

# Best Security Practices for SCADA Systems Utilizing the NERC Standard *matrix*



**ISS Solutions for Security Best Practices for Bulk Electric Systems  
Utilizing Standards Adopted by the North American Electric Reliability Council (NERC) -  
Urgent Action Standard 1200**

The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. For more information on NERC, please visit <http://www.nerc.com/>

*Source: NERC*

## Section 1201: Cyber Security Policy

1.1. The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall create and maintain a cyber security policy for the implementation of this standard.

1.2. The responsible entity shall assign a member of senior management with responsibility for leading and managing the entity's cyber security program. This person must authorize any deviation or exception from the requirements of this standard. Justification for any such deviation or exemption must be documented.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain its written cyber security policy stating the entity's commitment to protect critical cyber assets.</p> <p>2.2. The responsible entity shall review the cyber security policy at least annually.</p> <p>2.3. The current senior management official responsible for the cyber security program shall be identified by name, title, phone, address, and date of designation.</p> <p>2.4. The responsible entity shall maintain documentation justifying any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Collaborative Business Case Assessment</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Security Strategy Workshop</li> <li>• Documentation</li> </ul>

## Section 1202: Critical Security Assets

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify its critical cyber assets.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying critical cyber assets.</p> <p>2.2. The responsible entity shall review and update its critical cyber asset identification document at least annually or within 90 days of the addition or removal of any critical cyber assets.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul> <p><b>Proventia™ Integrated Security Appliances:</b>            Single, all-in-one protection for networks, servers and desktops combining:</p> <ul style="list-style-type: none"> <li>• Stateful Inspection Firewall</li> <li>• VPN</li> <li>• Antivirus</li> <li>• Intrusion Detection and Prevention</li> <li>• Content Filtering</li> <li>• Anti-spam</li> <li>• Application Protection</li> </ul>

## Section 1203: Electronic Security Perimeter

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify its electronic security perimeter(s).

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document depicting the electronic security perimeter(s), all interconnected critical cyber assets, and all electronic access points to the interconnected environment(s). The document shall verify that all critical cyber assets are within the electronic security perimeter(s).</p> <p>2.2. The responsible entity shall review and update its document referenced in 1203.2.1 at least annually or within 90 days of the modification of the network.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul> <p><b>Proventia</b></p>

## Section 1204: Electronic Access Controls

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying the access controls and their implementation for each electronic access point to the electronic security perimeter(s).</p> <p>2.2. The responsible entity shall review and update the documentation referenced in 1204.2.1 at least annually or within 90 days of the modification of the electronic security perimeter or the electronic access controls.</p>	<p>Assess Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul> <p><b>Managed Services</b></p> <ul style="list-style-type: none"> <li>• Managed Firewall Service</li> </ul> <p><b>Proventia</b></p>

## Section 1205: Physical Security Perimeter

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify its physical security perimeter(s) for the protection of critical cyber assets.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document depicting the physical security perimeter(s) and all physical access points to every such perimeter. The document shall verify that all critical cyber assets are within the physical security perimeter(s).</p> <p>2.2. The responsible entity shall review and update the document referenced in 1205.2.1 at least annually or within 90 days of the modification of the network.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul>

## Section 1206: Physical Access Controls

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify and implement physical access controls for access to critical cyber assets within the physical security perimeter(s).

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying the access controls and their implementation for each physical access point to the physical security perimeter(s).</p> <p>2.2. The responsible entity shall review and update the documentation referenced in 1206.2.1 at least annually or within 90 days of the modification of the physical security perimeter(s) or the physical access controls.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul>

## Section 1207: Personnel

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify all personnel, including contractors and service vendors, granted electronic or physical access to critical cyber assets.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeter(s).</p> <p>2.2. The responsible entity shall review the document referred to in 1207.2.1 at least quarterly and update the document within 24 hours of any change.</p> <p>2.3. The responsible entity shall conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul>

## Section 1208: Monitoring Physical Access

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall monitor physical access to critical cyber assets 24 hours a day, 7 days a week.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying its tools and procedures for physical access monitoring. This document shall verify that the tools and procedures are functioning and being used as planned.</p> <p>2.2. The responsible entity shall document physical access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights or controlled by video or other physical monitoring.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul>

