

## NERC CIP'S AND IDENTITY MANAGEMENT

### Executive Summary

NERC CIP requires significant recurring effort to prepare asset databases and report on access controls. This paper outlines, for each specific CIP, where identity management can assist you in reducing your overall costs, labor effort while at the same time strengthening your overall security.

### Author:

**Guy Huntington**

**President**

**Huntington Ventures Ltd – “The Business of Identity Management”**

## Table of Contents

|  |   |
|--|---|
| NERC CIP's and Identity Management ..... | 1 |
| Executive Summary .....                  | 1 |
| CIP 002.....                             | 3 |
| R2 and R3 .....                          | 3 |
| CIP 003.....                             | 4 |
| R1.2 .....                               | 4 |
| R2.1 and 2.2.....                        | 4 |
| R4 and 5 .....                           | 4 |
| CIP 004.....                             | 5 |
| R2.1 -2.3.....                           | 5 |
| R3.....                                  | 5 |
| R4 .....                                 | 5 |
| CIP 005.....                             | 6 |
| R2.....                                  | 6 |
| R3.....                                  | 6 |
| R5.....                                  | 6 |
| CIP - 006.....                           | 7 |
| R1 .....                                 | 7 |
| R2.....                                  | 7 |
| R3-5.....                                | 7 |
| CIP 007.....                             | 8 |
| R5.....                                  | 8 |
| R6 .....                                 | 8 |
| Conclusion.....                          | 9 |
| About the Author .....                   | 9 |

## CIP 002

### R2 and R3

Many utilities have more than one database that refers to critical assets. There is an operational problem in tying together the disparate databases to an authoritative source. These include:

- Naming convention in each database for the asset
- Adding, editing or removing assets in the different databases

A SCADA LDAP (Lightweight Directory Access Protocol) directory can assist in this. What is this?

A directory is a partition-able identity electronic touchstone for the enterprise. In the SCADA network, the directory would be automatically fed by the authoritative source for the asset. Each asset would be given a unique identification that the directory would store as well as any asset information that the enterprise deems important to store in the directory as well as the database.

The SCADA directory would then use a virtual directory to point to the different databases containing the same asset. When the authoritative source for the asset changes, the directory would either make the change itself in the database or trigger a message to the database admin to make the change.

This way, all asset databases are synced up. Creating the list of critical assets could be easily reported off the SCADA directory.

## CIP 003

### R1.2

The identity management system can be designed to automatically display the policies to personnel and then record that they have read the document. Personnel can be automatically selected for this based on the role they play, a department or group they belong to or to a physical location. This can then be automatically tracked in the identity management system and easily produced for auditors.

### R2.1 and 2.2

The identity management system can centrally administer roles. When an identity is assigned to this role, the regulatory report can be automatically produced with all the identity information required. Further, the senior manager's role can be automatically given access rights and privileges to fulfill CIP functionality required. Any change to the senior manager can be automatically documented the day it occurs. The identity management system is fed by the authoritative source for the identity. The role change for the senior manager is instantly picked up and then the identity is provisioned or deprovisioned with apps, systems, physical access and content privileges. CIP reports can be automatically produced.

### R4 and 5

Content management security policies are linked to the identity management system. Roles, groups, departments, etc are used to automatically assign content creation, viewing, editing and auditing policies for each document or groups of documents. Auditors can quickly be able to see what the security policy is for each piece of content and then be able to determine what identities access the content, when and what changes, if any, were made to the content. CIP reports can be automatically generated, for any time period, indicating what personnel have access rights to the content.

Attestation reports can be automatically generated and sent to the line managers. These ask the manager to attest to the rights the identities reporting to them have re content. They only take a few minutes to review and then to electronically approve. The attestation reports are then summed up to the Responsible Entity who can then approve all the reports and easily generate, at any time, a CIP compliance report.

The Responsible Entity will also approve all content management security policies, including all change management and be able to easily generate lists of these policies to auditors.

## CIP 004

### R2.1 -2.3

The identity management system can automatically enforce training on all identities that are accessing critical cyber assets. For example, when a new hire or a contractor is hired, the identity management system could automatically schedule them in for a training course. The system might be designed such that their security badge for physical access is only granted when the identity has successfully completed the course or viewed a program.

Further, the identity management system can track the time period that has elapsed with training not done. It can then automatically escalate this to senior managers at certain pre-determined points.

Automatic reports can be generated, at any time, showing what identities have access to critical cyber assets and when they have completed their training.

### R3

As part of the identity business process, the identity management system can automatically send off requests to local, state and federal agencies for things like background checks. The workflow can then be set up to have the documentation received back electronically approved by a manager before the identity is allowed to be created in the authoritative source or assigned access rights (both logical and physical) for the identity to critical cyber assets. Automatic CIP reports can be generated showing that all identities received their background checks and/or had their background check re-done after a fixed period of time.

### R4

By integrating the utility's physical access control system with identity management, it is very easy to design a system that automatically:

- Provisions electronic and physical access to cyber assets
- Updates identity access privileges when role changes occur
- Instantly terminate access privileges when the identity is terminated
- Produces reports each day, week, month, quarter, semi-annually and annually on who has access to what critical cyber assets
- Sends managers attestation reports on a pre-determined basis to ask them to attest the identities reporting to them and their access rights. These take only a few minutes to approve electronically.

