco ASA	Displays all inbound connections that have been denied by the Cisco ASA devices.
91	NERC: Denied Inbound Connections - Cisco FWSM	Displays all inbound connections that have been denied by the Cisco FWSM devices.
92	NERC: Denied Inbound Connections - Cisco PIX	Displays all inbound connections that have been denied by the Cisco PIX devices.
93	NERC: Denied Inbound Connections - Juniper Firewall	Displays all inbound connections that have been denied by the Juniper Firewalls.
94	NERC: Denied Outbound Connections - Check Point	Displays all outbound connections that have been denied by the Check Point.

Serial Number	TIBCO LogLogic Report	Description
95	NERC: Denied Outbound Connections - Cisco ASA	Displays all outbound connections that have been denied by the Cisco ASA.
96	NERC: Denied Outbound Connections - Cisco FWSM	Displays all outbound connections that have been denied by the Cisco FWSM.
97	NERC: Denied Outbound Connections - Cisco PIX	Displays all outbound connections that have been denied by the Cisco PIX.
98	NERC: Denied Outbound Connections - Juniper Firewall	Displays all outbound connections that have been denied by the Juniper Firewall.
99	NERC: DHCP Activities on Microsoft DHCP	Displays all DHCP activities on Microsoft DHCP Server.
100	NERC: DHCP Activities on VMware vShield	Displays all DHCP activities on VMware vShield Edge.
101	NERC: DNS Server Error	Displays all events when DNS server has errors.
102	NERC: Domain activities on Symantec Endpoint Protection	Displays all domain activities on Symantec Endpoint Protection.
103	NERC: Escalated Privilege Activities on Servers	Displays all privilege escalation activities performed on servers to ensure appropriate access.
104	NERC: ESX Accounts Activities	Displays all account activities on VMware ESX servers to ensure authorized and appropriate access.
105	NERC: ESX Accounts Created	Displays all accounts created on VMware ESX servers to ensure authorized and appropriate access.
106	NERC: ESX Accounts Deleted	Displays all accounts deleted on VMware ESX servers to ensure authorized and appropriate access.
107	NERC: ESX Failed Logins	Failed VMware ESX logins for known user.
108	NERC: ESX Group Activities	Displays all group activities on VMware ESX servers to ensure authorized and appropriate access.
109	NERC: ESX Kernel log daemon terminating	Displays all VMware ESX kernel log daemon terminating.
110	NERC: ESX Kernel logging Stop	Displays all VMware ESX kernel logging stops.
111	NERC: ESX Logins Failed Unknown User	Failed VMware ESX logins for unknown user.
112	NERC: ESX Logins Succeeded	Displays successful logins to VMware ESX to ensure only authorized personnel have access.

Serial Number	TIBCO LogLogic Report	Description
113	NERC: F5 BIG-IP TMOS Login Failed	Displays all F5 BIG-IP TMOS login events that have failed.
114	NERC: F5 BIG-IP TMOS Login Successful	Displays all F5 BIG-IP TMOS login events that have succeeded.
115	NERC: F5 BIG-IP TMOS Password Changes	Displays all password change activities on F5 BIG-IP TMOS to ensure authorized and appropriate access.
116	NERC: F5 BIG-IP TMOS Restarted	Displays all events when the F5 BIG-IP TMOS is restarted.
117	NERC: ESX Syslogd Restart	Displays all VMware ESX syslogd restarts.
118	NERC: Files Accessed on NetApp Filer Audit	Displays all files accessed on NetApp Filer Audit to ensure appropriate access.
119	NERC: Files Downloaded via Proxy - Microsoft IIS	Displays all proxy-based downloads to ensure authorized and appropriate access on Microsoft IIS.
120	NERC: Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
121	NERC: Files Accessed on Servers	Displays all files accessed on servers to ensure appropriate access.
122	NERC: Files Accessed through Juniper SSL VPN (Secure Access)	Displays all files Accessed through Juniper SSL VPN (Secure Access).
123	NERC: Files Accessed through PANOS	Displays all files Accessed through Palo Alto Networks.
124	NERC: Files Downloaded via Proxy	Displays all proxy-based downloads to ensure authorized and appropriate access.
125	NERC: Files Downloaded via Proxy - Blue Coat Proxy	Displays all proxy-based downloads to ensure authorized and appropriate access on Blue Coat Proxy.
126	NERC: Files Downloaded via Proxy - Cisco WSA	Displays all proxy-based downloads to ensure authorized and appropriate access on Cisco WSA.
127	NERC: Files Downloaded via the Web	Displays all web-based downloads to ensure authorized and appropriate access.
128	NERC: Files Downloaded via the Web - F5 BIG-IP TMOS	Displays all web-based downloads to ensure authorized and appropriate access on F5 BIG-IP TMOS.

Serial Number	TIBCO LogLogic Report	Description
129	NERC: Files Downloaded via the Web - Microsoft IIS	Displays all web-based downloads ensure authorized and appropriate access on Microsoft IIS.
130	NERC: Files Uploaded via Proxy	Displays all proxy-based uploads to ensure only authorized data can be uploaded.
131	NERC: Files Uploaded via Proxy - Blue Coat Proxy	Displays all proxy-based uploads to ensure only authorized data can be uploaded on Blue Coat Proxy.
132	NERC: Files Uploaded via Proxy - Cisco WSA	Displays all proxy-based uploads to ensure only authorized data can be uploaded on Cisco WSA.
133	NERC: Files Uploaded via Proxy - Microsoft IIS	Displays all proxy-based uploads to ensure only authorized data can be uploaded on Microsoft IIS.
134	NERC: Files Uploaded via the Web	Displays all web-based uploads to ensure only authorized data can be uploaded.
135	NERC: Files Uploaded via the Web - F5 BIG-IP TMOS	Displays all web-based uploads to ensure only authorized data can be uploaded on F5 BIG-IP TMOS.
136	NERC: Files Uploaded via the Web - Microsoft IIS	Displays all web-based uploads to ensure only authorized data can be uploaded on Microsoft IIS.
137	NERC: FortiOS: Attacks Detected	Displays attacks detected by FortiOS.
138	NERC: FortiOS: Attacks by Event ID	Displays FortiOS attacks by Event ID.
139	NERC: FortiOS: Attacks by Threat Name	Displays FortiOS attacks by threat name.
140	NERC: FortiOS DLP Attacks Detected	Displays all DLP attacks detected by FortiOS.
141	NERC: Group Activities on NetApp Filer Audit	Displays all group activities on NetApp Filer Audit to ensure authorized and appropriate access.
142	NERC: Group Activities on Symantec Endpoint Protection	Displays all group activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
143	NERC: Group Activities on TIBCO ActiveMatrix Administrator	Displays all group activities on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
144	NERC: Group Activities on UNIX Servers	Displays all group activities on UNIX servers to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
145	NERC: Group Activities on Windows Servers	Displays all group activities on Windows servers to ensure authorized and appropriate access.
146	NERC: Guardium SQL Guard Audit Configuration Changes	Displays all configuration changes on the Guardium SQL Guard Audit database.
147	NERC: Guardium SQL Guard Audit Logins	Displays all login attempts to the Guardium SQL Server Audit database.
148	NERC: Guardium SQL Guard Configuration Changes	Displays all configuration changes on the Guardium SQL Guard database.
149	NERC: Guardium SQL Guard Logins	Displays all login attempts to the Guardium SQL Server database.
150	NERC: HP NonStop Audit Configuration Changes	Displays all audit configuration changes on HP NonStop.
151	NERC: HP NonStop Audit Login Failed	Displays all HP NonStop Audit login events that have failed.
152	NERC: HP NonStop Audit Login Successful	Displays all HP NonStop Audit login events that have succeeded.
153	NERC: HP NonStop Audit Object Access	Displays HP NonStop Audit events related to object access.
154	NERC: HP NonStop Audit Object Changes	Displays HP NonStop Audit events related to object changes.
155	NERC: HP NonStop Audit Permissions Changed	Displays all permission modification activities on HP NonStop Audit to ensure authorized access.
156	NERC: Files Accessed through Pulse Connect Secure	Displays all files accessed through Pulse Connect Secure.
157	NERC: i5/OS Access Control List Modifications	Displays i5/OS events related to access control list modification.
158	NERC: i5/OS Audit Configuration Changes	Displays all audit configuration changes on i5/OS.
159	NERC: i5/OS DST Password Reset	Displays i5/OS events related to the reset of the DST (Dedicated Service Tools) password.
160	NERC: i5/OS Object Access	Displays i5/OS events related to object access.
161	NERC: i5/OS Restore Events	Displays i5/OS events related to object, program, and profile restoration.

Serial Number	TIBCO LogLogic Report	Description
162	NERC: i5/OS System Management Changes	Displays i5/OS events related to system management changes.
163	NERC: i5/OS User Profile Creation, Modification, or Restoration	Displays i5/OS events related to user profile creation, modification, or restoration.
164	NERC: Juniper Firewall HA State Changed	Displays all Juniper Firewall failover state change events.
165	NERC: Juniper Firewall Policy Changed	Displays all configuration changes to the Juniper Firewall policies.
166	NERC: Juniper Firewall Policy Out of Sync	Displays events indicating that the Juniper Firewall's HA policies are out of sync.
167	NERC: Juniper Firewall Reset Accepted	Displays events indicating that the Juniper Firewall is reset to its factory default state.
168	NERC: Juniper Firewall Reset Imminent	Displays events that indicate the Juniper Firewall will be reset to its factory default state.
169	NERC: FireEye MPS: Attacks by Event ID	Displays FireEye MPS attacks by Event ID.
170	NERC: FireEye MPS: Attacks by Threat Name	Displays FireEye MPS attacks by threat name.
171	NERC: FireEye MPS: Attacks Detected	Displays attacks detected by FireEye MPS.
172	NERC: Last Activities Performed by Administrators	Displays the latest activities performed by administrators and root users to ensure appropriate access.
173	NERC: Last Activities Performed by All Users	Displays the latest activities performed by all users to ensure appropriate access.
174	NERC: Logins by Authentication Type	Displays all logins categorized by the authentication type.
175	NERC: LogLogic DSM Configuration Changes	Displays all configuration changes on the LogLogic DSM database.
176	NERC: LogLogic DSM Logins	Displays all login attempts to the LogLogic DSM database.
177	NERC: LogLogic Management Center Account Activities	Displays all account activities on LogLogic management center to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
178	NERC: LogLogic Management Center Login	Displays all login events to the LogLogic management center.
179	NERC: LogLogic Management Center Password Changes	Displays all password change activities on LogLogic management center to ensure authorized and appropriate access.
180	NERC: LogLogic Management Center Restore Activities	Displays all restore activities on LogLogic management center.
181	NERC: LogLogic Universal Collector Configuration Changes	Displays LogLogic universal collector configuration changes.
182	NERC: McAfee Antivirus: Attacks Detected	Displays attacks detected by McAfee AntiVirus.
183	NERC: McAfee AntiVirus: Attacks by Event ID	Displays McAfee AntiVirus attacks by Event ID.
184	NERC: McAfee AntiVirus: Attacks by Threat Name	Displays McAfee AntiVirus Attacks by threat name.
185	NERC: Microsoft Operations Manager - Windows Accounts Activities	Displays all account activities on Windows servers to ensure authorized and appropriate access.
186	NERC: Microsoft Operations Manager - Windows Accounts Changed	Displays all accounts changed on Windows servers to ensure authorized and appropriate access.
187	NERC: Microsoft Operations Manager - Windows Accounts Created	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
188	NERC: Microsoft Operations Manager - Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.
189	NERC: Microsoft Operations Manager - Windows Events by Users	Displays a summary of access-related Windows events by source and target users.
190	NERC: Microsoft Operations Manager - Windows Password Changes	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
191	NERC: Microsoft Operations Manager - Windows Permissions Modified	Displays all permission modification activities on Windows servers to ensure authorized access.

Serial Number	TIBCO LogLogic Report	Description
192	NERC: Microsoft Operations Manager - Windows Policies Modified	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
193	NERC: Microsoft Sharepoint Content Deleted	Displays all events when content is deleted from Microsoft SharePoint.
194	NERC: Microsoft Sharepoint Content Updates	Displays all events when content is updated within Microsoft SharePoint.
195	NERC: Microsoft Sharepoint Permissions Changed	Displays all user/group permission events to Microsoft SharePoint.
196	NERC: Microsoft Sharepoint Policy Add, Remove, or Modify	Displays all events when a Microsoft SharePoint policy is added, removed, or modified.
197	NERC: Microsoft SQL Server Configuration Changes	Displays Microsoft SQL database configuration changes.
198	NERC: Microsoft SQL Server Database Failed Logins	Displays failed Microsoft SQL Server database logins.
199	NERC: Microsoft SQL Server Database Successful Logins	Displays successful Microsoft SQL Server database logins.
200	NERC: Microsoft SQL Server Database Permission Events	Displays events related to Microsoft SQL Server database permission modifications.
201	NERC: Microsoft SQL Server Database User Additions and Deletions	Displays Microsoft SQL Server events related to creation and deletion of database users.
202	NERC: Microsoft SQL Server Password Changes	Displays password changes for Microsoft SQL Server database accounts.
203	NERC: Most Active Ports Through Firewall - Check Point	Displays the most active ports used through the Check Point firewall.
204	NERC: Most Active Ports Through Firewall - Cisco ASA	Displays the most active ports used through the Cisco ASA firewall.
205	NERC: Most Active Ports Through Firewall - Cisco FWSM	Displays the most active ports used through the Cisco FWSM firewall.
206	NERC: Most Active Ports Through Firewall - Cisco PIX	Displays the most active ports used through the Cisco PIX firewall.
207	NERC: Most Active Ports Through Firewall - Fortinet	Displays the most active ports used through the Fortinet firewall.

