

An Oracle White Paper
April 2010

Protecting the Electric Grid in a Dangerous World

Introduction	1
Changing Threats in a Changing Industry.....	3
Danger Signals.....	3
The Federal Response.....	4
How Oracle Addresses NERC CIP Requirements.....	5
A Closer Look at the Requirements	8
Role and Attribute-Based Access	8
Role-Based Access Control	9
Build Protection around Digital Assets	10
Establish Centralized Access Control	13
Enforce User Provisioning Policies and Workflows.....	15
Conclusion	17

Introduction

Now required by Federal Energy Regulatory Commission (FERC), the NERC CIP standards mandate sweeping security programs for North America's electricity industry. Oracle's Security and Identity Management solutions empower bulk power companies to implement enterprise-wide change. North America's power suppliers and distributors are under intense pressure to protect the bulk electric system (BES). The widespread use of standard computing platforms and systems linked to the Internet exposes the electric grid to new risks of internal and external compromise and potential disruption that did not exist even a short decade ago.

The industry's efforts at self-regulation notwithstanding, the federal government has responded to this threat with a set of security standards for protecting cyber assets that comprise the BES, and set an aggressive schedule for mandatory compliance, beginning in 2007, with all covered entities required to be in "audit compliance" by June 2010. Non-compliance could cost power companies up to \$1 million per day in penalties.

The North American Energy Reliability Corporation (NERC) Critical Infrastructure Protection (NERC CIP) cyber security standards, mandated through the approval of the Federal Energy Regulatory Commission (FERC), provide a broad, though not very prescriptive guide to implement a comprehensive cyber security program, stressing responsibility and accountability for protecting the organization's critical assets.

The need for these mandated standards is clear in a world where the business of managing BES infrastructure and delivering electrical power depends increasingly on instantaneous global connectivity between suppliers, distributors, partners and

customers. The very changes that have enabled the business of supplying power to flourish have opened potential threats few would have imagined not long ago.

Among other requirements, this environment calls for pervasive and highly manageable identity management to ensure secure access to the appropriate assets with the appropriate level of authorization, and a data protection program to prevent the theft and misuse of critical information.

At their heart, these programs are about policy, process and people. The challenge is to implement and manage them, with thousands or millions of users -- from high-privilege administrators to business partners -- myriad commercial, proprietary and legacy applications and hundreds or thousands of data repositories, without taxing limited resources and impacting the business of reliable delivery of electricity.

Oracle's security solutions, in the areas of identity management and database security, offer an effective, defense-in-depth security strategy to help meet this challenge, playing a key role in NERC CIP compliance, security and efficient use of resources.

Changing Threats in a Changing Industry

There is mounting evidence that North America's bulk power systems are dangerously exposed to threats from both within and abroad. The root of this exposure is in the shift from closed, proprietary control systems to increasing dependence on modern, standard platforms and applications. Driven by cost considerations and competition, utilities are adopting standard IP-based network technologies to tie into control systems, such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS), for efficient management and communication across main stations and remote locations.

Web-based portals and applications are essential to business, but open up electricity suppliers to the same sorts of attacks that can plague financial institutions, online retailers and, increasingly, healthcare providers. Central control stations are relying more and more on standard Windows and Linux systems and the requisite security imperatives, from server hardening to timely patching.

Adoption of "smart grid" technology, driven, in part by \$4.5 billion earmarked in the Obama administration's economic stimulus package, raises additional concerns over security. The smart grid will link most of the country's power grid to the Internet, and there is concern about hacking "smart meters" and grid management software.

