imprivata®

The CIP Challenge

Securing Critical Cyber Assets in the Energy Industry

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Energy companies today have more to deal with than ever before—from a complex and challenging regulatory environment, to environmental challenges and pressure from investors and shareholders to increase profits. To survive, many energy companies have had to re-think the way they operate and make organizational changes to become more efficient. However, at the same time, concerns have increased throughout the industry about the security of energy companies' infrastructure and assets. In response to these concerns and the increased government oversight from the Federal Energy Regulatory Commission (FERC) that soon followed, the energy industry, through the North American Electric Reliability Corporation (NERC), developed new security standards regarding the protection of critical infrastructure.

The time has come for energy companies to determine whether their energy infrastructure and critical assets are as secure as they need to be and whether they have implemented best practices to protect information technology (IT) assets from both external and internal threats. These questions have taken on greater urgency in the post-9/11 world, and particularly since the energy industry, through NERC, has developed the new cyber-security standards.

While the goals of these Critical Infrastructure Protection (CIP) standards have been clearly defined, NERC has left it up to each energy company to determine how best to achieve them operationally. Although there has been a good deal of discussion and debate within the industry, best practices for CIP compliance are still evolving. The only thing agreed upon at this point is that most organizations are expected to achieve CIP compliance within the next three years—meaning that the majority of energy companies cannot wait until there is a consensus to act, as they could be facing the prospect of failed audits and substantial fines for non-compliance.

This whitepaper, produced in consultation with Imprivata customers and energy industry pundits, discusses the key issues surrounding CIP compliance and shows how Imprivata's OneSign® identity and access management platform can effectively support and accelerate a successful CIP compliance program.

THE CIP CHALLENGE—SELF-DEFINING AND SELF-SECURING ASSETS

For many energy companies, the mandate to secure all critical assets, and in particular critical cyber assets, is a daunting one. Not only do companies have to organize and define critical assets for themselves------a complex task on its own------but they have to secure the assets from both a physical and logical (IT) perspective and provide documentation of both. Then, they are likely to need to adopt newly deployed technology solutions to standardize and automate the process. Only then are they ready for the audit.

Adding to the challenge is that traditionally, there has been little overlap between energy companies' IT departments and the engineering organizations responsible for the Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS) that control their operations. Most energy companies have not dealt with the IT security requirements that other regulated industries have faced. As a result, they often do not have the in-house IT security expertise or dedicated resources needed to develop and implement a CIP compliance plan for cyber security. Timing is also a factor. The CIP standards went into effect on June 1, 2006 and most companies are mandated to be auditably compliant with all the standards before 2011, meaning the entity meets the full intent of the requirement and can demonstrate compliance to an auditor.

For more detail on the compliance timeline, NERC provides an implementation schedule that varies according to the different types of energy entities, such as Balancing Authorities, Transmission Operators, Transmission Service Providers, and Reliability Coordinators.

The challenge was well summed up in a recent article by Frost & Sullivan industry analyst Rob Ayoub in IT Compliance magazine. According to Ayoub, many organizations interviewed by his firm already failed to meet the first round requirements. “Most organizations agree that they will meet some of the standards and some companies believe that they, for one reason or another, will never really be compliant.” It is likely that the latter respondents are simply daunted by the magnitude of the compliance effort and are seeking help. However, the hefty costs associated with non-compliance—as much as $1 million for the most severe infractions—make it clear that inaction is not an option.

The good news is while some of the CIP standards require a significant commitment of time and human resources, there are technology solutions available that can—quickly, easily, and affordably—help organizations meet many of the CIP requirements, and, more importantly, ensure the security of all critical assets.

> “MOST ORGANIZATIONS AGREE THAT THEY WILL MEET SOME OF THE STANDARDS AND SOME COMPANIES BELIEVE THAT THEY, FOR ONE REASON OR ANOTHER, WILL NEVER REALLY BE COMPLIANT.”
>
> – Rob Ayoub,
> Frost & Sullivan industry analyst

Greater asset protection is not the only benefit

Despite the challenges, energy companies have more than one incentive to achieve CIP compliance. While the threat of terrorism has been the most urgent force driving the development of the CIP standards, the benefits of compliance go far beyond minimizing the risk and impact of cataclysmic physical attacks from external sources. Organizations that attain CIP compliance are also better prepared to respond to:

- Remote access threats to physical and IT assets;
- Internal threats to physical and IT assets;
- The need to safeguard confidential business and customer data in a networked environment;
- The need to improve reliability and minimize service interruptions; and
- Public safety concerns that may arise due to accidents or natural disasters.