Serial Number	TIBCO LogLogic Report	Description
208	NERC: Most Active Ports Through Firewall - Juniper Firewall	Displays the most active ports used through the Juniper Firewall.
209	NERC: Most Active Ports Through Firewall - Nortel	Displays the most active ports used through the Nortel firewall.
210	NERC: NetApp Filer Accounts Locked	Displays all accounts locked out of NetApp Filer to detect access violations or unusual activities.
211	NERC: NetApp Filer Audit Accounts Enabled	Displays all accounts enabled on NetApp Filer Audit to ensure authorized and appropriate access.
212	NERC: NetApp Filer Audit Group Members Added	Displays all accounts added to groups on NetApp Filer Audit to ensure appropriate access.
213	NERC: NetApp Filer Audit Group Members Deleted	Displays all accounts removed from groups on NetApp Filer Audit to ensure appropriate access.
214	NERC: NetApp Filer File Activity	Displays all file activities on NetApp Filer.
215	NERC: NetApp Filer Login Failed	Displays all NetApp Filer login events that have failed.
216	NERC: NetApp Filer Login Successful	Displays all NetApp Filer login events that have succeeded.
217	NERC: NetApp Filer Password Changes	Displays all password change activities on NetApp Filer to ensure authorized and appropriate access.
218	NERC: NetApp Filer Audit Login Failed	Displays all NetApp Filer Audit login events that have failed.
219	NERC: NetApp Filer Audit Login Successful	Displays all NetApp Filer Audit login events that have succeeded.
220	NERC: NetApp Filer Audit Policies Modified	Displays all policy modification activities on NetApp Filer Audit to ensure authorized and appropriate access.
221	NERC: Novell eDirectory Password Changes	Password changes on Novell eDirectory.
222	NERC: Oracle Database Configuration Changes	Displays Oracle database configuration changes.
223	NERC: Oracle Database Failed Logins	Displays failed login attempts to the Oracle database.

Serial Number	TIBCO LogLogic Report	Description
224	NERC: Oracle Database Successful Logins	Displays successful Oracle database login attempts.
225	NERC: Oracle Database Permission Events	Displays events related to Oracle Server database role and privilege management.
226	NERC: Oracle Database User Additions and Deletions	Displays Oracle database events related to creation and deletion of database users.
227	NERC: Password Changes on Windows Servers	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
228	NERC: PANOS: Attacks Detected	Displays attacks detected by Palo Alto Networks.
229	NERC: PANOS: Attacks by Event ID	Displays Palo Alto Networks attacks by Event ID.
230	NERC: PANOS: Attacks by Threat Name	Displays Palo Alto Networks attacks by threat name.
231	NERC: Periodic Review of Log Reports	Displays all review activities performed by administrators to ensure review for any access violations.
232	NERC: Periodic Review of User Access Logs	Displays all review activities performed by administrators to ensure review for any access violations.
233	NERC: Permissions Modified on Windows Servers	Displays all permission modification activities on Windows Servers to ensure authorized access.
234	NERC: Policies Modified on Windows Servers	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
235	NERC: Ports Allowed Access - Check Point	Displays all connections passed through the Check Point by port.
236	NERC: Ports Allowed Access - Cisco ASA	Displays all connections passed through the Cisco ASA by port.
237	NERC: Ports Allowed Access - Cisco IOS	Displays all connections passed through the Cisco IOS by port.
238	NERC: Ports Allowed Access - Cisco FWSM	Displays all connections passed through the Cisco FWSM by port.
239	NERC: Ports Allowed Access - Cisco Netflow	Displays all connections passed through the Cisco Netflow by port.

Serial Number	TIBCO LogLogic Report	Description
240	NERC: Ports Allowed Access - Cisco PIX	Displays all connections passed through the Cisco PIX by port.
241	NERC: Ports Allowed Access - F5 BIG-IP TMOS	Displays all connections passed through the F5 BIG-IP TMOS by port.
242	NERC: Ports Allowed Access - Fortinet	Displays all connections passed through the Fortinet by port.
243	NERC: Ports Allowed Access - Juniper Firewall	Displays all connections passed through the Juniper Firewall by port.
244	NERC: Ports Allowed Access - Juniper JunOS	Displays all connections passed through the Juniper JunOS by port.
245	NERC: Ports Allowed Access - Juniper RT Flow	Displays all connections passed through the Juniper RT Flow by port.
246	NERC: Ports Allowed Access - Nortel	Displays all connections passed through the Nortel by port.
247	NERC: Ports Allowed Access - PANOS	Displays all connections passed through the Palo Alto Networks by port.
248	NERC: Ports Allowed Access - Sidewinder	Displays all connections passed through the Sidewinder by port.
249	NERC: Ports Allowed Access - VMware vShield	Displays all connections passed through the VMware vShield by port.
250	NERC: Ports Denied Access - Check Point	Displays the applications that have been denied access the most by the Check Point.
251	NERC: Ports Denied Access - Cisco ASA	Displays the applications that have been denied access the most by the Cisco ASA.
252	NERC: Ports Denied Access - Cisco FWSM	Displays the applications that have been denied access the most by the Cisco FWSM.
253	NERC: Ports Denied Access - Cisco IOS	Displays the applications that have been denied access the most by the Cisco IOS.
254	NERC: Ports Denied Access - Cisco PIX	Displays the applications that have been denied access the most by the Cisco PIX.
255	NERC: Ports Denied Access - Cisco Router	Displays the applications that have been denied access the most by the Cisco Router.
256	NERC: Ports Denied Access - F5 BIG-IP TMOS	Displays the applications that have been denied access the most by the F5 BIG-IP TMOS.

Serial Number	TIBCO LogLogic Report	Description
257	NERC: Ports Denied Access - Fortinet	Displays the applications that have been denied access the most by the Fortinet.
258	NERC: Ports Denied Access - Juniper Firewall	Displays the applications that have been denied access the most by the Juniper Firewall.
259	NERC: Ports Denied Access - Juniper JunOS	Displays the applications that have been denied access the most by the Juniper JunOS.
260	NERC: Ports Denied Access - Juniper RT Flow	Displays the applications that have been denied access the most by the Juniper RT Flow.
261	NERC: Ports Denied Access - Nortel	Displays the applications that have been denied access the most by the Nortel.
262	NERC: Ports Denied Access - PANOS	Displays the applications that have been denied access the most by the Palo Alto Networks.
263	NERC: Ports Denied Access - Sidewinder	Displays the applications that have been denied access the most by the Sidewinder.
264	NERC: Ports Denied Access - VMware vShield	Displays the applications that have been denied access the most by the VMware vShield Edge.
265	NERC: RACF Accounts Created	Displays all accounts created on RACF servers to ensure authorized and appropriate access.
266	NERC: RACF Accounts Deleted	Displays all accounts deleted on RACF servers to ensure authorized and appropriate access.
267	NERC: RACF Accounts Modified	Displays all events when a network user profile is modified.
268	NERC: RACF Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
269	NERC: RACF Files Accessed	Displays all files accessed on RACF servers to ensure appropriate access.
270	NERC: RACF Password Changed	Displays all password change activities on RACF servers to ensure authorized and appropriate access.
271	NERC: RACF Permissions Changed	Displays all permission modification activities on RACF to ensure authorized access.
272	NERC: RACF Successful Logins	Displays successful logins to ensure only authorized personnel have access.
273	NERC: Root Logins	Displays root logins.

Serial Number	TIBCO LogLogic Report	Description
274	NERC: Sensors Generating Alerts	Displays the IDS sensors that generated the most alerts.
275	NERC: Sensors Generating Alerts - FireEye MPS	Displays the IDS sensors that generated the most alerts by FireEye MPS.
276	NERC: Sensors Generating Alerts - Cisco IOS	Displays the IDS sensors that generated the most alerts by Cisco IOS.
277	NERC: Sensors Generating Alerts - ISS SiteProtector	Displays the IDS sensors that generated the most alerts by ISS SiteProtector.
278	NERC: Sensors Generating Alerts - SiteProtector	Displays the IDS sensors that generated the most alerts by SiteProtector.
279	NERC: Sensors Generating Alerts - Sourcefire Defense Center	Displays the IDS sensors that generated the most alerts by Sourcefire Defense Center.
280	NERC: Sidewinder Configuration Changes	Displays Sidewinder configuration changes.
281	NERC: Successful Logins	Displays successful logins to ensure only authorized personnel have access.
282	NERC: Sybase ASE Database Configuration Changes	Displays configuration changes to the Sybase database.
283	NERC: Sybase ASE Database User Additions and Deletions	Displays Sybase database events related to creation and deletion of database users.
284	NERC: Sybase ASE Failed Logins	Displays failed Sybase ASE database logins.
285	NERC: Sybase ASE Successful Logins	Displays successful Sybase ASE database logins.
286	NERC: Symantec AntiVirus: Attacks by Event ID	Displays all Symantec AntiVirus Attacks by Event ID events.
287	NERC: Symantec AntiVirus: Attacks by Threat Name	Displays Symantec AntiVirus attacks by threat name.
288	NERC: Symantec AntiVirus: Attacks Detected	Displays attacks detected by Symantec AntiVirus.
289	NERC: Symantec AntiVirus: Scans	Displays scans using Symantec AntiVirus.
290	NERC: Symantec AntiVirus: Updated	Displays updates to Symantec AntiVirus.

Serial Number	TIBCO LogLogic Report	Description
291	NERC: Symantec Endpoint Protection: Attacks Detected	Displays attacks detected by Symantec Endpoint Protection.
292	NERC: Symantec Endpoint Protection: Attacks by Threat Name	Displays Symantec Endpoint Protection attacks by threat name.
293	NERC: Symantec Endpoint Protection Configuration Changes	Displays Symantec Endpoint Protection configuration changes.
294	NERC: Symantec Endpoint Protection Password Changes	Displays all password change activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
295	NERC: Symantec Endpoint Protection Policy Add, Remove, or Modify	Displays all events when a Symantec Endpoint Protection policy is added, removed, or modified.
296	NERC: Symantec Endpoint Protection: Scans	Displays scans using Symantec Endpoint Protection.
297	NERC: Symantec Endpoint Protection: Updated	Displays updates to Symantec Endpoint Protection.
298	NERC: TIBCO ActiveMatrix Administrator Failed Logins	Displays all TIBCO ActiveMatrix Administrator login events that have failed.
299	NERC: TIBCO ActiveMatrix Administrator Permission Changes	Displays all TIBCO ActiveMatrix Administrator permission modifications.
300	NERC: TIBCO ActiveMatrix Administrator Successful Logins	Displays successful logins to TIBCO ActiveMatrix Administrator to ensure only authorized personnel have access.
301	NERC: TIBCO Administrator Password Changes	Displays all password change activities on TIBCO Administrator to ensure authorized and appropriate access.
302	NERC: TIBCO Administrator Permission Changes	Displays events related to TIBCO Administrator permission modifications.
303	NERC: TrendMicro Control Manager: Attacks Detected	Displays attacks detected by TrendMicro Control Manager.
304	NERC: TrendMicro Control Manager: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro Control Manager by threat name.

Serial Number	TIBCO LogLogic Report	Description
305	NERC: TrendMicro OfficeScan: Attacks Detected	Displays attacks detected by TrendMicro OfficeScan.
306	NERC: TrendMicro OfficeScan: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro OfficeScan by threat name.
307	NERC: Trusted Domain Created on Windows Servers	Displays all trusted domains created on Windows servers to ensure authorized and appropriate access.
308	NERC: Trusted Domain Deleted on Windows Servers	Displays all trusted domains deleted on Windows servers to ensure authorized and appropriate access.
309	NERC: Unauthorized Logins	Displays all logins from unauthorized users to ensure appropriate access to data.
310	NERC: Unencrypted Logins	Displays all unencrypted logins to ensure secure access to data.
311	NERC: Unix Password Changes	Password changes on UNIX servers.
312	NERC: Users Created on Servers	Displays all users created on servers to ensure authorized and appropriate access.
313	NERC: Users Removed from Servers	Displays all users removed from servers to ensure timely removal of terminated users.
314	NERC: Users Using the Proxies	Displays users who have been surfing the web through the proxy servers.
315	NERC: Users Using the Proxies - Blue Coat Proxy	Displays users who have been surfing the web through the proxy servers on Blue Coat Proxy.
316	NERC: Users Using the Proxies - Cisco WSA	Displays users who have been surfing the web through the proxy servers on Cisco WSA.
317	NERC: Users Using the Proxies - Microsoft IIS	Displays users who have been surfing the web through the proxy servers on Microsoft IIS.
318	NERC: vCenter Change Attributes	Modification of VMware vCenter and VMware ESX properties.
319	NERC: vCenter Data Move	Entity is moved within the VMware vCenter infrastructure.
320	NERC: vCenter Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter.
321	NERC: vCenter Failed Logins	Failed logins to the VMware vCenter console.

Serial Number	TIBCO LogLogic Report	Description
322	NERC: vCenter Modify Firewall Policy	Displays changes to the VMware ESX allowed services firewall policy.
323	NERC: vCenter Orchestrator Change Attributes	Modification of VMware vCenter Orchestrator properties.
324	NERC: vCenter Orchestrator Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter Orchestrator.
325	NERC: vCenter Orchestrator Data Move	Entity is moved within the VMware vCenter Orchestrator infrastructure.
326	NERC: vCenter Orchestrator Failed Logins	Displays all failed logins for VMware vCenter Orchestrator.
327	NERC: vCenter Orchestrator Virtual Machine Created	Virtual machine is created from VMware vCenter Orchestrator.
328	NERC: vCenter Orchestrator Virtual Machine Deleted	Virtual machine is deleted from VMware vCenter Orchestrator.
329	NERC: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine is shut down or paused from VMware vCenter Orchestrator console.
330	NERC: vCenter Orchestrator Virtual Machine Started	Virtual machine is started or resumed from VMware vCenter Orchestrator console.
331	NERC: vCenter Orchestrator vSwitch Added, Changed or Removed	vSwitch is added, modified or removed from VMware vCenter Orchestrator console.
332	NERC: vCenter Resource Usage Change	Resources have changed on VMware vCenter.
333	NERC: vCenter Restart ESX Services	VMware vCenter restarted services running on VMware ESX Server.
334	NERC: vCenter Shutdown or Restart of ESX Server	VMware ESX Server is shutdown or restarted from VMware vCenter console.
335	NERC: vCenter Successful Logins	Successful logins to the VMware vCenter console.
336	NERC: vCenter User Permission Change	A permission role is added, changed, removed, or applied to a user on VMware vCenter server.
337	NERC: vCenter Virtual Machine Created	Virtual machine is created from VMware vCenter console.
338	NERC: vCenter Virtual Machine Deleted	Virtual machine is deleted or removed from VMware vCenter console.