Danger Signals

Here are a few of the warning signs of BES vulnerability:

- In June 2007, the Department of Homeland Security (DHS) leaked a video that showed how researchers launched a simulated attack that brought down a diesel electrical generator, leaving it coughing in a cloud of smoke, through a remote hack that was dubbed the Aurora vulnerability.
- In January 2008, a CIA analyst revealed that a number of cyber attacks had cut power to several cities outside the U.S.
- In May 2008, the Government Accountability Office (GAO) issued a scathing report on the number of security vulnerabilities at the Tennessee Valley Authority, the nation's largest public power company.
- In April 2009, *The Wall Street Journal* reported, according to unnamed current and former national security officials, that Russian and Chinese attackers penetrated the U.S. power grid, installing malware that could potentially be used to disrupt delivery.
- In July 2009, NERC CSO Michael Assante told the House subcommittee on Emerging Threats, Cyber security, and Science and Technology, "Cyber threats to control systems are

still evolving and are not yet fully understood. The potential for an intelligent attacker to exploit a common vulnerability that impacts many assets at once, and from a distance, is one of the most concerning aspects of this challenge.” Industry officials are particularly concerned that this type of attack would compromise the grid’s ability to compensate for failures in particular systems.

- In January 2010, a report by the Center for Strategic and International Studies said that SCADA systems are being attacked. The report, based largely on a survey of 600 IT and security critical infrastructure executives in 14 countries, said that, in many cases, security issues around the connection of SCADA systems to IP networks and the Internet weren’t being properly addressed.

The Federal Response

In this environment, once-closed control systems require comprehensive information security programs, with well defined policies and processes supported by appropriate tools. Accordingly, FERC mandated use of the once-voluntary NERC CIP standards across the electric power industry. Utilities are now accountable for the cyber security of their operations.

In brief, the eight security standards require:

- Identification and documentation of the critical cyber assets associated with the critical assets that support the reliable operation of the BES. (CIP-002)
- Minimum security management controls in place to protect critical cyber assets. (CIP-003).
- An appropriate level of personnel risk assessment, training, and security awareness for personnel having authorized cyber or unescorted physical access to critical cyber assets, including contractors and service vendors. (CIP-004)
- 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. (CIP-005)
- Implementation of a physical security program for the protection of critical cyber assets. (CIP-006)
- Defined methods, processes, and procedures for securing those systems determined to be critical cyber Assets, as well as the non-critical cyber assets within the electronic security perimeters. (CIP-007)
- Identification, classification, response, and reporting of cyber security incidents related to critical cyber assets. (CIP-008)
- Recovery plans for critical cyber assets that follow established business continuity and disaster recovery techniques and practices. (CIP-009)

How Oracle Addresses NERC CIP Requirements

Oracle’s Security and Identity Management products provide a complete single vendor defense-in-depth security solution that can address a broad set of requirements.

Oracle Access Manager, Oracle Identity Manager, Oracle Identity Analytics and other products in the suite of Oracle Identity Management solutions provides application and system-level security, giving power providers and distributors the tools to create sustainable, manageable and auditable controls over access to their critical assets. Identity management and access control are essential components in CIP-003, CIP-004, -005, -006, -007, and are applicable in -008, -009.

Oracle’s comprehensive data security portfolio, including Oracle Advanced Security, Oracle Data Masking, Oracle Database Vault, Oracle Label Security and Oracle Audit Vault, allow managing critical information throughout the data protection lifecycle by providing transparent data encryption, masking, privileged user and multi-factor access control, as well as continuous monitoring of database activity. Database security, especially data access controls and privileged user management are essential in CIP--003, -004, -005, -006, -007, -008 and -009.

Table 1 shows in detail how Oracle’s Security and Identity Management products help electrical utilities meet NERC CIP standards.

TABLE 1. ORACLE PRODUCT SUPPORT FOR NERC CIP COMPLIANCE

CIP STANDARD	ORACLE SOLUTION MAPPING
<p>CIP-003 Security Management Controls Requires that security management controls in place to protect critical cyber assets.</p>	<p>Oracle Access Manager provides policy-based authentication and authorization governed by a policy domain that specifies rules for protection. Policy Manager enables configuring resources to be protected and managing access policies.</p> <p>Oracle Identity Manager and Role Manager provide automated provisioning, using role and attribute-based policies tailored to corporate requirements.</p>
<p>R4. Implement and document a program to identify, classify, and protect information associated with critical cyber assets.</p>	<p>Oracle's identity management products empower utilities to manage role- based enterprise-wide authorization and authentication around critical assets.</p> <p>Oracle Advanced Security encrypts data at rest and in motion.</p> <p>Oracle Data Masking replaces sensitive information, such as credit card numbers with faux values in the same format.</p> <p>Oracle Database Vault provides privileged user access control and enforces separation of duties.</p>

