**CyberSoft VSTK-P Configuration for NERC STANDARD CIP-007-1 MAY 2, 2006 Standards**

**The North American Electric Reliability Corporation (NERC) is a federally sanctioned organization that sets and enforces standards for bulk power systems in the United States.**

**Quoting from their website of: www.nerc.com:**

**Since 1968, the North American Electric Reliability Corporation (NERC) has been committed to ensuring the reliability of the bulk power system in North America.**

To achieve that, NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast and winter and summer forecasts; monitors the bulk power system; and educates, trains, and certifies industry personnel. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada.

As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce reliability standards with all users, owners, and operators of the bulk power system in the United States, and made compliance with those standards mandatory and enforceable. Reliability standards are also mandatory and enforceable in Ontario and New Brunswick, and NERC is seeking to achieve comparable results in the other Canadian provinces. NERC will seek recognition in Mexico once the necessary legislation is adopted.

NERC is a non-government organization which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.

**The CyberSoft response to Standard CIP-007-1 resolves many requirements using the VSTK-P product. Additional open source products are suggested which may resolve other requirements. This report is made available at no charge.**

**Standard CIP–007–1 — Cyber Security — Systems Security Management**
**Adopted by Board of Trustees: May 2, 2006 Page 1 of 6**
**Effective Date: June 1, 2006**

**CyberSoft Operating Corporation has attempted to answer some of these requirements for computer security using our standard VSTK family of security tool kits. These answers are supplied in the color blue. Where we were not able to fulfill a requirement but found free software that could be used we provided answers in the color orange. Some of the URLs provided for free software are listed as starting places and not as a definitive answer.**

**CyberSoft is an expert in the field of computer security. While we do not advertise the fact that we can provide consulting, it is available to customers of our VSTK family of products. We feel that we can assist in the proper implementation of our products and specifically Unix computer security. In at least one case we where able to save the customer over one hundred thousand dollars per server by pointing out how to use our products to perform the same task as software they were purchasing in addition to our product. If you have an interest in these services please contact us.**

## A. Introduction

**1. Title:** Cyber Security — Systems Security Management
**2. Number:** CIP-007-1
**3. Purpose:** Standard CIP-007 requires Responsible Entities to define 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 Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

**4. Applicability:**
**4.1.** Within the text of Standard CIP-007, "Responsible Entity" shall mean:
**4.1.1** Reliability Coordinator.
**4.1.2** Balancing Authority.
**4.1.3** Interchange Authority.
**4.1.4** Transmission Service Provider.
**4.1.5** Transmission Owner.
**4.1.6** Transmission Operator.
**4.1.7** Generator Owner.
**4.1.8** Generator Operator.
**4.1.9** Load Serving Entity.
**4.1.10** NERC.
**4.1.11** Regional Reliability Organizations.
**4.2.** The following are exempt from Standard CIP-007:
**4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
**4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
**4.2.3** Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.
**5. Effective Date:** June 1, 2006
**B. Requirements**
The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

**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.

**General notes: This report discusses COTS products of the CyberSoft Operating Corporation (www.cybersoft.com). Specifically it discusses the VSTK and VSTK-P (VSTK Professional) products which are part of the VFind Security Tool Kit product line. Everything contained in the VSTK product is a subset of the VSTK-P which also includes the Avatar self healing tool.**

**Multiple third party certifying entities certifies the VSTK and VSTK-P products. In addition, they are listed as compliant to multiple government standards on government-managed lists. Finally, the products are fully Section 508 compliant for ADA.**

**Some additional white papers which may be of use in understanding these answers are:**

Use of the Avatar and CIT tools for Centralized Distribution and Control
**http://cybersoft.com/v3/whitepapers/paper_details.php?content=cs014**

Analysis of the VSTK/P product line in fulfilling US Federal Requirement DCID 6/3
**http://www.cybersoft.com/whitepapers/paper_details.php?id=52**

Secrets of the VFind Security Tool Kit Professional Plus
**http://cybersoft.com/v3/whitepapers/paper_details.php?content=cs005**

CyberSoft Support Center | Training (free training manuals)

**http://cybersoft.com/v3/support/training_index.php**

Script for CyberSoft CIT Training Video
http://cybersoft.com/v3/support/training_index.php

Script for CyberSoft VFind Training Video
http://cybersoft.com/v3/support/training_index.php

**R1.1.** The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

Use of the CyberSoft VSTK or VSTK-P computer security tool kits for Unix/Linux will insure that cyber security test procedures are implemented according to the authorized test plan. The primary tool for TEST RESULT ANALYSIS is the CIT tool. Use of the CIT tool prior to test plan implementation will insure the valididity of the system baseline test bed and use of the CIT tool after the implementation of the test plan will insure that the baseline system was maintained and that any changes to the system are in accordance with the authorized test plan.