Serial Number	TIBCO LogLogic Report	Description
339	NERC: vCenter Virtual Machine Shutdown	Virtual machine is shutdown or paused from VMware vCenter console.
340	NERC: vCenter Virtual Machine Started	Virtual machine is started or resumed from VMware vCenter console.
341	NERC: vCenter vSwitch Added, Changed or Removed	vSwitch on VMware ESX server is added, modified or removed from the VMware vCenter console.
342	NERC: vCloud Failed Logins	Failed logins to the VMware vCloud Director console.
343	NERC: vCloud Organization Created	VMware vCloud Director organization created events.
344	NERC: vCloud Organization Deleted	VMware vCloud Director organization deleted events.
345	NERC: vCloud Organization Modified	VMware vCloud Director organization modified events.
346	NERC: vCloud Successful Logins	Successful logins to the VMware vCloud Director console.
347	NERC: vCloud User Created	VMware vCloud Director user-created events.
348	NERC: vCloud User Deleted or Removed	VMware vCloud Director users have been deleted or removed from the system.
349	NERC: vCloud vApp Created, Modified, or Deleted	VMware vCloud Director vApp created, deleted, and modified events.
350	NERC: vCloud vDC Created, Modified, or Deleted	VMware vCloud Director virtual datacenter created, modified, or deleted events.
351	NERC: VPN Connections by Users	Displays users who are made the most connections.
352	NERC: VPN Denied Connections by Users	Displays users with the most number of denied connections.
353	NERC: VPN Sessions by Destination IPs	Displays all VPN sessions categorized by destination IP addresses.
354	NERC: VPN Sessions by Source IPs	Displays all VPN sessions categorized by source IP addresses.
355	NERC: VPN Sessions by Users	Displays all VPN sessions categorized by authenticated users.

Serial Number	TIBCO LogLogic Report	Description
356	NERC: VPN Users Accessing Corporate Network	Displays all users logging in to the corporate network via Virtual Private Network to ensure appropriate access.
357	NERC: vShield Edge Configuration Changes	Displays changes to the VMware vShield Edge policies.
358	NERC: vShield Risky Firewall Traffic	Displays all allowed VMware vShield Edge firewall traffic that are considered risky.
359	NERC: Web Access from All Users	Displays all web-based access by all users for regular reviews and updates.
360	NERC: Web Access from All Us ers - Fortinet	Displays all web-based access by all users for regular reviews and updates on Fortinet.
361	NERC: Web Access from All Us ers - F5 BIG-IP TMOS	Displays all web-based access by all users for regular reviews and updates on F5 BIG-IP TMOS.
362	NERC: Web Access from All Us ers - Microsoft IIS	Displays all web-based access by all users for regular reviews and updates on Microsoft IIS.
363	NERC: Web Access from All Us ers - PANOS	Displays all web-based access by all users for regular reviews and updates on Palo Alto Networks.
364	NERC: Web Access to Applicati ons - F5 BIG-IP TMOS	Displays all web-based access to applications to ensure appropriate and authorized access on F5 BIG-IP TMOS.
365	NERC: Web Access to Applications - Fortinet	Displays all web-based access to applications to ensure appropriate and authorized access on Fortinet.
366	NERC: Web Access to Applicati ons - Microsoft IIS	Displays all web-based access to applications to ensure appropriate and authorized access on Microsoft IIS.
367	NERC: Web Access to Applications - PANOS	Displays all web-based access to applications to ensure appropriate and authorized access on Palo Alto Networks.
368	NERC: Web Access to Applications	Displays all web-based access to applications to ensure appropriate and authorized access.
369	NERC: Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.
370	NERC: Windows Accounts Locked	Displays all accounts locked out of Windows servers to detect access violations or unusual activities.

Serial Number	TIBCO LogLogic Report	Description
371	NERC: Windows Events by Users	Displays a summary of access-related Windows events by source and target users.
372	NERC: Windows Group Members Added	Displays all accounts added to groups on the Windows servers to ensure appropriate access.
373	NERC: Windows Group Members Deleted	Displays all accounts removed from groups on the Windows servers to ensure appropriate access.

TIBCO LogLogic Alerts for NERC

The following table lists the alerts included in theLogLogic® Compliance Suite - NERC Edition.

Serial Number	TIBCO LogLogic Alert	Description
1	NERC: Accounts Created	Alerts when a new account is created on servers.
2	NERC: Accounts Deleted	Alerts when an account is deleted on servers.
3	NERC: Accounts Enabled	Alerts when an account is enabled on servers.
4	NERC: Accounts Locked	Alerts when an account is locked on servers.
5	NERC: Accounts Modified	Alerts when an account is modified on servers.
6	NERC: Active Directory Changes	Alerts when changes are made within Active Directory.
7	NERC: Allowed Connections	Allowed firewall connections.
8	NERC: Anomalous IDS Alerts	Alerts when IDS anomalies are above or below the defined thresholds.
9	NERC: Check Point Policy Changed	Alerts when a Check Point firewall's policy is modified.
10	NERC: Cisco ISE, ACS Configuration Changed	Alerts when configuration changes are made to the Cisco ISE or Cisco SecureACS.
11	NERC: Cisco ISE, ACS Passwords Changed	Alerts when a user changes the password via Cisco ISE or Cisco SecureACS.
12	NERC: Cisco PIX, ASA, FWSM Commands Executed	Alerts when Cisco PIX, ASA, or FWSM commands are run.
13	NERC: Cisco PIX, ASA, FWSM Failover Disabled	Alerts when a Cisco PIX, ASA, or FWSM HA configuration is disabled.

Serial Number	TIBCO LogLogic Alert	Description
14	NERC: Cisco PIX, ASA, FWSM Failover Errors	Alerts when an error has occurred during PIX, ASA, or FWSM failover.
15	NERC: Cisco PIX, ASA, FWSM Failover Performed	Alerts when a failover has occurred on the Cisco PIX, ASA, or FWSM devices.
16	NERC: Cisco PIX, ASA, FWSM Fragment Database Limit	The fragment database count has reached on Cisco PIX, ASA, or FWSM devices.
17	NERC: Cisco PIX, ASA, FWSM Logon Failure	Notifies about login failure attempts to the Cisco PIX, ASA, or FWSM devices.
18	NERC: Cisco PIX, ASA, FWSM Logon Success	Notifies about successful login attempts to the Cisco PIX, ASA, or FWSM firewall.
19	NERC: Cisco PIX, ASA, FWSM NAT Failure	Notifies about failures in Network Address Translation (NAT) on the Cisco PIX, ASA, or FWSM.
20	NERC: Cisco PIX, ASA, FWSM Policy Changed	Alerts when a Cisco PIX, ASA, or FWSM firewall policy is modified.
22	NERC: Cisco PIX, ASA, FWSM Protocol Failure	Alerts about possible network protocol failures on the Cisco PIX, ASA, or FWSM devices.
23	NERC: System Restarted	Alerts when system is restarted.
24	NERC: Cisco PIX, ASA, FWSM Routing Failure	Alerts when routing failure occurs in the Cisco PIX, ASA, or FWSM devices.
25	NERC: Cisco PIX, ASA, FWSM Shun Added	Alerts when a shun rule is added to the PIX, ASA, or FWSM configuration.
26	NERC: Cisco PIX, ASA, FWSM Shun Deleted	Alerts when a shun rule is removed from the PIX, ASA, or FWSM configuration.
27	NERC: Cisco PIX, ASA, FWSM VPN Tunnel Creation	A VPN tunnel is created on the Cisco PIX, ASA, or FWSM devices.
28	NERC: Cisco PIX, ASA, FWSM VPN Tunnel Teardown	Alers twhen a VPN tunnel is removed on the Cisco PIX, ASA, or FWSM devices.
29	NERC: Cisco Switch Card Insert	Alerts when a card module is inserted into a switch.
30	NERC: Cisco Switch Device Reload	Alerts when a command to reload a Cisco switch is run.
31	NERC: Cisco Switch Device Restart	Alerts when a router or switch is rebooted.

Serial Number	TIBCO LogLogic Alert	Description
32	NERC: Cisco Switch HA Failure (ver)	Alerts when an HA setup has version incompatibility issues.
33	NERC: Cisco Switch Interface Change	Alerts when network interfaces are going up or down.
34	NERC: Cisco Switch Interface Down	Alerts when Cisco switch interface is going down.
35	NERC: Cisco Switch Interface Up	Alerts when the Cisco switch interface is back up.
36	NERC: Cisco Switch Policy Changed	Alerts when Cisco router or switch configuration is modified.
37	NERC: DB2 Database Configuration Change	Alerts when a configuration is changed on a DB2 database.
38	NERC: DB2 Database User Added or Dropped	Alerts when a user is added or dropped from a DB2 database.
39	NERC: Disallowed Services	Disallowed firewall services.
40	NERC: DNS Server Shutdown	Alerts when DNS server is shut down.
41	NERC: DNS Server Started	Alerts when DNS server is started.
42	NERC: Excessive IDS Attack	IDS anomalies using message volume threshold alerts.
43	NERC: F5 BIG-IP TMOS Risky Traffic	F5 BIG-IP TMOS traffic considered risky.
44	NERC: Group Members Added	Alerts when new members are added to user groups.
45	NERC: Group Members Deleted	Alerts when members are removed from user groups.
46	NERC: Groups Created	Alerts when new user groups are created.
47	NERC: Groups Deleted	Alerts when a user group is deleted.
48	NERC: Groups Modified	Alerts when a user group is modified.
49	NERC: Guardium SQL Guard Config Changes	Alerts when a configuration is changed on Guardium SQL Database.
50	NERC: Guardium SQL Guard Logins	Alerts when a user logs in to the Guardium SQL Database.

Serial Number	TIBCO LogLogic Alert	Description
51	NERC: HP NonStop Audit Configuration Changed	Alerts when configuration changes are made to the HP NonStop Audit.
52	NERC: HP NonStop Audit Permission Changed	Alerts on HP NonStop Audit permission changed events.
53	NERC: IBM AIX Password Changed	Alerts when an account password is changed on IBM AIX servers.
54	NERC: Juniper Firewall HA State Change	Alerts when Juniper Firewall has changed its failover state.
55	NERC: Juniper Firewall Logon Failure	Login failure attempts to the Juniper Firewall.
56	NERC: Juniper Firewall Logon Success	Successful login attempts to the Juniper Firewall.
57	NERC: Juniper Firewall Peer Missing	Alerts when a Juniper Firewall HA peer is missing.
58	NERC: Juniper Firewall Policy Changes	Alerts when Juniper Firewall configuration is changed.
59	NERC: Juniper Firewall Policy Out of Sync	Alerts when the Juniper Firewall's policy is out of sync.
60	NERC: Juniper Firewall System Reset	Alerts when the Juniper Firewall is reset to system default.
61	NERC: Logins Failed	Alerts when login failures are over the defined threshold.
62	NERC: Logins Succeeded	Alerts when successful logins are over the defined threshold.
63	NERC: LogLogic DSM Configuration Changes	Alerts when a configuration is changed on LogLogic DSM database.
64	NERC: LogLogic DSM Logins	Alerts when a user logs into the LogLogic DSM database.
65	NERC: LogLogic File Retrieval Errors	Alerts when problems are detected during log file retrieval.
66	NERC: LogLogic Management Center Passwords Changed	Alerts when users have changed their passwords.
67	NERC: LogLogic Message Routing Errors	Alerts when problems are detected during message forwarding.

Serial Number	TIBCO LogLogic Alert	Description
68	NERC: LogLogic Universal Collector Configuration Changed	Alerts when configuration changes are made to the LogLogic universal collector.
69	NERC: Microsoft Operations Manager - Permissions Changed	Alerts when user or group permissions have been changed.
70	NERC: Microsoft Operations Manager - Windows Passwords Changed	Alerts when users have changed their passwords.
71	NERC: Microsoft Operations Manager - Windows Policies Changed	Alerts when Windows policies changed.
72	NERC: Microsoft Operations Manager - Windows Server Restarted	Alerts when a Windows server is restarted.
73	NERC: Microsoft Sharepoint Content Deleted	Alerts on Microsoft Sharepoint content deleted events.
74	NERC: Microsoft Sharepoint Content Updated	Alerts on Microsoft Sharepoint content updated events.
75	NERC: Microsoft Sharepoint Permission Changed	Alerts on Microsoft Sharepoint permission changed events.
76	NERC: Microsoft Sharepoint Policies Added, Removed, Modified	Alerts on Microsoft Sharepoint policy additions, deletions, and modifications.
77	NERC: Neoteris Files Accessed	Identifies all files accessed through the Juniper SSL VPN.
78	NERC: NetApp Authentication Failure	Alerts when NetApp authentication failure events occur.
79	NERC: NetApp Bad File Handle	Alerts when a bad file handle is detected on a NetApp device.
80	NERC: NetApp Bootblock Update	Alerts when the bootblock is updated on a NetApp Filer.
81	NERC: NetApp Filer Audit Policies Changed	Alerts when NetApp Filer Audit policies changed.
82	NERC: NetApp Filer Disk Failure	Alerts when a disk fails on a NetApp Filer.