<p>R4.2 Classify information to be protected based on the sensitivity of the asset.</p>	<p>Oracle Label Security enables data classification by assigning a data label to each row in an application table and mediates access based on the security clearance of the database or application user.</p>
<p>R4.3 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</p>	<p>Oracle Identity Manager polices resources under its management, detecting unauthorized accounts or changes to user access privileges.</p> <p>Oracle Access Manager and Identity Manager log all significant authorization, authentication and provisioning information for assessment, reporting and audit.</p> <p>Oracle Audit Vault provides audit assessment reports covering privileged users, account management, roles and privileges, and object and system management.</p>
<p>R5 Document and implement a program for managing access to protected critical cyber asset information.</p>	<p>Oracle Identity Manager, Role Manager and Access Manager provide highly granular, customizable enterprise-wide automated access control and role- and attribute-based user and system provisioning.</p> <p>Oracle Database Vault provides strong privileged user access control, preventing administrator's whose job is to keep systems running from having access to sensitive application data.</p>
<p>R6 Establish a process of change control and configuration management.</p>	<p>Oracle Configuration Management provides central database configuration management to detect configuration drift or unauthorized changes</p>
<p>CIP-004 Personnel and Training Requires an appropriate level of personnel risk assessment, training, and security awareness.</p>	
<p>R4 Maintain lists 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.</p>	<p>Oracle Access Manager and Identity Manager provide detailed information via console and reports on each user's access privileges to critical assets. Database Vault provides information on privileged user access.</p>
<p>R4.1 Review the lists of its personnel who have such access to critical cyber assets quarterly, and update the lists 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.</p>	<p>Oracle Identity Management products provide updates on changes in personnel and/or access rights on demand and in reports generated through logged information.</p>
<p>R4.2 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 access.</p>	<p>Oracle Identity Manager assures that terminated personnel and access privileges are de-provisioned throughout all managed systems.</p>
<p>CIP-005 Electronic Security Perimeters Identification and protection of the electronic security perimeters.</p>	

<p>R2 Implement and document processes and mechanisms to control electronic access to the security perimeters.</p>	<p>Oracle Access Manager gives organizations the means to implement policy-based authorization and mandate authentication mechanisms. Identity Manager and Role Manager provision users for appropriate access.</p>
<p>R2.4 Implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party.</p>	<p>Oracle Access Manager establishes and enforces authentication based on user/password, forms, X.509 certificates, smart cards, tokens, and biometrics.</p>
<p>R2.5 Required documentation shall identify and describe the processes for access request and authorization; authentication methods and the review process for authorization rights.</p>	<p>Oracle Identity Manager enables and request/approval/verification workflow for user and system provisioning based on roles and provides historical and current provisioning data for compliance reporting. Oracle Access Manager enables authorization and authentication policy and management, and logs report information based on accounts, authorization, authentication and access activity, including access testing, identity history and users created and deleted.</p>
<p>R3 Implement and document electronic or manual processes for monitoring and logging access at access points..</p>	<p>Oracle Access Manager provides monitoring, logging and reporting on account and user activity.</p> <p>Oracle Identity Manager detects rogue accounts and changes in user authorization.</p>
<p>CIP-006 Physical Security Ensure the implementation of a physical security program for the protection of critical cyber assets</p>	<p>Oracle Access Manager and Identity Manager manage user and system provisioning, authorization and authentication methods for physical as well as logical access control, supporting convergent authentication technologies, such as smart cards and biometrics, and integrating with physical control systems.</p>
<p>CIP-007 Security Systems Management Define methods, processes, and procedures for securing critical cyber assets.</p>	
<p>R5 Establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and minimize the risk of unauthorized access.</p>	<p>Oracle Access Manager sets and enforces policy-based authentication and monitors user access activity. Identity Manager detects rogue accounts and changes to user access privileges.</p> <p>Oracle Audit Vault and Oracle Database Vault tightly control access and monitor activity to databases.</p>
<p>R5.1 Ensure that individual and shared system accounts and authorized access permissions are based on need to know.</p>	<p>Oracle Identity Manager and Role Manager provision users and systems based on role and attribute.</p> <p>Oracle Database Vault enables separation of duties and access controls for privileged database users.</p>
<p>R6 Implement automated tools or process controls to monitor system security events.</p>	<p>Oracle Identity Manager detects unauthorized accounts or changes to user access privileges. Access Manager logs security related events.</p> <p>Oracle Audit Vault continuously monitors the inbound audit data,</p>