**R1.2.** The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

Use of the CyberSoft CIT tool will identify all devation from the accepted baseline configuration including but not limited to identification of all files which were added to the system but are not part of the baseline configuration control standard, files which are part of the baseline and have been deleted and files which are part of the baseline but whose contents were modified.

Use of the CyberSoft Avatar tool will identify everything the CIT tool identifies in addition to ownership/group permissions and permission bit settings. The Avatar tool, if allowed, will automatically correct any changes from the approved baseline thereby insuring compliance with the accepted baseline configuration.

**R1.3.** The Responsible Entity shall document test results.

Documentation of the test results effect on the systems baseline configuation shall be automated by use of the CyberSoft CIT tool.

**R2.** Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

Live changes to the ports and services can be identified on systems by using standard command (Example: netstat http://en.wikipedia.org/wiki/Netstat) or (Example: Solaris 10 using “ps –ejawk” and “pfiles” http://www.computing.net/answers/solaris/open-ports-on-solaris-10/4811.html) to display actual ports and services in use to a file. Once this file has been MD5 hashed by the CIT tool any changes to the file contents will be identified which will then indicate a breach of the port or services baseline configuration by a stealthy attack such as started “by hand”. Any changes to the configuration files which would normally control the ports and services will be identified as a normal part of the CIT or Avatar operation.

Once a baseline configuration system has been created, a CIT or Avatar database will

identify any changes to the configuration. System reports which can identify the correct operation of the system (such as ports and services) can be made part of the configuration.

**R2.1.** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

Once this has been determined either the CIT or Avatar tools can identify any changes to the baseline. The Avatar tool can also repair unauthorized changes to the baseline.

**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).

Use of the CIT tool with a standardized CIT database which identifies the correct production baseline configuration will insure that this requirement has been complied with.

**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 or an acceptance of risk.

Once the compensation configuration management has been completed the CIT or Avatar programs can identify or correct any deviation from the standard.

**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 and document 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).

Once a patch has been certified as part of the approved baseline configuration it can be added to both the CIT and Avatar databases. CIT will then identify files which are no longer in compliance with the update approved baseline configuration on production systems. The Avatar system can also identify these files but will also apply the patches to the systems as part of maintaining the configuration baseline management process.

**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.

The CIT tool if executed every day can keep track of all changes made to the system baseline configuration on a daily basis. Review of the CIT reports or database can identify if patches and upgrades were made within the approved time period.

**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 or an acceptance of risk.

The CIT tool can automatically document the installation of all baseline configuration changes and by use of the MD5 hash code identify which patches/upgrades were installed on a system and when.

**R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus 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).

The VFind tool, which is a standard part of the VSTK and VSTK-P tool kits along with the UAD tool, will virus scan the entire system for malware. Use of the UAD tool insures that all files are correctly identified and if a compound file (.zip, .tar, etc…) or an encapsulated file (mime, uuencode, etc…) will drill down to the bottom layer to insure complete coverage. There are several options for mitigation including use of the Avatar tool to restore the infected file to it's uninfected state. OLE infections are mitigated using the MvFilter program (part of VSTK and VSTK-P). The MvFilter program is unusual in that it will not leave a ghost infection and it can also be used proactively to remove all macros from OLE documents.

There are several configuration options available for use of VFind, UAD, CIT, mitigation options and Avatar. All of these tools are fully scriptable in Bourne Shell, C-Shell, Korn Shell, Perl and other script like languages. Many options and standard configurations are delivered as tools with the VSTK product. Help with configuration of Bourne scripts to implement requirements is available at no charge.

**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 or an acceptance of risk.

Installation of the VSTK and VSTK-P tool kits are logged as a standard part of the installation process. In addition, once a CIT baseline configuration database includes these tools the CIT tool will report if they are not installed, were removed or tampered with. In addition, virus definitions are updated daily using SSL encryption over the network and are verified by use of both passwords and MD5 cryptographic hash codes. Virus definition updates are logged.