Serial Number	TIBCO LogLogic Alert	Description
83	NERC: NetApp Filer Disk Inserted	Alerts when a disk is inserted in the NetApp Filer.
84	NERC: NetApp Filer Disk Missing	Alerts when a disk is missing on the NetApp Filer device.
85	NERC: NetApp Filer Disk Pulled	Alerts when a RAID disk is pulled from the Filer device.
86	NERC: NetApp Filer Disk Scrub Suspended	Alerts when the disk scrubbing process is suspended.
87	NERC: NetApp Filer File System Full	Alerts when the file system is full on the NetApp Filer device.
88	NERC: NetApp Filer NIS Group Update	Alerts when the NIS group is updated on the Filer device.
89	NERC: NetApp Filer Snapshot Error	Alerts when an error is detected during a NetApp Filer snapshot.
90	NERC: NetApp Filer Unauthorized Mounting	Alerts when an unauthorized mount event occurs.
91	NERC: Oracle Database Configuration Change	Alerts when an ALTER or an UPDATE command is executed on an Oracle database.
92	NERC: Oracle Database User Added or Deleted	Alerts when a user is added or deleted from an Oracle database.
93	NERC: Policy Violation	Firewall policy violations.
94	NERC: RACF Files Accessed	Alerts when files are accessed on the RACF servers.
95	NERC: RACF Passwords Changed	Alerts when users have changed their passwords.
96	NERC: RACF Permissions Changed	Alerts when user or group permissions have been changed.
97	NERC: Sidewinder Configuration Changed	Alerts when configuration changes are made to the Sidewinder.
98	NERC: Sybase ASE Database Config Changes	Alerts on Sybase ASE Database configuration change events.
99	NERC: Symantec Endpoint Protection Configuration Changed	Alerts when configuration changes are made to the Symantec Endpoint Protection.

Serial Number	TIBCO LogLogic Alert	Description
100	NERC: Symantec Endpoint Protection Policy Add, Delete, Modify	Alerts on Symantec Endpoint Protection additions, deletions, and modifications.
101	NERC: System Anomalies	Detects and alerts any anomalies based on past log patterns.
102	NERC: TIBCO ActiveMatrix Administrator Permissions Changed	Alerts on TIBCO ActiveMatrix Administrator permission changed events.
103	NERC: UNIX Groups Added	Alerts when a new group is added to the UNIX/ Linux servers.
104	NERC: UNIX Groups Deleted	Alerts when a user group is deleted on UNIX/Linux servers.
105	NERC: UNIX Groups Modified	Alerts when a user group is modified on UNIX/Linux servers.
106	NERC: UNIX Privilege Escalated	Alerts when a user has escalated privileges using commands such as su/sudo.
107	NERC: vCenter Create Virtual Machine	Alerts when virtual machine is created from VMware vCenter console.
108	NERC: vCenter Data Move	Alerts when entity is moved within the VMware vCenter infrastructure.
109	NERC: vCenter Datastore Event	Alert on create, modify, and delete datastore events on VMware vCenter.
110	NERC: vCenter Delete Virtual Machine	Alerts when a virtual machine is deleted or removed from VMware vCenter console.
111	NERC: vCenter Firewall Policy Change	Alerts when changes to the VMware ESX allowed services firewall policy.
112	NERC: vCenter Orchestrator Create Virtual Machine	Alerts when a virtual machine is created from VMware vCenter Orchestrator console.
113	NERC: vCenter Orchestrator Data Move	Entity is moved within the VMware vCenter Orchestrator Infrastructure.
114	NERC: vCenter Orchestrator Datastore Events	Alerts on create, modify, and delete datastore events on VMware vCenter Orchestrator.
115	NERC: vCenter Orchestrator Delete Virtual Machine	Alerts when a virtual machine is deleted or removed from VMware vCenter Orchestrator console.

Serial Number	TIBCO LogLogic Alert	Description
116	NERC: vCenter Orchestrator Login Failed	Failed logins to the VMware vCenter Orchestrator console.
117	NERC: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine is shut down or paused from VMware vCenter Orchestrator console.
118	NERC: vCenter Orchestrator Virtual Machine Started	Virtual machine is started or resumed from VMware vCenter Orchestrator console.
119	NERC: vCenter Orchestrator vSwitch Add, Modify or Delete	vSwitch on VMware ESX server is added, modified or removed from vCenter Orchestrator.
120	NERC: vCenter Permission Change	Alerts when a permission role is added, changed, removed, or applied on VMware vCenter.
121	NERC: vCenter Restart ESX Services	Alerts when VMware vCenter restarted services running on VMware ESX Server.
122	NERC: vCenter Shutdown or Restart ESX	Alerts when VMware ESX Server is shut down from vCenter console.
123	NERC: vCenter User Login Failed	Alerts about failed logins to the VMware vCenter console
124	NERC: vCenter User Login Successful	Alerts on successful logins to the VMware vCenter console.
125	NERC: vCenter Virtual Machine Shutdown	Alerts when a virtual machine is shut down or paused from VMware vCenter console.
126	NERC: vCenter Virtual Machine Started	Alerts when a virtual machine is started or resumed from VMware vCenter console.
127	NERC: vCenter vSwitch Add, Modify or Delete	Alerts when a vSwitch on VMware ESX server is added, modified or removed from vCenter.
128	NERC: vCloud Director Login Failed	Alert on failed logins to the VMware vCloud Director console.
129	NERC: vCloud Director Login Success	Alert on successful logins to the VMware vCloud Director console.
130	NERC: vCloud Organization Created	Alerts when organization successfully created on VMware vCloud Director.
131	NERC: vCloud Organization Deleted	Alerts when organization successfully deleted on VMware vCloud Director.
132	NERC: vCloud Organization Modified	Alerts when organization successfully modified on VMware vCloud Director.

Serial Number	TIBCO LogLogic Alert	Description
133	NERC: vCloud User Created	Alerts when a user successfully created on VMware vCloud Director.
134	NERC: vCloud User, Group, or Role Modified	Alerts when VMware vCloud Director user, group, or role is modified.
135	NERC: vCloud vApp Created, Deleted, or Modified	Alerts when VMware vCloud Director vApp is created, deleted, or modified.
136	NERC: vCloud vDC Created, Modified, or Deleted	Alerts when VMware vCloud Director Virtual Datacenters have been created, deleted, or modified.
137	NERC: vShield Edge Configuration Change	Alerts when configuration changes to VMware vShield Edge policies.
138	NERC: vShield Risky Traffic	Alerts when VMware vShield Edge traffic considered risky.
139	NERC: Windows Audit Log Cleared	Alerts when audit logs on Windows servers have been cleared.
140	NERC: Windows Files Accessed	Show files accessed on the Windows servers.
141	NERC: Windows Group Members Added	Alerts when new members are added to user groups on Windows servers.
142	NERC: Windows Group Members Deleted	Alerts when members are removed from user groups on Windows servers.
143	NERC: Windows Groups Created	Alerts when new user groups are created on Windows servers.
144	NERC: Windows Groups Deleted	Alerts when a user group is deleted on Windows servers.
145	NERC: Windows Groups Modified	Alerts when a user group is modified on Windows servers.
146	NERC: Windows Passwords Changed	Alerts when users have changed their passwords.
147	NERC: Windows Permissions Changed	Alerts when user or group permissions have been changed.
148	NERC: Windows Policies Changed	Alerts when Windows policies changed.
149	NERC: Windows Privileges Escalated	Alerts when a user or program has escalated the privileges.

Serial Number	TIBCO LogLogic Alert	Description
150	NERC: System Restarted	Alerts when system is restarted.

TIBCO LogLogic Reports and Alerts Quick Reference

The following table lists the reports and alerts included in the LogLogic® Compliance Suite - NERC Edition.

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1		
CIP-003-1 R3.2	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	**Compliance Suite Reports** NERC: Escalated Privilege Activities on Servers **Compliance Suite Alerts** NERC: UNIX Privilege Escalated
CIP-003-1 R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	**Compliance Suite Reports** NERC: Account Activities on UNIX Servers NERC: Account Activities on Windows Servers NERC: Accounts Changed on NetApp Filer NERC: Accounts Changed on TIBCO Administrator NERC: Accounts Changed on TIBCO ActiveMatrix Administrator NERC: Accounts Changed on UNIX Servers NERC: Accounts Changed on Windows Servers NERC: Accounts Created on NetApp Filer NERC: Accounts Created on NetApp Filer Audit NERC: Accounts Created on Sidewinder NERC: Accounts Created on Symantec Endpoint Protection NERC: Accounts Created on TIBCO Administrator NERC: Accounts Created on TIBCO ActiveMatrix Administrator

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	**Compliance Suite Reports** (Cont.) NERC: Accounts Created on UNIX Servers NERC: Accounts Created on Windows Servers NERC: Accounts Deleted on NetApp Filer NERC: Accounts Deleted on NetApp Filer Audit NERC: Accounts Deleted on Symantec Endpoint Protection NERC: Accounts Deleted on TIBCO Administrator NERC: Accounts Deleted on TIBCO ActiveMatrix Administrator NERC: Accounts Deleted on Sidewinder NERC: Accounts Deleted on UNIX Servers NERC: Accounts Deleted on Windows Servers NERC: Cisco ISE, ACS Accounts Created NERC: Cisco ISE, ACS Accounts Removed NERC: DB2 Database Successful Logins NERC: ESX Accounts Activities NERC: ESX Accounts Created NERC: ESX Accounts Deleted NERC: ESX Logins Succeeded NERC: F5 BIG-IP TMOS Login Successful NERC: Guardium SQL Guard Audit Logins NERC: Guardium SQL Guard Logins NERC: HP NonStop Audit Login Successful NERC: LogLogic DSM Logins NERC: LogLogic Management Center Account Activities NERC: LogLogic Management Center Login NERC: Microsoft Operations Manager - Windows Accounts Activities NERC: Microsoft Operations Manager - Windows Accounts Changed NERC: Microsoft Operations Manager - Windows Accounts Created NERC: Microsoft Operations Manager - Windows Accounts Enabled NERC: Microsoft SQL Server Database Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	**Compliance Suite Reports** (Cont.) NERC: NetApp Filer Audit Accounts Enabled NERC: NetApp Filer Audit Group Members Added NERC: NetApp Filer Audit Group Members Deleted NERC: NetApp Filer Audit Login Successful NERC: NetApp Filer Login Successful NERC: Oracle Database Successful Logins NERC: RACF Accounts Created NERC: RACF Accounts Deleted NERC: RACF Accounts Modified NERC: RACF Successful Logins NERC: Successful Logins NERC: Sybase ASE Successful Logins NERC: TIBCO ActiveMatrix Administrator Successful Logins NERC: vCenter Successful Logins NERC: vCloud Successful Logins NERC: vCloud User Created NERC: vCloud User Deleted or Removed NERC: Windows Accounts Enabled NERC: Windows Accounts Locked NERC: Windows Group Members Added NERC: Windows Group Members Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	**Compliance Suite Alerts** NERC: Accounts Created NERC: Accounts Deleted NERC: Accounts Enabled NERC: Accounts Locked NERC: Accounts Modified NERC: Group Members Added NERC: Group Members Deleted NERC: Guardium SQL Guard Logins NERC: Logins Succeeded NERC: LogLogic DSM Logins NERC: vCenter User Login Successful NERC: vCloud Director Login Success NERC: vCloud User Created NERC: Windows Group Members Added NERC: Windows Group Members Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	**Compliance Suite Reports** NERC: Check Point Configuration Changes NERC: Cisco ISE, ACS Configuration Changes NERC: Cisco PIX, ASA, FWSM Failover Disabled NERC: Cisco PIX, ASA, FWSM Failover Performed NERC: Cisco PIX, ASA, FWSM Policy Changed NERC: Cisco PIX, ASA, FWSM Restarted NERC: Cisco Switch Policy Changes NERC: DB2 Database Failed Logins NERC: DB2 Database Configuration Changes NERC: ESX Failed Logins NERC: ESX Logins Failed Unknown User NERC: F5 BIG-IP TMOS Login Failed NERC: Failed Logins NERC: Guardium SQL Guard Audit Configuration Changes NERC: Guardium SQL Guard Configuration Changes NERC: HP NonStop Audit Configuration Changes NERC: HP NonStop Audit Login Failed NERC: HP NonStop Audit Object Changes NERC: i5/OS Audit Configuration Changes NERC: i5/OS System Management Changes NERC: i5/OS User Profile Creation, Modification, or Restoration NERC: Juniper Firewall HA State Changed NERC: Juniper Firewall Policy Changed NERC: Juniper Firewall Policy Out of Sync NERC: LogLogic DSM Configuration Changes NERC: LogLogic Universal Collector Configuration Changes NERC: Microsoft Sharepoint Policy Add, Remove, or Modify NERC: Microsoft SQL Server Configuration Changes NERC: Microsoft SQL Server Database Failed Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	**Compliance Suite Reports** (Cont.) NERC: NetApp Filer Audit Login Failed NERC: NetApp Filer Login Failed NERC: Oracle Database Configuration Changes NERC: Oracle Database Failed Logins NERC: RACF Failed Logins NERC: Sidewinder Configuration Changes NERC: Sybase ASE Database Configuration Changes NERC: Sybase ASE Failed Logins NERC: Symantec Endpoint Protection Configuration Changes NERC: TIBCO ActiveMatrix Administrator Failed Logins NERC: vCenter Change Attributes NERC: vCenter Failed Logins NERC: vCenter Modify Firewall Policy NERC: vCenter Orchestrator Change Attributes NERC: vCenter Orchestrator Failed Logins NERC: vCenter Orchestrator vSwitch Added, Changed or Removed NERC: vCenter Resource Usage Change NERC: vCenter vSwitch Added, Changed or Removed NERC: vCloud Failed Logins NERC: vShield Edge Configuration Changes **Compliance Suite Alerts** NERC: Check Point Policy Changed NERC: Cisco ISE, ACS Configuration Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	**Compliance Suite Alerts** (Cont.) NERC: System Restarted NERC: Cisco PIX, ASA, FWSM Failover Disabled NERC: Cisco PIX, ASA, FWSM Failover Performed NERC: Cisco PIX, ASA, FWSM Logon Failure NERC: Cisco PIX, ASA, FWSM Logon Success NERC: Cisco PIX, ASA, FWSM Policy Changed NERC: Cisco PIX, ASA, FWSM Shun Added NERC: Cisco PIX, ASA, FWSM Shun Deleted NERC: Cisco Switch Card Insert NERC: Cisco Switch Device Reload NERC: Cisco Switch Device Restart NERC: Cisco Switch HA Failure (ver) NERC: Cisco Switch Interface Change NERC: Cisco Switch Interface Down NERC: Cisco Switch Interface Up NERC: Cisco Switch Policy Changed NERC: DB2 Database Configuration Change NERC: Disallowed Services NERC: DNS Server Shutdown NERC: DNS Server Started NERC: Excessive IDS Attack NERC: Guardium SQL Guard Config Changes NERC: HP NonStop Audit Configuration Changed NERC: Juniper Firewall HA State Change NERC: Juniper Firewall Logon Failure NERC: Juniper Firewall Logon Success NERC: Juniper Firewall Policy Changes NERC: Juniper Firewall Policy Out of Sync NERC: Juniper Firewall Peer Missing NERC: Juniper Firewall System Reset NERC: Logins Failed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	**Compliance Suite Alerts** (Cont.) NERC: LogLogic DSM Configuration Changes NERC: LogLogic Universal Collector Configuration Changed NERC: Microsoft Sharepoint Policies Added, Removed, Modified NERC: NetApp Authentication Failure NERC: NetApp Bad File Handle NERC: NetApp Bootblock Update NERC: NetApp Filer Disk Failure NERC: NetApp Filer File System Full NERC: NetApp Filer Disk Inserted NERC: NetApp Filer Disk Pulled NERC: NetApp Filer Snapshot Error NERC: NetApp Filer Unauthorized Mounting NERC: Oracle Database Configuration Change NERC: Policy Violation NERC: Sidewinder Configuration Changed NERC: Sybase ASE Database Config Changes NERC: Symantec Endpoint Protection Configuration Changed NERC: Symantec Endpoint Protection Policy Add, Delete, Modify NERC: System Anomalies NERC: UNIX Groups Added NERC: UNIX Groups Deleted NERC: UNIX Groups Modified NERC: vCenter Firewall Policy Change NERC: vCenter Orchestrator Login Failed NERC: vCenter Orchestrator vSwitch Add, Modify or Delete NERC: vCenter User Login Failed NERC: vCenter vSwitch Add, Modify or Delete NERC: vCloud Director Login Failed NERC: vCloud User, Group, or Role Modified NERC: vShield Edge Configuration Change