	evaluating information against alert conditions
CIP-008 Incident Reporting and Response Ensure the identification, classification, response, and reporting of security incidents	<p>Oracle Identity Manager and Access Manager monitor and log report information on user and resource accounts and authorization, authentication and access activity.</p> <p>Oracle Database Audit leverages Oracle's industry leading database security and data warehousing technology for managing, analyzing, storing, and archiving audit data for incident reporting, response and investigation.</p>
CIP-009 Recovery Plans Ensure that recovery plans are put in place for critical cyber assets	Oracle Role Manager helps to automating emergency access based on preconfigured business continuity models.
R4 Have processes and procedures for the backup and storage of information required to restore critical cyber assets	<p>Oracle Advanced Security in combination with Oracle RMAN enables secure backup to disk and swift recovery, enabling encrypted backup to disk or any other storage media.</p> <p>Oracle Secure Backup provides comprehensive secure backup management to tape for Oracle database files as well as non-Oracle database related operating system files. Oracle Secure Backup manages the encryption keys used to encrypt the data sent to tape. The Oracle Secure Backup Cloud module enables database backups to Amazon S3.</p>

Utility companies that incorporate best practices to control who has access to specified digital resources; properly define and enforce the level of authorization and appropriate authentication for those users, and build tight protection and access controls around the data itself, will successfully address the heart of the NERC CIP requirements and the essentials of a first-class security program.

A Closer Look at the Requirements

Role and Attribute-Based Access

As in any enterprise, people in large utility companies come and go. They change jobs within the organization. They may get added responsibilities or need short-term or long-term access to digital resources based on project assignments, new applications or databases, etc. Contractors, partners, and outsourcers all need special access.

Attaching rights to groups and then assigning users to the applicable group or groups is how authorization and authentication policies are generally administered. Assigning specific rights and privileges to individual users or creating additional groups is how exceptions are typically

handled. This approach is both inefficient, making it difficult to apply fine-grained controls based on shifting needs, and insecure, as it is all too easy to grant too much privilege by mistake - - or because it is simply easier -- allowing users to gain unauthorized access to critical assets.

The NERC CIP requirements for access control are not prescriptive; the standards don't tell utilities "how" to implement strong access control, but it makes clear that they must do it, and do it well. For example, CIP-003, which deals with security management, simply states, "The responsible entity shall document and implement a program for managing access to protected critical cyber asset information."

The key word is "protected." The purpose of NERC CIP is to protect the nation's critical infrastructure, and the expectation is that utilities will fulfill their responsibility. It's important to note that beyond the simple directive on access control comes strong wording regarding accountability. Companies have to identify each person responsible for granting logical and physical access and the information for which they are responsible.

And, CIP-007, which deals with securing cyber assets within security perimeters, states, "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."

Further, NERC CIP requires at least annual review to confirm that access privileges are correct and that they correspond with the company's needs and personnel roles and responsibilities.

In short, the directive carries an implicit expectation of best practice for access control and sets responsibility for it.

Similarly, end users should be restricted to handle only the data they need, and they're authorized only to perform operations they require to perform their duties.