**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 installing the signatures.

The standardized and normal daily update of VSTK anti-virus and malware prevention signatures are automatically updated, verified and installed as part of a standard cron process. This is logged both by the VSTK update process and by cron.

**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.

The CIT tool can assist in this requirement.

Answers to many of the R5 requirements are operating system dependant. For example most the account/password requirements are functions of the operating system such as Sun Solaris. Other requirements are easy to fulfill by examination of the /etc/passwd and /etc/group files. Finally there are many audit tools available that can assist in this area. Some free ones are:

| Name | A URL where you can start |
|---|---|
| Satan/Sara | http://www.linux.com/archive/feed/51230 |
| Tiger | http://www.nongnu.org/tiger/ |
| Crack | http://www.cybersoft.com/cs_downloads/unix.php |
| COPS | http://www.cybersoft.com/cs_downloads/unix.php |

CyberSoft has the ability to assist in almost all computer security areas on a consulting basis. Please contact us if you want additional information in that area.

**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 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.

The CIT tool will provide detailed reports of everything that happens on the systems’ filesystem. This includes sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days. Please read the white paper, “Script for CyberSoft CIT Training Video” referenced above.

**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.

The CIT tool can be used to insure that the passwords were changes. If the /etc/passwd file is not shown as modified when the entry in the CIT database contains the unchanged passwords then a problem exists. It is noted that this operates only on a file basis and not on a password entry layer. A script can be created that will perform the same function at the account entry layer.

**R5.2.2.** The Responsible Entity shall identify those 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, as technically feasible:

**R5.3.1.** Each password shall be a minimum of six characters.

**R5.3.2.** Each password shall consist of a combination of alpha, numeric, and "special" characters.

**R5.3.3.** Each password shall be changed at least annually, or more frequently based on risk.

**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.

The VSTK tools such as CIT, UAD/VFind and Avatar can be used to implement automated tools to monitor system events at the file system layer that are related to cyber security.

**R6.1.** The Responsible Entity shall implement and document the organizational processes
and technical and procedural mechanisms for monitoring for 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.** Disposal or Redeployment — The Responsible Entity shall establish 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.

The use of the VSTK tools can aid in establishing formal methods, processes and procedures for disposal or redeployment of Cyber Assets.

**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.

The VFind tool can be used to insure that no key words are contained on the disk by reading the disk as a raw image. (Example; dd if=disk |vfind) While the filesystem may be destroyed that does not certify that the data no longer exists. Scaning of the raw disk will insure that no data can be read. Please read the document, “Script for CyberSoft VFind Training Video” referenced above.

**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.

The VFind tool can be used to insure that no key words are contained on the disk by reading the disk as a raw image. (Example; dd if=disk |vfind) While the filesystem may be destroyed that does not certify that the data no longer exists. Scaning of the raw disk will insure that no data can be read. Please read the document, “Script for CyberSoft VFind Training Video” referenced above.

**R7.3.** The Responsible Entity shall maintain records that such assets were disposed of or
redeployed in accordance with documented procedures.

**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 and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

**C. Measures**

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

**M1.** Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.

**M2.** Documentation as specified in Requirement R2.

**M3.** Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.

**M4.** Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.

**M5.** Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.

**M6.** Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.

**M7.** Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

**M8.** Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

**M9.** Documentation and records demonstrating the review and update as specified in Requirement R9.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Monitoring Responsibility

**1.1.1** Regional Reliability Organizations for Responsible Entities.
**1.1.2** NERC for Regional Reliability Organization.
**1.1.3** Third-party monitor without vested interest in the outcome for NERC.

#### 1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

#### 1.3. Data Retention

**1.3.1** The Responsible Entity shall keep all documentation and records from the previous full calendar year.
**1.3.2** The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.
**1.3.3** The compliance monitor shall keep audit records for three calendar years.

#### 1.4. Additional Compliance Information.

**1.4.1** Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.
**1.4.2** Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

### 2. Levels of Noncompliance

#### 2.1. Level 1:

**2.1.1** System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or
**2.1.2** One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,
**2.1.3** One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,
**2.1.4** Any one of:
• Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
• A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
• Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.



#### 2.2. Level 2:

**2.2.1** System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,

**2.2.2** Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

**2.3. Level 3:**

**2.3.1** System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,

**2.3.2** Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

**2.4. Level 4:**

**2.4.1** System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,

**2.4.2** Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

**2.4.3** No logs exist.

## E. Regional Differences

None identified.

## Version History

**Version Date Action Change Tracking**