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity-or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	**Compliance Suite Reports** NERC: Check Point Configuration Changes NERC: Cisco ISE, ACS Configuration Changes NERC: Cisco PIX, ASA, FWSM Failover Disabled NERC: Cisco PIX, ASA, FWSM Failover Performed NERC: Cisco PIX, ASA, FWSM Policy Changed NERC: Cisco PIX, ASA, FWSM Restarted NERC: Cisco Switch Policy Changes NERC: DB2 Database Failed Logins NERC: DB2 Database Configuration Changes NERC: ESX Failed Logins NERC: ESX Logins Failed Unknown User NERC: F5 BIG-IP TMOS Login Failed NERC: Failed Logins NERC: Guardium SQL Guard Audit Configuration Changes NERC: Guardium SQL Guard Configuration Changes NERC: HP NonStop Audit Configuration Changes NERC: HP NonStop Audit Login Failed NERC: HP NonStop Audit Object Changes NERC: i5/OS Audit Configuration Changes NERC: i5/OS System Management Changes NERC: i5/OS User Profile Creation, Modification, or Restoration NERC: Juniper Firewall HA State Changed NERC: Juniper Firewall Policy Changed NERC: Juniper Firewall Policy Out of Sync NERC: LogLogic DSM Configuration Changes NERC: LogLogic Universal Collector Configuration Changes NERC: Microsoft Sharepoint Policy Add, Remove, or Modify NERC: Microsoft SQL Server Configuration Changes NERC: Microsoft SQL Server Database Failed Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity-or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	**Compliance Suite Reports** (Cont.) NERC: NetApp Filer Audit Login Failed NERC: NetApp Filer Login Failed NERC: Oracle Database Configuration Changes NERC: Oracle Database Failed Logins NERC: RACF Failed Logins NERC: Sidewinder Configuration Changes NERC: Sybase ASE Database Configuration Changes NERC: Sybase ASE Failed Logins NERC: Symantec Endpoint Protection Configuration Changes NERC: TIBCO ActiveMatrix Administrator Failed Logins NERC: vCenter Change Attributes NERC: vCenter Failed Logins NERC: vCenter Modify Firewall Policy NERC: vCenter Orchestrator Change Attributes NERC: vCenter Orchestrator Failed Logins NERC: vCenter Orchestrator Virtual Machine Created NERC: vCenter Orchestrator Virtual Machine Deleted NERC: vCenter Orchestrator vSwitch Added, Changed or Removed NERC: vCenter Resource Usage Change NERC: vCenter Virtual Machine Created NERC: vCenter Virtual Machine Deleted NERC: vCenter vSwitch Added, Changed or Removed NERC: vCloud Failed Logins NERC: vCloud Organization Created NERC: vCloud Organization Deleted NERC: vCloud Organization Modified NERC: vCloud vApp Created, Modified, or Deleted NERC: vCloud vDC Created, Modified, or Deleted NERC: vShield Edge Configuration Changes **Compliance Suite Alerts**

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: Check Point Policy Changed NERC: Cisco ISE, ACS Configuration Changed
CIP-003-1 R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	**Compliance Suite Alerts** (Cont.) NERC: System Restarted NERC: Cisco PIX, ASA, FWSM Failover Disabled NERC: Cisco PIX, ASA, FWSM Failover Performed NERC: Cisco PIX, ASA, FWSM Logon Failure NERC: Cisco PIX, ASA, FWSM Logon Success NERC: Cisco PIX, ASA, FWSM Policy Changed NERC: Cisco PIX, ASA, FWSM Shun Added NERC: Cisco PIX, ASA, FWSM Shun Deleted NERC: Cisco Switch Card Insert NERC: Cisco Switch Device Reload NERC: Cisco Switch Device Restart NERC: Cisco Switch HA Failure (ver) NERC: Cisco Switch Interface Change NERC: Cisco Switch Interface Down NERC: Cisco Switch Interface Up NERC: Cisco Switch Policy Changed NERC: DB2 Database Configuration Change NERC: Disallowed Services NERC: DNS Server Shutdown NERC: DNS Server Started NERC: Excessive IDS Attack NERC: Guardium SQL Guard Config Changes NERC: HP NonStop Audit Configuration Changed NERC: Juniper Firewall HA State Change NERC: Juniper Firewall Logon Failure NERC: Juniper Firewall Logon Success NERC: Juniper Firewall Policy Changes NERC: Juniper Firewall Policy Out of Sync NERC: Juniper Firewall Peer Missing NERC: Juniper Firewall System Reset NERC: Logins Failed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	**Compliance Suite Alerts** (Cont.) NERC: LogLogic DSM Configuration Changes NERC: LogLogic Universal Collector Configuration Changed NERC: Microsoft Sharepoint Policies Added, Removed, Modified NERC: NetApp Authentication Failure NERC: NetApp Bad File Handle NERC: NetApp Bootblock Update NERC: NetApp Filer Disk Failure NERC: NetApp Filer File System Full NERC: NetApp Filer Disk Inserted NERC: NetApp Filer Disk Pulled NERC: NetApp Filer Snapshot Error NERC: NetApp Filer Unauthorized Mounting NERC: Oracle Database Configuration Change NERC: Policy Violation NERC: Sidewinder Configuration Changed NERC: Sybase ASE Database Config Changes NERC: Symantec Endpoint Protection Configuration Changed NERC: Symantec Endpoint Protection Policy Add, Delete, Modify NERC: System Anomalies NERC: UNIX Groups Added NERC: UNIX Groups Deleted NERC: UNIX Groups Modified NERC: vCenter Create Virtual Machine NERC: vCenter Delete Virtual Machine NERC: vCenter Firewall Policy Change NERC: vCenter Orchestrator Create Virtual Machine NERC: vCenter Orchestrator Delete Virtual Machine NERC: vCenter Orchestrator Login Failed NERC: vCenter Orchestrator vSwitch Add, Modify or Delete

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-003-1 R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	**Compliance Suite Alerts** (Cont.) NERC: vCenter User Login Failed NERC: vCenter vSwitch Add, Modify or Delete NERC: vCloud Director Login Failed NERC: vCloud Organization Created NERC: vCloud Organization Deleted NERC: vCloud Organization Modified NERC: vCloud User, Group, or Role Modified NERC: vCloud vApp Created, Deleted, or Modified NERC: vCloud vDC Created, Modified, or Deleted NERC: vShield Edge Configuration Change
CIP-005-1		

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	**Compliance Suite Reports** NERC: Active Connections for Cisco ASA NERC: Active Connections for Cisco FWSM NERC: Active Connections for Cisco PIX NERC: Active VPN Connections for Cisco VPN Concentrators NERC: Active VPN Connections for Nortel Contivity NERC: Active VPN Connections for RADIUS NERC: Denied Connections by IP Addresses NERC: Denied Connections - Cisco Router NERC: Denied Connections - Cisco IOS NERC: Denied Connections - Cisco NXOS NERC: Denied Connections - F5 BIG-IP TMOS NERC: Denied Connections - Sidewinder NERC: Denied Connections - VMware vShield NERC: Denied Inbound Connections - Check Point NERC: Denied Inbound Connections - Cisco ASA NERC: Denied Inbound Connections - Cisco FWSM NERC: Denied Inbound Connections - Cisco PIX NERC: Denied Inbound Connections - Juniper Firewall NERC: Denied Outbound Connections - Check Point NERC: Denied Outbound Connections - Cisco ASA NERC: Denied Outbound Connections - Cisco FWSM NERC: Denied Outbound Connections - Cisco PIX NERC: Denied Outbound Connections - Juniper Firewall NERC: Files Downloaded via Proxy NERC: Files Downloaded via Proxy - Blue Coat Proxy NERC: Files Downloaded via Proxy - Cisco WSA NERC: Files Downloaded via Proxy - Microsoft IIS NERC: Files Downloaded via the Web NERC: Files Downloaded via the Web - F5 BIG-IP TMOS

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: Files Downloaded via the Web - Microsoft IIS NERC: Files Uploaded via Proxy - Microsoft IIS
CIP-005-1 R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	**Compliance Suite Reports** -(Cont.) NERC: Files Uploaded via the Web - Microsoft IIS NERC: Files Uploaded via Proxy NERC: Files Uploaded via Proxy - Blue Coat Proxy NERC: Files Uploaded via Proxy - Cisco WSA NERC: Files Uploaded via the Web NERC: Files Uploaded via the Web - F5 BIG-IP TMOS NERC: Most Active Ports Through Firewall - Check Point NERC: Most Active Ports Through Firewall - Cisco ASA NERC: Most Active Ports Through Firewall - Cisco FWSM NERC: Most Active Ports Through Firewall - Cisco PIX NERC: Most Active Ports Through Firewall - Fortinet NERC: Most Active Ports Through Firewall - Juniper Firewall NERC: Most Active Ports Through Firewall - Nortel NERC: NetApp Filer Accounts Locked NERC: Ports Allowed Access - Cisco IOS NERC: Ports Allowed Access - Cisco Netflow NERC: Ports Allowed Access - Cisco PIX NERC: Ports Allowed Access - Check Point NERC: Ports Allowed Access - Cisco ASA NERC: Ports Allowed Access - Cisco FWSM NERC: Ports Allowed Access - F5 BIG-IP TMOS NERC: Ports Allowed Access - Fortinet NERC: Ports Allowed Access - Juniper Firewall NERC: Ports Allowed Access - Juniper JunOS NERC: Ports Allowed Access - Juniper RT Flow NERC: Ports Allowed Access - PANOS

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R1.6	The Responsible Entity shall maintain documentation related to the following entities: • Electronic Security Perimeters • Interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeters • Electronic access points to the Electronic Security Perimeters • Cyber Assets deployed for the access control and monitoring of these access points	**Compliance Suite Reports** (Cont.) NERC: Ports Allowed Access - Sidewinder NERC: Ports Allowed Access - Nortel NERC: Ports Allowed Access - VMware vShield NERC: VPN Denied Connections by Users NERC: vShield Risky Firewall Traffic **Compliance Suite Alerts** NERC: F5 BIG-IP TMOS Risky Traffic NERC: vShield Risky Traffic
CIP-005-1 R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	**Compliance Suite Reports** NERC: Allowed URLs by Source IPs NERC: Allowed URLs by Source IPs - F5 BIG-IP TMOS NERC: Allowed URLs by Source IPs - Microsoft IIS NERC: Allowed URLs by Source Users NERC: Allowed URLs by Source Users - F5 BIG-IP TMOS NERC: Allowed URLs by Source Users - Microsoft IIS NERC: Blocked URLs by Source IPs NERC: Blocked URLs by Source IPs - F5 BIG-IP TMOS NERC: Blocked URLs by Source IPs - Microsoft IIS NERC: Blocked URLs by Source Users NERC: Blocked URLs by Source Users - F5 BIG-IP TMOS NERC: Blocked URLs by Source Users - Microsoft IIS **Compliance Suite Alerts** None

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R2.3	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	**Compliance Suite Reports** NERC: Logins by Authentication Type **Compliance Suite Alerts** None