Role-Based Access Control

Role-based access control (RBAC) has long been considered a superior approach for large, complex organizations. Roles are created for particular job functions and the necessary permissions defined for each role. Roles can then be assigned to individuals, making it easy to add or change responsibilities. Roles and combinations of roles can be as granular as required and assigned or revoked as required. Compare this to the somewhat cumbersome and error-prone process of assigning permissions to individuals or assigning individuals to groups that are either too general or "coarse" to be effective at a granular level or too bloated with permissions to be secure.

Privileged user roles should be defined with the principle of separation of duties (SOD) in mind, their actions limited by the role(s) to which they are assigned.

The problem for most organizations has been making the commitment of time and resources to define roles and establish a role-based approach across the enterprise according to business and

security requirements. This is a significant undertaking, requiring management support and buy-in and commitment from departments and business units across the enterprise.

Information about users, responsibilities and lines of reporting are typically in silos throughout the organization, and may not be particularly well organized even within those silos. The challenge is compounded when you consider partner and supplier information and relationships.

Oracle Solutions for RBAC

Oracle provides robust tools to help utility companies actualize and manage access controls around their applications, databases and systems.

Oracle identity and access management products reduce manual maintenance and audit costs, increasing business efficiency while improving security.

Oracle Identity Analytics provides policy-based role creation and automated role provisioning based on corporate information resources -- such as employee white pages, reporting structures and partner and customer information -- which can be consolidated and leveraged in a centralized repository. Identity Analytics enables organizations to use this data to model organizational structures and relationships, which form the basis for corporate role policy.

Identity Analytics is tightly integrated out of the box with Oracle Identity Manager to automate accurate user provisioning based on changes in role assignments (new hires, job changes, project assignments, etc.) or changes in business role and IT role mappings.

Build Protection around Digital Assets

Again, NERC CIP is not prescriptive in its directives. CIP-002 requires, in part, that “the responsible entity shall implement and document a program to identify, classify, and protect information associated with critical cyber assets.”

Thus, a strong data security plan is every bit as essential as user access control to protect critical information from intruders or malicious insiders who could use that information to plan potential attacks that could, in a worst case scenario, cause widespread disruption of the electric grid.

Many databases are critical assets with electric utilities. They back production systems, so a hacker could compromise them to cause outages. Any systems where the database affects running applications can be impacted. These are not just databases within control systems. With the widespread use of IP networks, standard operating systems and commercial applications, systems that were once closed to the world can be exposed through corporate and IT networks.

The data itself must be protected, particularly information identified in CIP-003: operational procedures, lists of critical assets, 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

Further, as in any type of organization typical business information such as financial databases, HR records and supply chain management must be protected.

In this environment, comprehensive data security is best practice, not paranoia.

Best Practices

Best practices for data security include:

- Critical asset identification and documentation, as called for in CIP-002.
- Data classification. CIP-002 explicitly requires “the responsible entity shall classify information to be protected under this program based on the sensitivity of the critical cyber asset information.
- Encryption of data at rest and in transit.
- Data masking to hide information, for example, in test and development environments.
- Separation of duties to define administrative roles according to need.
- Privileged user access control, closely tied to separation of duties, allows administrators only that access required to perform their jobs.
- Database access monitoring, alerting and reporting. CIP-005 and CIP-007, for example, require asset monitoring and alerting for incidents of unauthorized access.
- Change control and configuration management. (required by CIP-006)

Oracle Data Security Solutions

Oracle provides strong controls on privileged user access to application data. Privileged users have the ability to maintain the database, reflecting the minimum access required to do their jobs, but generally not be allowed to see or manipulate critical data or more importantly from a CIP perspective make unauthorized changes to critical applications through modification of application objects. Oracle’s defense-in-depth suite of data security solutions gives electric utilities the tools they need to implement and manage a best-performer data security program.

Defense-in-depth data security means looking at data security holistically. To do that, one needs to look at the entire life cycle of the data, where the data resides, what applications access the data, who is accessing the data and under what conditions, and ensuring that the systems have been properly configured and remain that way. Three key elements of this approach are Encryption and Data Masking, Access Control, and Monitoring.