## CIP 005

### R2

The identity management system's access controls should have an installation in place in the SCADA network and a separate implementation in the IT network. This provides the utility with an enterprise access control system that automatically enforces authentication, authorization and audit policies.

Stronger authentication for both logical and physical access points should be used based on risk. The identity management access control system provides a framework to allow for easy change of different authentication methods, over time, based on risk and new attack vectors. For instance, if the utility decides that a biometric plus a smart card is now required for a group of cyber assets, the new authentication policy and interface only has to be done once at the enterprise access control system and not for each device or application that it is controlling.

Creation of authorization rights are controlled by the identity management provisioning system. Enforcement of the authorization can take place by the identity management access system or by the application or device itself.

External access controls are also administered by the identity management access system. The use of stronger authentication, where required, is then enforced.

Appropriate use banners can be easily integrated by the enterprise and SCADA identity management access control systems.

### R3

Monitoring for SCADA, IT and Physical security should be done at a central security ops command console. The identity management system, integrated with the physical security system, is a key piece of the monitoring data. For example, it will report things like:

- Failed authentications both physical and logical
- Number of authentications per second and per minute
- Number of authorizations per second and per minute
- Number of failed authorizations per second and per minute
- Door entries per minute per facility per location in the facility

When this is integrated in the command console with perimeter defense data, it will become quickly apparent when a cyber attack is in progress and defensive measures can be quickly taken.

### R5

All identity management access logs should be available for at least the last three years.

## CIP – 006

### R1

As part of the identity management business processes, identity processes should be created that determine which facility or portions thereof, an identity type is allowed physical access to and whether or not it should be escorted or unescorted.

By integrating the physical security system with the identity management system, the following will occur:

- Quick provisioning, role change and termination of physical security badges
- Integrated monitoring of all physical access points with identity management
- Easy CIP and auditor reporting showing compliance

### R2

#### 2.1 – Card keys

If the keys are going to use a digital certificate, then the actual digital cert will be issued and stored in the enterprise directory. A copy of this may then be automatically passed to the physical security systems database as part of the provisioning process done by the identity management system on the physical security system. When an identity is terminated, the enterprise identity management system then revokes the digital certificate which in turn is automatically revoked in the physical security system.

#### 2.2 – Special Locks

The identity management system will track each key and master building key issued to an identity. When the identity undergoes a role change or is terminated, the identity management system will automatically notify the identity's current manager of the need to recover the key. After a pre-determined amount of time, if the key hasn't been recovered by the manager, this will automatically be escalated to senior management. It is possible to link return of the master keys to the final payment made to the identity upon termination.

### 2.4

Stronger authentication can be universally enforced for physical access across the utility's system by the identity management and integrated physical security system. Further, if required, the identity management system can do regular segregation of duty checks to ensure that identities only have access to certain areas and not others.

### R3-5

Monitoring of physical assets can be combined by integrating different physical security devices to the identity management system. This allows for centralization of monitoring and designing escalation triggers for certain data points.

## CIP 007

### R5

Automatic account management reports can be generated by the identity management system. Enforcement of the account management policies is done by the identity management provisioning and access systems.

Provisioning of the account may be done after receiving one or many management electronic approvals via the identity management provisioning system. This enforces the “need to know” policies of the enterprise. Exception privileges, for example in an emergency, will also be enforced by the identity management system. A complete audit trail of all permissions granted is always immediately available from the identity management system.

In cases where passwords are used, the identity management system will enforce password policies. These will include enforcement of password type, length, password failures allowed, time until reset, new password times, etc. The identity management system can also provide a user self-serve feature to allow users to quickly and easily reset their passwords.

The number of passwords an identity has to remember will be dramatically lowered. This allows the enterprise to work with their identities on having one long password complete with upper and lower case characters as well as numbers and special characters. Finally, passwords like other forms of authentication will be instantly disabled when an identity is terminated by the identity management system.

### R6

As previously mentioned in this paper, the monitoring of the cyber security assets can be enhanced by implanting identity management integrated with physical security. See CIP 005 R3 for more information.

## Conclusion

A large part of CIP revolves around:

- Identities interacting with cyber security assets both physically and logically
- Who has the rights to these assets
- Who approves them
- Privileges granted
- Use of different authentication methods
- Authorization privileges
- Monitoring
- Reporting

If you're like most utilities, you're probably scrambling to comply. You likely are creating numerous spreadsheets, lists and databases to track all of this. The amount of effort involved and costs are very significant.

You can lower your overall costs and time effort to comply, year after year, by deploying identity management. It will significantly reduce the effort to:

- Cross-link critical cyber assets to their databases
- Produce CIP and audit reports on who was given access to what when
- Enforce management approvals for granting physical and electronic access to cyber assets
- Enforce enterprise authentication and authorization policies
- Ensure that all workers are properly trained

## About the Author

Guy Huntington, President, Huntington Ventures Ltd., has lead and rescued many large Fortune 500 identity projects including Boeing, Capital One and Kaiser Permanente. He has also lead Toronto Hydro's identity project and been instrumental in developing their security architecture. Guy can be reached at [guy@hvl.net](mailto:guy@hvl.net), [www.authenticationworld.com](http://www.authenticationworld.com) or cell at 604-861-6804.