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	**Compliance Suite Reports** NERC: DB2 Database User Additions and Deletions NERC: DB2 Database Successful Logins NERC: Denied Connections by IP Addresses NERC: Denied Connections - Cisco IOS NERC: Denied Connections - Cisco NXOS NERC: Denied Connections - Cisco Router NERC: Denied Connections - F5 BIG-IP TMOS NERC: Denied Connections - Sidewinder NERC: Denied Connections - VMware vShield NERC: Denied Inbound Connections - Check Point NERC: Denied Inbound Connections - Cisco ASA NERC: Denied Inbound Connections - Cisco FWSM NERC: Denied Inbound Connections - Cisco PIX NERC: Denied Inbound Connections - Juniper Firewall NERC: Denied Outbound Connections - Check Point NERC: Denied Outbound Connections - Cisco ASA NERC: Denied Outbound Connections - Cisco FWSM NERC: Denied Outbound Connections - Cisco PIX NERC: Denied Outbound Connections - Juniper Firewall NERC: ESX Logins Succeeded NERC: F5 BIG-IP TMOS Login Successful NERC: Files Accessed on Servers NERC: Files Accessed on NetApp Filer Audit NERC: Files Accessed through Juniper SSL VPN (Secure Access) NERC: Files Accessed through PANOS NERC: Files Accessed Through Pulse Connect Secure NERC: Guardium SQL Guard Audit Logins NERC: Guardium SQL Guard Logins NERC: HP NonStop Audit Login Successful NERC: HP NonStop Audit Object Access

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: i5/OS Object Access NERC: LogLogic DSM Logins NERC: LogLogic Management Center Login NERC: Microsoft Sharepoint Content Deleted NERC: Microsoft Sharepoint Content Updates

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	**Compliance Suite Reports** (Cont.) NERC: Microsoft SQL Server Database Permission Events NERC: Microsoft SQL Server Database Successful Logins NERC: Microsoft SQL Server Database User Additions and Deletions NERC: NetApp Filer Audit Login Successful NERC: NetApp Filer Audit Group Members Deleted NERC: NetApp Filer File Activity NERC: NetApp Filer Login Successful NERC: Oracle Database Successful Logins NERC: Oracle Database Permission Events NERC: Oracle Database User Additions and Deletions NERC: Ports Denied Access - Check Point NERC: Ports Denied Access - Cisco ASA NERC: Ports Denied Access - Cisco FWSM NERC: Ports Denied Access - Cisco IOS NERC: Ports Denied Access - Cisco PIX NERC: Ports Denied Access - Cisco Router NERC: Ports Denied Access - F5 BIG-IP TMOS NERC: Ports Denied Access - Fortinet NERC: Ports Denied Access - Juniper Firewall NERC: Ports Denied Access - Juniper JunOS NERC: Ports Denied Access - Juniper RT Flow NERC: Ports Denied Access - Nortel NERC: Ports Denied Access - PANOS NERC: Ports Denied Access - Sidewinder NERC: Ports Denied Access - VMware vShield NERC: RACF Files Accessed NERC: RACF Successful Logins NERC: Root Logins NERC: Successful Logins NERC: Sybase ASE Database User Additions and Deletions

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: Sybase ASE Successful Logins
CIP-005-1 R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	**Compliance Suite Reports** (Cont.) NERC: TIBCO ActiveMatrix Administrator Successful Logins NERC: Unauthorized Logins NERC: vCenter Data Move NERC: vCenter Datastore Events NERC: vCenter Orchestrator Datastore Events NERC: vCenter Orchestrator Data Move NERC: vCenter Successful Logins NERC: vCloud Successful Logins NERC: VPN Denied Connections by Users NERC: VPN Users Accessing Corporate Network NERC: Windows Group Members Deleted **Compliance Suite Alerts** NERC: DB2 Database User Added or Dropped NERC: Group Members Deleted NERC: Guardium SQL Guard Logins NERC: Logins Succeeded NERC: LogLogic DSM Logins NERC: Microsoft Sharepoint Content Deleted NERC: Microsoft Sharepoint Content Updated NERC: Neoteris Files Accessed NERC: Oracle Database User Added or Deleted NERC: RACF Files Accessed NERC: vCenter Data Move NERC: vCenter Datastore Event NERC: vCenter Orchestrator Data Move NERC: vCenter Orchestrator Datastore Events NERC: vCenter User Login Successful NERC: vCloud Director Login Success NERC: Windows Files Accessed NERC: Windows Group Members Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week	**Compliance Suite Reports** NERC: Active Directory System Changes NERC: Cisco ISE, ACS Password Changes NERC: DB2 Database Failed Logins NERC: DB2 Database Successful Logins NERC: DNS Server Error NERC: ESX Failed Logins NERC: ESX Logins Failed Unknown User NERC: ESX Logins Succeeded NERC: F5 BIG-IP TMOS Login Failed NERC: F5 BIG-IP TMOS Login Successful NERC: F5 BIG-IP TMOS Password Changes NERC: Failed Logins NERC: Guardium SQL Guard Audit Logins NERC: Guardium SQL Guard Logins NERC: HP NonStop Audit Login Failed NERC: HP NonStop Audit Login Successful NERC: HP NonStop Audit Permissions Changed NERC: LogLogic DSM Logins NERC: LogLogic Management Center Login NERC: LogLogic Management Center Password Changes NERC: Microsoft Operations Manager - Windows Permissions Modified NERC: Microsoft Sharepoint Content Deleted NERC: Microsoft Sharepoint Content Updates NERC: Microsoft Sharepoint Permissions Changed NERC: Microsoft Sharepoint Policy Add, Remove, or Modify NERC: Microsoft SQL Server Database Failed Logins NERC: Microsoft SQL Server Database Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week	**Compliance Suite Reports** (Cont.) NERC: NetApp Filer Audit Login Failed NERC: NetApp Filer Audit Login Successful NERC: NetApp Filer Login Failed NERC: NetApp Filer Login Successful NERC: NetApp Filer Password Changes NERC: Oracle Database Failed Logins NERC: Oracle Database Successful Logins NERC: Periodic Review of Log Reports NERC: Periodic Review of User Access Logs NERC: Permissions Modified on Windows Servers NERC: RACF Failed Logins NERC: RACF Permissions Changed NERC: RACF Successful Logins NERC: Sensors Generating Alerts NERC: Sensors Generating Alerts - Cisco IOS NERC: Sensors Generating Alerts - ISS SiteProtector NERC: Sensors Generating Alerts - SiteProtector NERC: Sensors Generating Alerts - Sourcefire Defense Center NERC: Successful Logins NERC: Sybase ASE Failed Logins NERC: Sybase ASE Successful Logins NERC: Symantec Endpoint Protection Password Changes NERC: TIBCO ActiveMatrix Administrator Failed Logins NERC: TIBCO ActiveMatrix Administrator Permission Changes NERC: TIBCO ActiveMatrix Administrator Successful Logins NERC: TIBCO Administrator Password Changes NERC: TIBCO Administrator Permission Changes NERC: Unauthorized Logins NERC: vCenter Change Attributes NERC: vCenter Data Move NERC: vCenter Datastore Events

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week	**Compliance Suite Reports** (Cont.) NERC: vCenter Failed Logins NERC: vCenter Modify Firewall Policy NERC: vCenter Orchestrator Change Attributes NERC: vCenter Orchestrator Datastore Events NERC: vCenter Orchestrator Data Move NERC: vCenter Orchestrator Failed Logins NERC: vCenter Orchestrator Virtual Machine Created NERC: vCenter Orchestrator Virtual Machine Deleted NERC: vCenter Orchestrator Virtual Machine Shutdown NERC: vCenter Orchestrator Virtual Machine Started NERC: vCenter Orchestrator vSwitch Added, Changed or Removed NERC: vCenter Resource Usage Change NERC: vCenter Shutdown or Restart of ESX Server NERC: vCenter Successful Logins NERC: vCenter User Permission Change NERC: vCenter Virtual Machine Created NERC: vCenter Virtual Machine Deleted NERC: vCenter Virtual Machine Shutdown NERC: vCenter Virtual Machine Started NERC: vCenter vSwitch Added, Changed or Removed NERC: vCloud Failed Logins NERC: vCloud Organization Created NERC: vCloud Organization Deleted NERC: vCloud Organization Modified NERC: vCloud Successful Logins NERC: vCloud vApp Created, Modified, or Deleted NERC: vCloud vDC Created, Modified, or Deleted NERC: VPN Sessions by Destination IPs NERC: VPN Sessions by Source IPs NERC: VPN Sessions by Users

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: vShield Edge Configuration Changes **Compliance Suite Alerts** NERC: Accounts Enabled NERC: Accounts Locked

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week	**Compliance Suite Alerts** (Cont.) NERC: Active Directory Changes NERC: Allowed Connections NERC: Cisco ISE, ACS Passwords Changed NERC: Cisco PIX, ASA, FWSM Commands Executed NERC: System Restarted NERC: Cisco PIX, ASA, FWSM Failover Errors NERC: Cisco PIX, ASA, FWSM Failover Performed NERC: Cisco PIX, ASA, FWSM Fragment Database Limit NERC: Cisco PIX, ASA, FWSM Logon Failure NERC: Cisco PIX, ASA, FWSM Logon Success NERC: Cisco PIX, ASA, FWSM NAT Failure NERC: Cisco PIX, ASA, FWSM Policy Changed NERC: Cisco PIX, ASA, FWSM Protocol Failure NERC: Cisco PIX, ASA, FWSM Routing Failure NERC: Cisco PIX, ASA, FWSM Shun Added NERC: Cisco PIX, ASA, FWSM Shun Deleted NERC: Cisco PIX, ASA, FWSM VPN Tunnel Creation NERC: Cisco PIX, ASA, FWSM VPN Tunnel Teardown NERC: Cisco Switch Card Insert NERC: Cisco Switch Device Reload NERC: Cisco Switch Device Restart NERC: Cisco Switch HA Failure (ver) NERC: Cisco Switch Interface Change NERC: Cisco Switch Interface Down NERC: Cisco Switch Interface Up NERC: Cisco Switch Policy Changed NERC: Disallowed Services NERC: DNS Server Shutdown NERC: DNS Server Started NERC: Excessive IDS Attack NERC: Groups Created

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week	**Compliance Suite Alerts** (Cont.) NERC: Groups Deleted NERC: Groups Modified NERC: Group Members Added NERC: Group Members Deleted NERC: Guardium SQL Guard Logins NERC: HP NonStop Audit Permission Changed NERC: IBM AIX Password Changed NERC: Juniper Firewall HA State Change NERC: Juniper Firewall Logon Failure NERC: Juniper Firewall Logon Success NERC: Juniper Firewall Peer Missing NERC: Juniper Firewall Policy Changes NERC: Juniper Firewall Policy Out of Sync NERC: Juniper Firewall System Reset NERC: Logins Failed NERC: Logins Succeeded NERC: LogLogic DSM Logins NERC: LogLogic File Retrieval Errors NERC: LogLogic Management Center Passwords Changed NERC: LogLogic Message Routing Errors NERC: Microsoft Operations Manager - Permissions Changed NERC: Microsoft Operations Manager - Windows Passwords Changed NERC: Microsoft Operations Manager - Windows Policies Changed NERC: Microsoft Operations Manager - Windows Server Restarted NERC: Microsoft Sharepoint Content Deleted NERC: Microsoft Sharepoint Content Updated NERC: Microsoft Sharepoint Permission Changed NERC: Microsoft Sharepoint Policies Added, Removed, Modified

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	**Compliance Suite Alerts** (Cont.) NERC: Neoteris Files Accessed NERC: NetApp Authentication Failure NERC: NetApp Bad File Handle NERC: NetApp Bootblock Update NERC: NetApp Filer Audit Policies Changed NERC: NetApp Filer Disk Failure NERC: NetApp Filer Disk Missing NERC: NetApp Filer Disk Scrub Suspended NERC: NetApp Filer File System Full NERC: NetApp Filer NIS Group Update NERC: NetApp Filer Disk Inserted NERC: NetApp Filer Disk Pulled NERC: NetApp Filer Snapshot Error NERC: NetApp Filer Unauthorized Mounting NERC: Policy Violation NERC: RACF Files Accessed NERC: RACF Passwords Changed NERC: RACF Permissions Changed NERC: Symantec Endpoint Protection Policy Add, Delete, Modify NERC: System Anomalies NERC: TIBCO ActiveMatrix Administrator Permission Changed NERC: UNIX Groups Added NERC: UNIX Groups Deleted NERC: UNIX Groups Modified NERC: UNIX Privilege Escalated NERC: vCenter Create Virtual Machine NERC: vCenter Data Move NERC: vCenter Datastore Event NERC: vCenter Delete Virtual Machine NERC: vCenter Firewall Policy Change NERC: vCenter Orchestrator Data Move NERC: vCenter Orchestrator Datastore Events

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	**Compliance Suite Alerts** (Cont.) NERC: vCenter Orchestrator Create Virtual Machine NERC: vCenter Orchestrator Delete Virtual Machine NERC: vCenter Orchestrator Login Failed NERC: vCenter Orchestrator Virtual Machine Shutdown NERC: vCenter Orchestrator Virtual Machine Started NERC: vCenter Orchestrator vSwitch Add, Modify or Delete NERC: vCenter Permission Change NERC: vCenter Shutdown or Restart ESX NERC: vCenter User Login Failed NERC: vCenter User Login Successful NERC: vCenter Virtual Machine Shutdown NERC: vCenter Virtual Machine Started NERC: vCenter vSwitch Add, Modify or Delete NERC: vCloud Director Login Failed NERC: vCloud Director Login Success NERC: vCloud Organization Created NERC: vCloud Organization Deleted NERC: vCloud Organization Modified NERC: vCloud User Created NERC: vCloud User, Group, or Role Modified NERC: vCloud vApp Created, Deleted, or Modified NERC: vCloud vDC Created, Modified, or Deleted NERC: vShield Edge Configuration Change NERC: Windows Audit Log Cleared NERC: Windows Files Accessed NERC: Windows Group Members Added NERC: Windows Group Members Deleted NERC: Windows Groups Created NERC: Windows Groups Deleted NERC: Windows Groups Modified NERC: Windows Passwords Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: Windows Permissions Changed NERC: Windows Policies Changed NERC: Windows Privileges Escalated NERC: System Restarted
CIP-005-1 R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	**Compliance Suite Reports** NERC: VPN Sessions by Destination IPs NERC: VPN Sessions by Source IPs NERC: VPN Sessions by Users **Compliance Suite Alerts** None