By fulfilling the CIP requirements, energy firms can also gain greater control over their operations and resources, improve service levels, and compete more effectively.

The NERC mandate.

As the electric reliability organization for North America, NERC’s mandate is to improve reliability and security throughout the bulk power system in the United States and Canada. The initial standards intended to address cyber security in the energy infrastructure were issued in 2003 as NERC 1200 UAS, followed shortly thereafter by NERC 1300. The final set of standards was passed as NERC CIP in May of 2006. The first 83 NERC reliability standards were approved by FERC in early 2007, making them the first mandatory and legally enforceable standards for the U.S. bulk power system. These standards encompass all aspects of power generation and distribution operations.

THE CIP STANDARDS AND THE PROBLEMS THEY SOLVE

NERC has passed the following nine CIP cyber security standards:

- CIP-001 Sabotage Reporting
- CIP-002 Critical Cyber Assets
- CIP-003 Security Management Controls
- CIP-004 Personnel & Training
- CIP-005 Electronic Security
- CIP-006 Physical Security of Critical Cyber Assets

- CIP-007 Systems Security Management
- CIP-008 Incident Reporting and Response Planning
- CIP-009 Recovery Plans for Critical Cyber Assets

Each of these standards spells out the requirements for energy companies, the "responsible entity" charged with meeting the requirements, and what constitutes non-compliance.

Beyond trying to understand what the CIP standards require, it is equally essential for companies to understand what problems the standards are intended to solve. In a separate report entitled Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations published in March 2007 (http://www.nerc.com/~filez/cipfiles.html), NERC and the U.S. Department of Energy's National SCADA Test Bed Program filled in some of the blanks by identifying the following critical vulnerabilities in the energy industry:

1. Inadequate policies, procedures, and culture that govern control system security.
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms.
3. Remote access to the control system without appropriate access control.
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.
5. Use of inadequately secured WiFi wireless communication for control.
6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes.
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity.
8. Unauthorized or inappropriate applications or devices on control system networks.
9. Control systems command and control data not authenticated.
10. Inadequately managed, designed, or implemented critical support infrastructure.

In the report, NERC and the U.S. Department of Energy issued a set of recommended "foundational" (minimal), "intermediate" (next steps), and "advanced" (long-term) mitigations for the 10 vulnerabilities. Their recommendations include the following:

- Document and implement a cyber security policy that represents management's commitment and ability to secure its critical infrastructure assets. Periodically review and update.
- Ensure policies and procedures comprehensively include other parts of the enterprise, vendors, or contractors as appropriate.
- Implement strong procedural or technical controls at the access points to the electronic security perimeter to ensure authenticity of the accessing party, where feasible (e.g., restrict remote access to field devices).
- Implement physical security of network access points, including access control, or electronic methods for restricting access (e.g., MAC address filtering).
- Develop and implement policy for managing user and system access, including password policies.
- Change all default passwords where possible.
- Do not allow unauthenticated remote access to the control system.
- Use secure communication technology when the Internet is used for sensitive communications (e.g., VPN, SSH, SSL, IPSEC).
- External connections should be controlled and secured with an authentication method, firewall, or physical disconnection when not in use. This secure method should be established and monitored in accordance with the established security policy and procedures.

- Define levels of access based on roles or work requirements. Assign access level and unique identifiers for each operator. Isolate user access to compartmentalized areas based on specific user needs. Log system access at all levels.
- Use multifactor authentication (e.g., two-factor, non-re-playable credentials).
- Use proximity based authentication technology, such as RFID Tokens.
- Revoke authorization rights and access privileges of users upon termination or transfer.
- Remove, disable or rename administrator, shared and other generic account privileges including factory default accounts where possible.
- Establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity.
- Automate removal of user accounts tied to badge systems or human resources upon employee termination.
- Limit physical and electronic access to devices based upon organizational roles.

Identity management to the rescue.