Encryption and masking are important for protecting data outside the access control perimeter of the database. Data sitting on disk underneath the database and applications, data in test and development environments, data traveling over the network and data on backup media needs protection that only encryption and masking can offer. Discarded disk drives and the presence

of super users on the operating system leave open the possibility of unimpeded access to sensitive data that bypasses the authentication and access controls within the database. Movement of production data to other departments for testing and development purposes unnecessarily exposes sensitive data to individuals without a true “need-to-know”. Most certainly, data traveling over the wire is perhaps the most at risk of unauthorized access.

Access controls beyond the application level are now vital to enabling organization to achieve the benefits of data consolidation, off-shoring and cloud computing. Historically applications have been designed to scale to Internet requirements and provide role based functional access. Today, however, regulations and privacy laws require limited access to application data, even by the database administrator and especially from ad-hoc tools that can be used to bypass the application.

While encryption and access control are key components to protecting data, even the best security systems are not complete without a monitoring system in place. Just as video cameras supplement audible alarms in homes and businesses, monitoring provides the corresponding who, what and when that complements the encryption, masking and access control systems.

Oracle Database Vault

Oracle Database Vault provides strong privileged user access control, adding powerful controls within the database itself. Granular command rules define privileged user access based on a wide range of factors. Oracle Database Vault enables separation of duty to enforce a least privilege model on existing databases and protects data by placing it in “realms” to shield it from unauthorized privileged users. Command rules provide the ability to strictly control changes to applications, preventing adhoc modifications to applications.

Oracle Advanced Security

Oracle Advanced Security transparently encrypts data when written to disk and decrypts it after a user has been successfully authenticated and authorized. It supports both column and tablespace encryption. Transparent data encryption prevents attempts to bypass the database and access files directly. Oracle Advanced Security can provide SSL/TLS encryption to protect data going to and from the database, enforcing appropriate authentication according to corporate policy.

Oracle Data Masking

Oracle Data Masking replaces sensitive information, such as credit card numbers which can be replaced with faux values in the same format, allowing production data to be safely used for development, testing or sharing with partners.

Oracle Audit Vault

Oracle Audit Vault securely consolidates audit data generated by Oracle and non-Oracle databases into a secure central repository and provides audit assessment reports covering privileged users, account management, roles and privileges, object management and system management across the enterprise, monitors database transactions and issues alerts on suspicious activity.

Oracle Label Security

Oracle Label Security enables data classification by assigning a data label to each row in an application table. This goes beyond simple classification to data access control, by comparing the data label to the user label. Oracle Label Security integrates with Oracle Identity Manager for enterprise-wide management.

Establish Centralized Access Control

Effective access management requires centralized authentication, authorization, and auditing, so that access control can be maintained efficiently, according to policy, across the enterprise.

Think in terms of attempting to efficiently manage access control, authorization and appropriate authentication across an electric company's labyrinth of legacy and modern control and support systems, commercial and proprietary applications, critical database assets, business units, partner extranets, customer portals, etc.

- Establishing and administering authorization and authentication for each application and resource means fragmented management, disjointed policy and uneven security controls, and difficult user experiences that place additional burdens on IT resources.
- Determining, implementing and enforcing appropriate authentication levels, based on criticality of the assets are extremely difficult in this very common scenario.
- Database access control is often poorly defined and, in practice, poorly enforced. Privileged users often have access to production, personnel and/or customer information that has nothing to do with their jobs. Database access control policies and practices may vary from business unit to business unit, from department to department. Excessive access is granted because it is the easiest way to get things done.
- Producing auditable reports and proof of NERC CIP compliance that reflect some sort of systematic approach to compliance is problematic, at best. Preparing for audits and responding to auditor requests will be manual and error prone, and difficult to coordinate. Administrators have to collect and query access logs, for example, from diverse applications, *if* they are available.

In addition to the access control requirements previously described, CIP-007 requires that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.

Oracle Access Control Solutions

An access management system, such as Oracle Access Manager, secures access control through centralized authorization, authentication and audit, enabling single sign-on capabilities transparent to the user. It scales natively to bring centralized management to Oracle ERP, CRM and collaboration suite applications and provides out of the box integration and APIs to commercial and custom applications.