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	**Compliance Suite Reports** NERC: Denied Connections by IP Addresses NERC: Denied Connections - Cisco IOS NERC: Denied Connections - Cisco NXOS NERC: Denied Connections - Cisco Router NERC: Denied Connections - F5 BIG-IP TMOS NERC: Denied Connections - Sidewinder NERC: Denied Connections - VMware vShield NERC: Denied Inbound Connections - Check Point NERC: Denied Inbound Connections - Cisco ASA NERC: Denied Inbound Connections - Cisco FWSM NERC: Denied Inbound Connections - Cisco PIX NERC: Denied Inbound Connections - Juniper Firewall NERC: Denied Outbound Connections - Check Point NERC: Denied Outbound Connections - Cisco ASA NERC: Denied Outbound Connections - Cisco FWSM NERC: Denied Outbound Connections - Cisco PIX NERC: Denied Outbound Connections - Juniper Firewall NERC: DHCP Activities on Microsoft DHCP NERC: DHCP Activities on VMware vShield NERC: Unauthorized Logins NERC: VPN Denied Connections by Users **Compliance Suite Alerts** None

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R1.4	The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. LogLogic solution can assist with the vulnerability assessment by providing a report on the access points and ports that are available for services.	**Compliance Suite Reports** NERC: DHCP Activities on Microsoft DHCP NERC: DHCP Activities on VMware vShield

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R4.2	A review to verify that only ports and services required for operations at these access points are enabled.	**Compliance Suite Reports** NERC: Allowed URLs by Source IPs NERC: Allowed URLs by Source IPs - F5 BIG-IP TMOS NERC: Allowed URLs by Source IPs - Microsoft IIS NERC: Allowed URLs by Source Users NERC: Allowed URLs by Source Users - F5 BIG-IP TMOS NERC: Allowed URLs by Source Users - Microsoft IIS NERC: Blocked URLs by Source IPs NERC: Blocked URLs by Source IPs - F5 BIG-IP TMOS NERC: Blocked URLs by Source IPs - Microsoft IIS NERC: Blocked URLs by Source Users NERC: Blocked URLs by Source Users - F5 BIG-IP TMOS NERC: Blocked URLs by Source Users - Microsoft IIS NERC: Ports Denied Access - Check Point NERC: Ports Denied Access - Cisco ASA NERC: Ports Denied Access - Cisco FWSM NERC: Ports Denied Access - Cisco IOS NERC: Ports Denied Access - Cisco PIX NERC: Ports Denied Access - Cisco Router NERC: Ports Denied Access - F5 BIG-IP TMOS NERC: Ports Denied Access - Fortinet NERC: Ports Denied Access - Juniper Firewall NERC: Ports Denied Access - Juniper JunOS NERC: Ports Denied Access - Juniper RT Flow NERC: Ports Denied Access - Nortel NERC: Ports Denied Access - PANOS NERC: Ports Denied Access - Sidewinder NERC: Ports Denied Access - VMware vShield **Compliance Suite Alerts** None

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-005-1 R4.4	A review of controls for default accounts, passwords, and network management community strings.	**Compliance Suite Reports** NERC: Juniper Firewall Reset Accepted NERC: Juniper Firewall Reset Imminent NERC: i5/OS Restore Events NERC: LogLogic Management Center Restore Activities **Compliance Suite Alerts** None
CIP-005-1 R5	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	N/A
CIP-005-1 R5.3	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	**Compliance Suite Reports** NERC: VPN Users Accessing Corporate Network **Compliance Suite Alerts** None
CIP-006-1		
CIP-006-1 R4	Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using computerized logging as one of the methods.	N/A

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-006-1 R5	Access log retention for at least 90 days.	N/A
CIP-007		

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R4	Use anti-virus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets within the Electronic Security Perimeter(s).	**Compliance Suite Reports** NERC: Attackers by Service - FireEye MPS NERC: Attackers by Signature - FireEye MPS NERC: Cisco ESA: Attacks by Event ID NERC: Cisco ESA: Attacks Detected NERC: Cisco ESA: Attacks by Threat Name NERC: Cisco ESA: Scans NERC: Cisco ESA: Updated NERC: FireEye MPS: Attacks by Event ID NERC: FireEye MPS: Attacks by Threat Name NERC: FireEye MPS: Attacks Detected NERC: FortiOS: Attacks Detected NERC: FortiOS: Attacks by Event ID NERC: FortiOS: Attacks by Threat Name NERC: FortiOS DLP Attacks Detected NERC: McAfee AntiVirus: Attacks Detected NERC: McAfee AntiVirus: Attacks by Event ID NERC: McAfee AntiVirus: Attacks by Threat Name NERC: PANOS: Attacks by Event ID NERC: PANOS: Attacks by Threat Name NERC: PANOS: Attacks Detected NERC: Symantec AntiVirus: Attacks by Event ID NERC: Symantec AntiVirus: Attacks by Threat Name NERC: Symantec AntiVirus: Attacks Detected NERC: Symantec AntiVirus: Scans NERC: Symantec AntiVirus: Updated NERC: Symantec Endpoint Protection: Attacks Detected NERC: Symantec Endpoint Protection: Attacks by Threat Name NERC: Symantec Endpoint Protection: Scans NERC: Symantec Endpoint Protection: Updated NERC: TrendMicro Control Manager: Attacks Detected NERC: TrendMicro Control Manager: Attacks Detected by Threat Name

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007-5 R1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports.	**Compliance Suite Reports** NERC: Ports Allowed Access - Check Point NERC: Ports Allowed Access - Cisco ASA NERC: Ports Allowed Access - Cisco FWSM NERC: Ports Allowed Access - Cisco IOS NERC: Ports Allowed Access - Cisco Netflow NERC: Ports Allowed Access - Cisco PIX NERC: Ports Allowed Access - F5 BIG-IP TMOS NERC: Ports Allowed Access - Fortinet NERC: Ports Allowed Access - Juniper Firewall NERC: Ports Allowed Access - Juniper JunOS NERC: Ports Allowed Access - Juniper RT Flow NERC: Ports Allowed Access - Nortel NERC: Ports Allowed Access - PANOS NERC: Ports Allowed Access - Sidewinder NERC: Ports Allowed Access - VMware vShield
CIP-007-5 R1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**Compliance Suite Reports** NERC: Ports Denied Access - Check Point NERC: Ports Denied Access - Cisco ASA NERC: Ports Denied Access - Cisco FWSM NERC: Ports Denied Access - Cisco IOS NERC: Ports Denied Access - Cisco Router NERC: Ports Denied Access - Cisco PIX NERC: Ports Denied Access - F5 BIG-IP TMOS NERC: Ports Denied Access - Fortinet NERC: Ports Denied Access - Juniper Firewall NERC: Ports Denied Access - Juniper JunOS NERC: Ports Denied Access - Juniper RT Flow NERC: Ports Denied Access - Nortel NERC: Ports Denied Access - PANOS NERC: Ports Denied Access - Sidewinder NERC: Ports Denied Access - VMware vShield

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007-5 R2	Document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets in the Electronic Security Perimeters.	**Compliance Suite Reports** NERC: Cisco ESA: Updated NERC: Symantec AntiVirus: Updated NERC: Symantec Endpoint Protection: Updated
CIP-007-5 R2.1	Document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets in the Electronic Security Perimeters.	**Compliance Suite Reports** NERC: vCenter Restart ESX Services **Compliance Suite Alerts** NERC: vCenter Restart ESX Services

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007-5 R3	Use anti-virus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets in the Electronic Security Perimeters.	**Compliance Suite Reports** NERC: Administrator Logins on Windows Servers NERC: Cisco ESA: Attacks by Event ID NERC: Cisco ESA: Attacks Detected NERC: Cisco ESA: Attacks by Threat Name NERC: Cisco ESA: Scans NERC: Cisco ESA: Updated NERC: DB2 Database Failed Logins NERC: DB2 Database Successful Logins NERC: ESX Failed Logins NERC: ESX Logins Failed Unknown User NERC: ESX Logins Succeeded NERC: F5 BIG-IP TMOS Login Failed NERC: F5 BIG-IP TMOS Login Successful NERC: Failed Logins NERC: Files Accessed on Servers NERC: Files Accessed on NetApp Filer Audit NERC: Files Accessed through Juniper SSL VPN (Secure Access) NERC: Files Accessed through PANOS NERC: Files Downloaded via Proxy NERC: Files Downloaded via Proxy - Blue Coat Proxy NERC: Files Downloaded via Proxy - Cisco WSA NERC: Files Downloaded via Proxy - Microsoft IIS NERC: Files Downloaded via the Web NERC: Files Downloaded via the Web - F5 BIG-IP TMOS NERC: Files Downloaded via the Web - Microsoft IIS NERC: Files Uploaded via Proxy NERC: Files Uploaded via Proxy - Blue Coat Proxy NERC: Files Uploaded via Proxy - Cisco WSA NERC: Files Uploaded via the Web - F5 BIG-IP TMOS NERC: Files Uploaded via Proxy - Microsoft IIS NERC: Files Uploaded via the Web - Microsoft IIS

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: Files Uploaded via the Web NERC: FireEye MPS: Attackers by Service NERC: FireEye MPS: Attackers by Signature NERC: FireEye MPS: Attacks by Event ID NERC: FireEye MPS: Attacks by Threat Name NERC: FireEye MPS: Attacks Detected NERC: Files Accessed Through Pulse Connect Secure

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007-5 R3	Use anti-virus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets in the Electronic Security Perimeters.	**Compliance Suite Reports** (Cont.) NERC: FortiOS: Attacks Detected NERC: FortiOS: Attacks by Event ID NERC: FortiOS: Attacks by Threat Name NERC: FortiOS DLP Attacks Detected NERC: Guardium SQL Guard Audit Logins NERC: Guardium SQL Guard Logins NERC: HP NonStop Audit Login Failed NERC: HP NonStop Audit Login Successful NERC: i5/OS Access Control List Modifications NERC: Last Activities Performed by Administrators NERC: Last Activities Performed by All Users NERC: Logins by Authentication Type NERC: LogLogic DSM Logins NERC: LogLogic Management Center Login NERC: McAfee AntiVirus: Attacks Detected NERC: McAfee AntiVirus: Attacks by Event ID NERC: McAfee AntiVirus: Attacks by Threat Name NERC: Microsoft Sharepoint Content Updates NERC: Microsoft SQL Server Database Failed Logins NERC: Microsoft SQL Server Database Successful Logins NERC: NetApp Filer Audit Login Failed NERC: NetApp Filer Audit Login Successful NERC: NetApp Filer File Activity NERC: NetApp Filer Login Failed NERC: NetApp Filer Login Successful NERC: Oracle Database Failed Logins NERC: Oracle Database Successful Logins NERC: PANOS: Attacks by Event ID NERC: PANOS: Attacks by Threat Name NERC: PANOS: Attacks Detected NERC: RACF Failed Logins NERC: RACF Files Accessed NERC: RACF Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: Root Logins
CIP-007-5 R3	Use anti-virus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets in the Electronic Security Perimeters.	**Compliance Suite Reports** (Cont.) NERC: Successful Logins NERC: Sybase ASE Failed Logins NERC: Sybase ASE Successful Logins NERC: Symantec AntiVirus: Attacks by Event ID NERC: Symantec AntiVirus: Attacks by Threat Name NERC: Symantec AntiVirus: Attacks Detected NERC: Symantec AntiVirus: Scans NERC: Symantec AntiVirus: Updated NERC: Symantec Endpoint Protection: Attacks Detected NERC: Symantec Endpoint Protection: Attacks by Threat Name NERC: Symantec Endpoint Protection: Scans NERC: Symantec Endpoint Protection: Updated NERC: TIBCO ActiveMatrix Administrator Failed Logins NERC: TIBCO ActiveMatrix Administrator Successful Logins NERC: TrendMicro Control Manager: Attacks Detected NERC: TrendMicro Control Manager: Attacks Detected by Threat Name NERC: TrendMicro OfficeScan: Attacks Detected NERC: TrendMicro OfficeScan: Attacks Detected by Threat Name NERC: Unencrypted Logins NERC: vCenter Failed Logins NERC: vCenter Orchestrator Failed Logins NERC: vCenter Successful Logins NERC: vCloud Failed Logins NERC: vCloud Successful Logins NERC: VPN Connections by Users NERC: Web Access from All Users

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007-5 R3	Use anti-virus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets in the Electronic Security Perimeters.	**Compliance Suite Reports** (Cont.) NERC: Web Access from All Users - Fortinet NERC: Web Access from All Users - F5 BIG-IP TMOS NERC: Web Access from All Users - Microsoft IIS NERC: Web Access from All Users - PANOS NERC: Web Access to Applications - Fortinet NERC: Web Access to Applications - F5 BIG-IP TMOS NERC: Web Access to Applications - Microsoft IIS NERC: Web Access to Applications - PANOS NERC: Web Access to Applications
CIP-007-5 R3	Use anti-virus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets in the Electronic Security Perimeters.	**Compliance Suite Alerts** NERC: Cisco PIX, ASA, FWSM Logon Failure NERC: Guardium SQL Guard Logins NERC: Juniper Firewall Logon Failure NERC: Logins Failed NERC: Logins Succeeded NERC: LogLogic DSM Logins NERC: Microsoft SharePoint Content Updated NERC: vCenter User Login Failed NERC: vCenter User Login Successful NERC: vCenter Orchestrator Login Failed NERC: vCloud Director Login Failed NERC: vCloud Director Login Success