Many of these recommendations are based on the following key IT security concepts:

- **Identity management**: the establishment and enforcement of policies to reliably verify the identity of each user accessing IT resources;
- **Access management**: the establishment and enforcement of policies that govern how users may be permitted to gain access to IT resources;
- **Strong authentication**: a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network; and
- **Security auditing**: a systematic, measurable technical assessment of how an organization's security policy is employed at a specific site.

An organization that employs identity management, access management, strong authentication, and security auditing is better equipped to: identify system users; govern how each user accesses IT resources; keep user identity information confidential; and prove that security policies are in place and enforced.

All of the mitigation steps outlined above further the CIP compliance effort, and many of them require the use of technology products. However, technology alone cannot achieve regulatory compliance. It is equally vital that the people leading the CIP compliance effort clearly define policies and controls, and follow the procedures to execute these controls. Technology's role is to support policies and automate processes, making it easier to establish and maintain compliance without putting an onerous burden on IT staff and users.

This is where Imprivata OneSign comes in. Each of the above threat mitigation recommendations can be affordably implemented with the support of OneSign solutions------often within a matter of weeks, at minimal cost, and with minimal impact on operations and user productivity. The OneSign platform gives organizations of all sizes the ability to substantially strengthen the protection of their critical assets, and in doing so, fulfill many of the CIP requirements within compliance deadlines.

HOW ONESIGN SUPPORTS CIP COMPLIANCE

OneSign, Imprivata's Converged Identity and Access Management Platform, offers solutions that can play a prominent role in supporting CIP compliance and further strengthening overall IT and physical security:

- ***Imprivata OneSign Authentication Management*** increases network security and simplifies the cost and complexity of network authentication management by replacing the Windows login with a broad range of strong authentication device options. These options include integrated management of One-Time-Password (OTP) tokens, finger biometrics, smartcards, and building access cards. Imprivata OneSign can mix and match these various authentication modalities to provide greater employee access security through flexible user authentication management, whether accessed through the network locally, via remote VPN, or while working offline. The industry's most powerful and innovative identity and access management appliance also delivers options for a seamless upgrade to Single Sign-On and/or integrated Physical/Logical capabilities.

- ***Imprivata OneSign Single Sign-On (SSO***) quickly and effectively solves password management and employee application access issues. Its breakthrough technology helps organizations benefit from increased user productivity and reduced password management costs by enabling single sign-on to all enterprise applications--- legacy, client/server, JAVA and Web. OneSign SSO does not require any custom scripting, changes to existing directories, or inconvenient end-user workflow changes. Companies benefit through centralized password administration, lower help-desk costs, increased user productivity and satisfaction, and ability to demonstrate compliance. With integrated support for multiple, strong authentication methods and centralized password policies, it allows companies to implement levels of security that are appropriate for their environments. Additionally, OneSign SSO's robust reporting capability can track login history of all users to each application, furthering the compliance tracking effort.
- ***Imprivata OneSign Physical/Logical*** integrates building and network access systems for unified enterprise security management. OneSign makes physical/logical security that's simplified, streamlined yet powerful. Beyond simply leveraging the building access badge, OneSign Physical/Logical consolidates identities between physical access systems and IT directories to enable creation and deployment of a single, converged security policy for allowing or denying network or remote access based on a user's physical location, user role, and/or employee status. OneSign delivers physical/logical security that satisfies complex business requirements. For the first time, events from physical security access systems can now be incorporated into network access decisions, providing a finer layer of authentication for closing security gaps, and providing organizations with broader monitoring and reporting capabilities in order to better demonstrate regulatory compliance.

For a more in-depth overview, the table below outlines many of NERC's "Top 10 Vulnerabilities", along with the related CIP requirement(s), and the role OneSign solutions can play in mitigating key control system vulnerabilities and supporting CIP compliance.

Vulnerability & Mitigation Strategies		**How OneSign Helps Meet the Standards**
1. Inadequate policies, procedures, and culture that govern control system security.		
Foundational Mitigation Strategy:		
CIP-003-1 R1 ***CIP-004-1 R3*** ***CIP-006-1 R1*** ***CIP-007-1 R1*** ***CIP-007-1 R8***	Document and implement a cyber security policy that represents management's commitment and ability to secure its critical infrastructure assets. Periodically review and update.	OneSign products require little or no change in staff work habits and preferences, making it easy for users to fully comply with even stringent policies and procedures. OneSign provides the means to define, enforce and confirm (through auditing) the application of policies.