By separating authorization from the application, electric utilities can assign, manage and monitor access privileges on an enterprise-wide basis, according to business requirements, based on policies and rules that can be customized using Oracle Access Manager. Centralized authorization and authentication enhances security, as well as cutting costs, by freeing developers of the need to build this logic into each application.

CIP-007 also directs covered entities to “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.” Using *Access Manager*, electric utilities can implement the appropriate authentication based on asset criticality, including user ID and password, X.509 certificates, smart cards, two-factor tokens and forms-based authentication. They can establish hierarchies of authentication, so that users might need simple ID and password for an employee portal, but two-factor token authentication for an HR self-service application.

Centralized access management also helps with CIP-006 requirements for physical access security for controls that are managed, monitored and digitally logged. This is particularly useful for convergent digital and physical access technologies, such as smart cards and biometrics.

Oracle Access Manager is a powerful tool for security, operational, compliance reporting, as a wide range of information can be logged into Oracle or any relational database and exported to third-party reporting engines or further analyzed through Oracle Identity Analytics. Common audit reports include: authentication statistics (success/failed rates across all access servers), authorization statistics (success/failed rates across all access servers), failed authorizations (by user), failed authorizations (by resource), access testing, group history (all changes to all group profiles), identity history (by user), locked-out users, password changes, users created/deactivated/reactivated/deleted, user profile modification history (for all users), deactivated users report and workflow execution time.

Access to protected resources can be controlled based on user, group, role and attributes. As part of the Oracle Identity Management suite, Oracle Access Manager is used to best effect with Oracle Identity Manager and Oracle Identity Analytics. In addition, Oracle Identity Federation extends Oracle’s comprehensive identity management capabilities to partners, outsourcers, suppliers, customers etc.

Databases, arguably a utility’s most critical information assets, require dedicated, centrally managed access control reflecting enterprise policy based on the principle of least privilege.

Oracle Database Vault provides strong privileged user access control strengthening a utilities ability to comply with applicable NERC CIP requirements, using the concept of realms to create a firewall within the database. Sensitive tables or application can be placed in a “realm,” so privileged users can do their jobs without having access to sensitive data. So, for example, a DBA can perform his job without being able to see financial or privacy information in an application. Granular control rules employ multiple factors such as IP address, time of day and authentication method can be used in a flexible and adaptable manner to enforce access control. Database Vault also enables separation of duty to enforce a least privilege model on existing databases.

Enforce User Provisioning Policies and Workflows

Establish Clear Roles and Procedures

Sound security and compliance practice requires a policy-driven, clearly defined and auditable lifecycle management process for provisioning and de-provisioning user access privileges, not only for employees, but partners, outsourcers, suppliers, etc. to resources inside and outside the organization’s direct control. Granular entitlements should be based on both role- and attribute-based access controls, so that each user receives exactly the right level of authorized access, no more, no less. Granting too little access quickly becomes apparent: Managers and end users will let IT know quickly enough if restrictive controls are inhibiting business operations. Provisioning users with too much privilege will typically pass under the radar: They have what they need to do the job, and will, at best, ignore superfluous privilege, at worst abuse it.

In either case, poorly constructed user provisioning exposes the utility to potential security risk and manifests poor access control practices, which are likely to be an issue for NERC CIP audits. As cited above, accountability is a cornerstone of the standards. An inferior provisioning program puts department and line managers who are responsible for making and approving access and resource requests squarely between the crosshairs, along with the IT, security and business managers and administrators responsible for establishing roles and access policies.

An effective and secure user access provisioning program must rest on a foundation of carefully defined roles and attributes, so there is no room for interpretation. Atop this foundation should be a clearly established and thoroughly documented request, approval and verification workflow. Putting role-based approval in the hands of business managers assures that users will get access to the resources they require with minimal delay, while enforcing security and compliance by requiring that users and managers follow established policy and procedures. This workflow process also assigns responsibility and documents accountability. If the system is working, there should be no difficulty when someone asks, “Who authorized that?”