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5	Establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity and that minimize the risk of unauthorized system access.	**Compliance Suite Reports** NERC: Administrator Logins on Windows Servers NERC: DB2 Database Failed Logins NERC: DB2 Database Successful Logins NERC: ESX Failed Logins NERC: ESX Logins Failed Unknown User NERC: ESX Logins Succeeded NERC: F5 BIG-IP TMOS Login Failed NERC: F5 BIG-IP TMOS Login Successful NERC: Failed Logins NERC: Files Accessed on Servers NERC: Files Accessed on NetApp Filer Audit NERC: Files Accessed through Juniper SSL VPN (Secure Access) NERC: Files Accessed through PANOS NERC: Files Accessed Through Pulse Connect Secure NERC: Files Downloaded via Proxy NERC: Files Downloaded via Proxy - Blue Coat Proxy NERC: Files Downloaded via Proxy - Cisco WSA NERC: Files Downloaded via Proxy - Microsoft IIS NERC: Files Downloaded via the Web NERC: Files Downloaded via the Web - F5 BIG-IP TMOS NERC: Files Downloaded via the Web - Microsoft IIS NERC: Files Uploaded via Proxy NERC: Files Uploaded via Proxy - Blue Coat Proxy NERC: Files Uploaded via Proxy - Cisco WSA NERC: Files Uploaded via Proxy - Microsoft IIS NERC: Files Uploaded via the Web NERC: Files Uploaded via the Web - F5 BIG-IP TMOS NERC: Files Uploaded via the Web - Microsoft IIS NERC: Guardium SQL Guard Audit Logins NERC: Guardium SQL Guard Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: HP NonStop Audit Login Failed NERC: HP NonStop Audit Login Successful NERC: i5/OS Access Control List Modifications

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5	Establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity and that minimize the risk of unauthorized system access.	**Compliance Suite Reports** (Cont.) NERC: Last Activities Performed by Administrators NERC: Last Activities Performed by All Users NERC: Logins by Authentication Type NERC: LogLogic DSM Logins NERC: LogLogic Management Center Login NERC: Microsoft SQL Server Database Failed Logins NERC: Microsoft SQL Server Database Successful Logins NERC: NetApp Filer Audit Login Failed NERC: NetApp Filer Audit Login Successful NERC: NetApp Filer File Activity NERC: NetApp Filer Login Failed NERC: NetApp Filer Login Successful NERC: Oracle Database Failed Logins NERC: Oracle Database Successful Logins NERC: RACF Failed Logins NERC: RACF Files Accessed NERC: RACF Successful Logins NERC: Root Logins NERC: Successful Logins NERC: Sybase ASE Failed Logins NERC: Sybase ASE Successful Logins NERC: TIBCO ActiveMatrix Administrator Failed Logins NERC: TIBCO ActiveMatrix Administrator Successful Logins NERC: Unauthorized Logins NERC: Unencrypted Logins NERC: Users Using the Proxies NERC: Users Using the Proxies - Blue Coat Proxy NERC: Users Using the Proxies - Cisco WSA NERC: Users Using the Proxies - Microsoft IIS

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5	Establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity and that minimize the risk of unauthorized system access.	**Compliance Suite Reports** (Cont.) NERC: vCenter Failed Logins NERC: vCenter Orchestrator Failed Logins NERC: vCloud Failed Logins NERC: vCenter Successful Logins NERC: vCloud Successful Logins NERC: VPN Connections by Users NERC: Web Access from All Users NERC: Web Access from All Users - F5 BIG-IP TMOS NERC: Web Access from All Users - Fortinet NERC: Web Access from All Users - Microsoft IIS NERC: Web Access from All Users - PANOS NERC: Web Access to Applications - Fortinet NERC: Web Access to Applications - F5 BIG-IP TMOS NERC: Web Access to Applications - Microsoft IIS NERC: Web Access to Applications - PANOS NERC: Web Access to Applications
CIP-007 R5	Establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity and that minimize the risk of unauthorized system access.	**Compliance Suite Alerts** NERC: Cisco PIX, ASA, FWSM Logon Failure NERC: Guardium SQL Guard Logins NERC: Juniper Firewall Logon Failure NERC: Logins Failed NERC: Logins Succeeded NERC: LogLogic DSM Logins NERC: vCenter User Login Failed NERC: vCenter User Login Successful NERC: vCenter Orchestrator Login Failed NERC: vCloud Director Login Failed NERC: vCloud Director Login Success

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5.1.1	Ensure that user accounts are implemented as approved by designated personnel as specified in CIP-003 Requirement 5.	**Compliance Suite Reports** NERC: Account Activities on UNIX Servers NERC: Account Activities on Windows Servers NERC: Accounts Changed on NetApp Filer NERC: Accounts Changed on TIBCO Administrator NERC: Accounts Changed on TIBCO ActiveMatrix Administrator NERC: Accounts Changed on UNIX Servers NERC: Accounts Changed on Windows Servers NERC: Accounts Created on NetApp Filer NERC: Accounts Created on NetApp Filer Audit NERC: Accounts Created on Sidewinder NERC: Accounts Created on Symantec Endpoint Protection NERC: Accounts Created on TIBCO Administrator NERC: Accounts Created on TIBCO ActiveMatrix Administrator NERC: Accounts Created on UNIX Servers NERC: Accounts Created on Windows Servers NERC: Accounts Deleted on NetApp Filer NERC: Accounts Deleted on NetApp Filer Audit NERC: Accounts Deleted on Symantec Endpoint Protection NERC: Accounts Deleted on TIBCO Administrator NERC: Accounts Deleted on TIBCO ActiveMatrix Administrator NERC: Accounts Deleted on Sidewinder NERC: Accounts Deleted on UNIX Servers NERC: Accounts Deleted on Windows Servers NERC: Cisco ISE, ACS Accounts Created NERC: Cisco ISE, ACS Accounts Removed NERC: ESX Accounts Activities NERC: ESX Accounts Created NERC: ESX Accounts Deleted NERC: LogLogic Management Center Account Activities

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5.1.1	Ensure that user accounts are implemented as approved by designated personnel as specified in CIP-003 Requirement 5.	**Compliance suite Reports** (Cont.) NERC: Microsoft Operations Manager - Windows Accounts Activities NERC: Microsoft Operations Manager - Windows Accounts Changed NERC: Microsoft Operations Manager - Windows Accounts Created NERC: Microsoft Operations Manager - Windows Accounts Enabled NERC: NetApp Filer Audit Accounts Enabled NERC: NetApp Filer Audit Group Members Added NERC: NetApp Filer Audit Group Members Deleted NERC: RACF Accounts Created NERC: RACF Accounts Deleted NERC: RACF Accounts Modified NERC: vCloud User Created NERC: vCloud User Deleted or Removed NERC: Windows Accounts Enabled NERC: Windows Accounts Locked NERC: Windows Group Members Added NERC: Windows Group Members Deleted **Compliance Suite Alerts** NERC: Accounts Created NERC: Accounts Deleted NERC: Accounts Enabled NERC: Accounts Locked NERC: Accounts Modified NERC: Group Members Added NERC: Group Members Deleted NERC: vCloud User Created NERC: Windows Group Members Added NERC: Windows Group Members Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5.1.2 / CIP-007-5 R4.1	Establish methods and procedures that generate logs of sufficient detail to create historical and audit trails to individual user account access activity for a minimum of 90 days.	**Compliance Suite Reports** NERC: Account Activities on UNIX Servers NERC: Account Activities on Windows Servers NERC: Bandwidth Usage by User NERC: ESX Accounts Activities NERC: ESX Group Activities NERC: ESX Kernel log daemon terminating NERC: ESX Kernel logging Stop NERC: ESX Syslogd Restart NERC: F5 BIG-IP TMOS Restarted NERC: Group Activities on NetApp Filer Audit NERC: Group Activities on Symantec Endpoint Protection NERC: Group Activities on TIBCO ActiveMatrix Administrator NERC: Group Activities on UNIX Servers NERC: Group Activities on Windows Servers NERC: LogLogic Management Center Account Activities NERC: Microsoft Operations Manager - Windows Accounts Activities NERC: Microsoft Operations Manager - Windows Events by Users NERC: Users Created on Servers NERC: Users Removed from Servers NERC: Users Using the Proxies NERC: Users Using the Proxies - Blue Coat Proxy NERC: Users Using the Proxies - Cisco WSA NERC: Users Using the Proxies - Microsoft IIS NERC: vCenter Restart ESX Services NERC: VPN Connections by Users NERC: VPN Sessions by Users NERC: VPN Users Accessing Corporate Network NERC: Windows Events by Users **Compliance Suite Alerts** NERC: vCenter Restart ESX Services

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5.2 / CIP-007-5 R5.3	Implement a policy to minimize and manage the scope and acceptable use of admin, shared and other generic account privileges.	**Compliance Suite Reports** NERC: Accounts Changed on NetApp Filer NERC: Accounts Changed on TIBCO Administrator NERC: Accounts Changed on TIBCO ActiveMatrix Administrator NERC: Accounts Changed on UNIX Servers NERC: Accounts Changed on Windows Servers NERC: Administrator Logins on Windows Servers NERC: DB2 Database Successful Logins NERC: Domain activities on Symantec Endpoint Protection NERC: ESX Logins Succeeded NERC: F5 BIG-IP TMOS Login Successful NERC: Guardium SQL Guard Audit Logins NERC: Guardium SQL Guard Logins NERC: HP NonStop Audit Login Successful NERC: HP NonStop Audit Permissions Changed NERC: LogLogic DSM Logins NERC: LogLogic Management Center Login NERC: Microsoft Operations Manager - Windows Accounts Changed NERC: Microsoft Operations Manager - Windows Permissions Modified NERC: Microsoft Operations Manager - Windows Policies Modified NERC: Microsoft Sharepoint Permissions Changed NERC: Microsoft SQL Server Database Successful Logins NERC: NetApp Filer Audit Group Members Added NERC: NetApp Filer Audit Group Members Deleted NERC: NetApp Filer Audit Login Successful NERC: NetApp Filer Audit Policies Modified NERC: NetApp Filer Login Successful NERC: Oracle Database Successful Logins NERC: Permissions Modified on Windows Servers NERC: Policies Modified on Windows Servers

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		NERC: RACF Accounts Modified
CIP-007 R5.2 / CIP-007-5 R5.3	Implement a policy to minimize and manage the scope and acceptable use of admin, shared and other generic account privileges.	**Compliance Suite Reports** (Cont.) NERC: RACF Permissions Changed NERC: RACF Successful Logins NERC: Successful Logins NERC: Sybase ASE Successful Logins NERC: Symantec Endpoint Protection Policy Add, Remove, or Modify NERC: TIBCO Administrator Permission Changes NERC: TIBCO ActiveMatrix Administrator Permission Changes NERC: TIBCO ActiveMatrix Administrator Successful Logins NERC: Trusted Domain Created on Windows Servers NERC: Trusted Domain Deleted on Windows Servers NERC: vCenter Successful Logins NERC: vCenter User Permission Change NERC: vCloud Successful Logins NERC: Windows Group Members Added NERC: Windows Group Members Deleted **Compliance Suite Alerts** NERC: Accounts Modified NERC: Guardium SQL Guard Logins NERC: HP NonStop Audit Permission Changed NERC: Logins Succeeded NERC: LogLogic DSM Logins NERC: Microsoft Operations Manager - Permissions Changed NERC: Microsoft Operations Manager - Windows Policies Changed NERC: Microsoft Sharepoint Permission Changed NERC: NetApp Filer Audit Policies Changed NERC: RACF Permissions Changed NERC: TIBCO ActiveMatrix Administrator Permission Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R5.2 / CIP-007-5 R5.3	Implement a policy to minimize and manage the scope and acceptable use of admin, shared and other generic account privileges.	**Compliance Suite Reports** (Cont.) NERC: vCenter Permission Change NERC: vCenter User Login Successful NERC: vCloud Director Login Success NERC: Windows Group Members Deleted NERC: Windows Permissions Changed NERC: Windows Policies Changed
CIP-007 R5.3.3 / CIP-007-5 R5.6	Each password shall be changed at least annually or more frequently based on risk.	**Compliance Suite Reports** NERC: Cisco ISE, ACS Password Changes NERC: F5 BIG-IP TMOS Password Changes NERC: i5/OS DST Password Reset NERC: LogLogic Management Center Password Changes NERC: Microsoft Operations Manager - Windows Password Changes NERC: Microsoft SQL Server Password Changes NERC: NetApp Filer Password Changes NERC: Novell eDirectory Password Changes NERC: Password Changes on Windows Servers NERC: RACF Password Changed NERC: Symantec Endpoint Protection Password Changes NERC: TIBCO Administrator Password Changes NERC: Unix Password Changes **Compliance Suite Alerts** NERC: Cisco ISE, ACS Passwords Changed NERC: IBM AIX Password Changed NERC: LogLogic Management Center Passwords Changed NERC: Microsoft Operations Manager - Windows Passwords Changed NERC: RACF Passwords Changed NERC: Windows Passwords Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
CIP-007 R6.2 / CIP-007-5 R4.2	The security monitoring controls shall issue automated or manual alerts for security incidents.	**Compliance Suite Reports** NERC: Attackers by Service NERC: Attackers by Signature NERC: Attackers by Service - Cisco IOS NERC: Attackers by Service - ISS SiteProtector NERC: Attackers by Service - SiteProtector NERC: Attackers by Service - Sourcefire Defense Center NERC: Attackers by Signature - Cisco IOS NERC: Attackers by Signature - ISS SiteProtector NERC: Attackers by Signature - SiteProtector NERC: Attackers by Signature - Sourcefire Defense Center NERC: Attacks Detected NERC: Attacks Detected - Cisco IOS NERC: Attacks Detected - HIPS NERC: Attacks Detected - ISS SiteProtector NERC: Attacks Detected - SiteProtector NERC: Attackers Detected - Sourcefire Defense Center NERC: FireEye MPS: Sensors Generating Alerts **Compliance Suite Alerts** NERC: Anomalous IDS Alerts NERC: Sensors Generating Alerts - FireEye MPS
CIP-007 R6.5 / CIP-007-5 R4.4	Review logs of system events related to cyber security and maintain records documenting review of logs.	**Compliance Suite Reports** NERC: Periodic Review of Log Reports NERC: Periodic Review of User Access Logs **Compliance Suite Alerts** None