Vulnerability & Mitigation Strategies		How OneSign Helps Meet the Standards
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms.		
Foundational Mitigation Strategy:		
CIP-003-1 R5 ***CIP-005-1 R2***	Implement strong procedural or technical controls at the access points to the electronic security perimeter to ensure authenticity of the accessing party.	OneSign controls the critical choke points that determine whether users are granted or denied access to resources. These are at the network logon, remote access authentication (through Radius) and applications (through SSO). Users cannot access the network or application unless they have the proper authorization credentials, based on the user's identity and role within the organization.
Advanced Mitigation Strategies:		
CIP-005-1 R3 ***CIP-006-1 R1***	Implement physical security of the network access points, including access control, or electronic methods for restricting access.	OneSign also offers support for strong multifactor authentication, including: OTP tokens, proximity cards (active or passive), smart cards, USB tokens and finger biometrics as well as integration with physical access systems to correlate network access with presence in the facility.

3. Remote access to the control system without appropriate access control.		
Foundational Mitigation Strategies		
CIP-003-1 R5 ***CIP-004-1 R4*** ***CIP-007-1 R5***	Develop and implement a policy for managing user and system access, including password policies	OneSign provides a powerful set of policies to manage passwords and/or stronger forms of authentication into the network and for OneSign-enabled applications. Auditing permits detailed verification that policies are being applied and enforced.
CIP-007-1 R5	Change all default passwords where possible	Default passwords can be disabled or changed on production systems before putting a system into production. Afterwards, a policy can be set to automatically change passwords behind the scenes at regular intervals, based on the requirements of each application. Password sharing reports can be used for SSO-enabled applications to find accounts where the same logon credentials are being used.
CIP-005-1 R1	Do not allow unauthenticated remote access to the control system	OneSign supports strong authentication using OTP tokens for remote access through either IpSec or SSL VPN and audit their use through the built-in Radius server.

Vulnerability & Mitigation Strategies		How OneSign Helps Meet the Standards
CIP-007-1 R5	External connections should be controlled and secured with an authentication method, firewall, or physical disconnection when not in use.	OneSign Physical/Logical can interlock remote network connections through IpSec or SSL VPN with the user's location and badge status. The remote access policy for a user can disable VPN use while the user is in the building and logged onto the network. OneSign contains an embedded RADIUS server for use with VASCO Digipass tokens, and can optionally redirect authentication requests to 3rd-party networked RSA SecurID or Secure Computing SafeWord authentication servers.
CIP-007-1 R4	Use secure communication technology when the Internet is used for sensitive communications (VPN, SSH, SSL, IPSEC).	User credentials are encrypted on the workstation and securely transmitted between remote OneSign users and the OneSign Server using SSL and AES encryption.
Intermediate Mitigation Strategies:		
CIP-007-1 R5	Define levels of access based on roles or work requirements. Assign access level and unique identifiers for each operator. Isolate user access to compartmentalized areas based on specific user needs.	Users cannot access the network or application unless they have the proper authorization credentials. OneSign's user policy features can assign capabilities based on users, their roles, group affiliation or on a per machine basis. OneSign can also assign multiple levels of access and control to a hierarchy of OneSign administrators for so that each subordinate administrator has fewer administrative rights than his/her superior.
Advanced Mitigation Strategies		
CIP-004-1 R4	Automate removal of user accounts tied to badge systems or human resources upon employee termination.	OneSign Physical/Logical works together with building access security to enforce location or zone-based access to networks and applications. Upon employee termination, a user's physical and network access can be shut off simultaneously by invalidating the user's physical access card. This automated interlock is keyed off the user's badge status and triggers an instant lockout of the account once facility access is terminated.
CIP-007-1 R5	Limit user accounts with administrator or root privileges when practical; limit shared accounts to the extent practicable, except when necessary for safety or operational considerations.	A shared usage log report can be run to better understand if users are sharing credentials for access to SSO-enabled applications.