The key is to have business-efficient processes in place that enforce security policies and enable organizations to attest to NERC CIP requirements to have an access control program that can identify users and systems that have access to sensitive data.

Provisioning Pitfalls

In practice, user provisioning is often both inefficient and inaccurate in many organizations. Even if roles are well-defined and documented workflows are in place, the brunt of the work falls on overtaxed IT administrators and help desks. Users and managers may navigate around required procedures and administrators may take shortcuts around policy “just to get it done.” There are serious gaps between policy and practice, and utilities will be hard-pressed to demonstrate to auditors that users are actually assigned the correct authorizations.

As a result, poorly implemented identity management is also plagued by rogue or orphaned (sometimes called “ghost”) accounts, the result of out-of-process account creation and failure to quickly de-provision employees who have been terminated or have changed jobs within the organization, or, for example, contractors whose engagement has ended. These accounts present huge security risks, and, in fact, NERC CIP-004 requires that utilities revoke access to critical cyber assets for personnel terminated for cause within 24 hours and seven days for other personnel who no longer require access.

The gap between good intention and good execution is exacerbated by disparate, unconnected systems, data stores and applications across the enterprise, and no efficient way to centrally manage the request-approval-verification workflow among them. The result, again, is overtaxed resources, spotty policy compliance and weak accountability.

Oracle Identity Manager

Oracle Identity Manager plays a vital role by translating well-conceived provisioning policies into practical centrally managed and automated programs for smoother business operations, tighter security and auditable adherence to NERC CIP requirements. It allows administrators to set specified access levels to corporate resources to be provisioned. Utilities can employ both role- and attribute-based automated provisioning, best realized through its tight integration with Oracle Identity Analytics.

It supports separation of approval and provisioning workflow to follow best practices to efficiently manage corporate resources on the one hand, while automating IT provisioning tasks.

It provides a workflow “visualizer” that offers a graphical representation of workflow processes, allowing business users, IT administrators, and auditors to see and understand the process flow.

Oracle Identity Manager addresses the problem of connecting disparate systems, providing preconfigured connectors for the most popular commercial applications and interface technologies out of the box. This allows quick and scalable deployment in complex enterprises. In addition, Oracle’s Adapter Factory technology provides rapid integration to commercial or custom systems.

The reconciliation engine detects any unauthorized accounts or changes to user access privileges and takes corrective action, such as undoing the change or notifying an administrator. The

reconciliation engine also helps to detect and map existing accounts in target resources, enabling the creation of an enterprise-wide identity and access profile for each employee, partner or customer user. The reconciliation, in conjunction with access denial features and workflow controls allow organizations to detect and eliminate rogue and orphaned accounts.

Oracle Identity Manager provides historical and current provisioning data for compliance reporting, including user identity profile history, user group membership history, user resource access and entitlement history. This can be combined with the transaction data from workflow, policy, and reconciliation engines to address audit inquiries.

Conclusion

Bulk power companies are partners with the federal government in protecting North America's electric grid from potential disruption by malicious forces, given the motive and the means to attack our critical infrastructure.

The warning signs are clear that the bulk electric system is vulnerable hence the movement from voluntary to mandatory security controls. The NERC CIP standards will evolve as industry and government experts and auditors assess their breadth, depth and effectiveness, and translate the high-level guidelines into requirements for auditable compliance.

The industry recognizes the threat, and the goal, which is not compliance, but national security. Power suppliers and distributors are coming to grips with a new environment, in which closed, more secure control systems are exposed to the world -- in some cases, a hostile world.

Identity and access management and data security programs are about policy, process and people first, tools second. Tools are ineffective without the institutional will to effect change, and that change cannot be efficiently, practically implemented and managed without effective security products to help get the job done.

With its suites of integrated identity management and data security products, Oracle is a key member of the partnership for NERC CIP compliance and the security of the bulk power industry.



Protecting the Electric Grid in a Dangerous
World
April 2010
Author: Oracle

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com



| Oracle is committed to developing practices and products that help protect the environment

Copyright © 2010, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.