Vulnerability & Mitigation Strategies		How OneSign Helps Meet the Standards
5. Use of inadeqately secured WiFi wireless communication for control.		
Foundational Mitigation Strategies:		
CIP-005-1 R3 ***CIP-007-1 R5***	Treat all wireless connections as remote access points. Document and implement a program for managing access to sensitive systems.	OneSign supports remote access via secure SSL/ VPN connection to a RADIUS server. OneSign contains an embedded RADIUS server (for VASCO Digipass tokens) or can redirect to third-party authentication servers from RSA or Secure Computing.

7. Insufficient application of tools to detect ad report on anomalous or inappropriate activity.		
Foundational Mitigation Strategies:		
CIP-006-1 R4	Regularly audit system logs, when available. Timestamp system logs for event correlation. Preserve system logs for subsequent analysis.	OneSign provides full auditing and reporting capabilities and stores network, remote and application event data in its own database. This enables organizations to perform detailed access audits, automatically generate reports, and export event logs for event correlation.

8. Unauthorized or inappropriate applications or devices on control system networks.		
Foundational Mitigation Strategies:		
CIP-005-1 R3	Establish policy/procedures to implement strong controls at the access points into the control system for all devices to ensure authenticity of the accessing party.	OneSign administrators can enable or disable users, or apply an appropriate OneSign user security policy, which includes defining policies around user authentication (including biometrics), SSO session management, password self-services, and access policy.
CIP-007-1 R5	Limit physical and electronic access to devices based upon organizational roles.	Users can be assigned individual policy settings based on role or group affiliation as well as location within the building.

Vulnerability & Mitigation Strategies		How OneSign Helps Meet the Standards
9. Control systems command and control data not authenticated.		
Foundational Mitigation Strategy:		
	Use control system protocols that contain appropriate authentication and integrity attributes without affecting performance as the technology becomes available.	OneSign ProveID provides a standards-based API that can be used by third-party applications to confirm user identity within a transaction or to reinforce authentication within existing applications. The same strong authentication means (biometrics, password, token, smartcards) used to enforce network access can be applied to specific command and control applications.

10. Inadequately managed, designed, or implemented critical support infrastructure.		
Foundational Mitigation Strategy:		
CIP-002-1 R3 ***CIP-009-1 R4***	Include critical support infrastructure functionality in continuity of operational planning. Periodically exercise/test recovery plans.	OneSign supports business continuity by providing full failover and disaster recovery capabilities. Backups can be regularly scheduled. OneSign also can be run in a distributed and load-balanced manner.

BENEFITS BEYOND CIP COMPLIANCE

The Imprivata OneSign platform is a powerful tool in the effort to achieve CIP compliance, but its value goes well beyond that one area of concern. The added benefits of OneSign products include:

Simplified password administration.

With OneSign Single Sign-On, administrators can implement a straightforward password policy across all applications based on users' primary authentication. To increase password security, OneSign can cycle application passwords behind the scenes and disable any user with a single mouse-click.

Reduced helpdesk costs.

When users have multiple application passwords to remember, they often forget them--- leading them to call their IT helpdesks for assistance. According to industry analysts, more than 30% of helpdesk calls are password-related. With a single helpdesk call costing an estimated $25*, the annual cost of password problems can be considerable. OneSign can reduce the number of helpdesk calls and the resource costs associated with them.

Increased user productivity.

With OneSign Single Sign-On and OneSign Authentication Management, users can gain more immediate access to the applications they need to do their work, and spend less time tracking down forgotten passwords.

* Source: Meta Group

MEETING THE CIP CHALLENGE

With its detailed requirements, lack of best practices and looming deadlines, CIP compliance remains a formidable challenge for the entire energy industry. However, it also represents an opportunity for companies to gain greater control over their critical assets and facilities, to ensure policies and procedures are in place and followed, and to improve service reliability for their customers. Imprivata's identity and access management solutions can be essential components in achieving, maintaining and demonstrating CIP compliance, and in helping to ensure the safety and reliability of an energy company's critical infrastructure.

For more details on Imprivata's Converged Identity and Access Management Platform - OneSign, please visit: http://www.imprivata.com or contact Imprivata at 1 877 ONESIGN.

To learn more about the CIP standards, please visit: http://www.nerc.com.

imprivata®

Offices In:
Belgium • Germany
Italy • Singapore
UK • USA

1 877 ONESIGN
1 781 674 2700
www.imprivata.com