## Section 1209: Monitoring Electronic Access

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall monitor electronic access to critical cyber assets, 24 hours a day, 7 days a week.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying electronic access monitoring tools and procedures. This document shall verify that the tools and procedures are functioning and being used as planned.</p> <p>2.2. The responsible entity shall document electronic access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights.</p>	<p>Assess</p> <p>Design</p> <p>Manage and Support</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul> <p><b>SiteProtector™</b></p> <p><b>Managed Services:</b></p> <ul style="list-style-type: none"> <li>• Managed Protection Services</li> <li>• Managed Firewall Service</li> <li>• Managed Intrusion Detection and Prevention Services</li> <li>• Vulnerability Management</li> <li>• Customer Portal</li> </ul>

## Section 1210: Information Protection

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall protect information associated with critical cyber assets and the policies and practices used to keep them secure.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying the access limitations to sensitive information related to critical cyber assets. At a minimum, this document must address access to procedures, critical asset inventories, maps, floor plans, equipment layouts and configurations.</p> <p>2.2. The responsible entity shall review and update the document referred to in 1210.2.1 as necessary and at least annually.</p>	<p>Deploy</p>	<p><b>Proventia</b></p> <p><b>SiteProtector™</b></p> <p><b>Managed Services:</b></p> <ul style="list-style-type: none"> <li>• Managed Protection Services</li> <li>• Managed Firewall Service</li> <li>• Managed Intrusion Detection and Prevention Services</li> <li>• Vulnerability Management</li> <li>• Customer Portal</li> </ul> <p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Incident Response Planning</li> <li>• Emergency Response Services</li> <li>• Security Strategy Workshop</li> </ul>

## Section 1211: Training

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall train personnel commensurate with their access to critical cyber assets. The training shall address, at a minimum: the cyber security policy, physical and electronic access controls to critical cyber assets, the release of critical cyber asset information, potential threat incident reporting, and action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Training shall be conducted upon initial employment and reviewed annually.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall develop and maintain a company-specific cyber security training program that includes, at a minimum, the following required items:</p> <p>2.1.1. The cyber security policy;</p> <p>2.1.2. Physical and electronic access controls to critical cyber assets;</p> <p>2.1.3. The release of critical cyber asset information;</p> <p>2.1.4. Potential threat incident reporting; and</p> <p>2.1.5. Action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.</p> <p>2.2. The responsible entity shall maintain a document identifying all personnel who have access to critical cyber assets and the date of the successful completion of their training.</p> <p>2.3. The responsible entity shall document that it has reviewed its training program at least annually.</p>	<p>Educate</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Security Awareness Program</li> </ul> <p><b>X-Force™ Education Services</b></p>

## Section 1212: Systems Management

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall establish systems management policies and procedures for configuring and securing critical cyber assets.

- 1.1. The use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment;
- 1.2. The authorization and periodic review of computer accounts and access rights;
- 1.3. The disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights;
- 1.4. The disabling of unused network services and ports;
- 1.5. Secure dial-up modem connections;
- 1.6. Firewall management;
- 1.7. Intrusion detection processes;
- 1.8. Security patch management;
- 1.9. The installation and update of anti-virus software;
- 1.10. The retention and review of operator logs, application logs, and intrusion detection logs; and
- 1.11. Identification of vulnerabilities and responses.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying system management policies and procedures.</p> <p>2.2. The responsible entity shall review and update the document referred to in 1212.2.1 as necessary and at least annually.</p> <p>2.3. The system management policies and procedures document shall address all items in requirement 1212.1.</p> <p>2.4. The responsible entity shall implement system management policies and procedures as described in the system management policies and procedures document.</p>	<p>Deploy</p> <p>Manage and Support</p>	<p><b>Proventia</b></p> <p><b>SiteProtector</b></p> <p><b>Managed Services:</b></p> <ul style="list-style-type: none"> <li>• Managed Protection Services</li> <li>• Managed Firewall Service</li> <li>• Managed Intrusion Detection and Prevention Services</li> <li>• Vulnerability Management</li> <li>• Customer Portal</li> </ul> <p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA systems</li> <li>• Gap Analysis</li> <li>• Security Awareness Program</li> <li>• Documentation</li> </ul>

**Section 1213: Test Procedures**

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall establish test procedures and acceptance criteria to ensure that critical cyber assets installed or modified comply with the security requirements in this standard. Test procedures shall require that testing and acceptance be conducted in an isolated test environment.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document identifying test and acceptance criteria for the installation or modification of critical cyber assets.</p> <p>2.2. The responsible entity shall maintain a document verifying that it has implemented the test and acceptance criteria.</p>	<p>Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA Systems</li> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Business Risk Assessment</li> <li>• Penetration Test</li> <li>• Incident Response Plan</li> <li>• Documentation</li> </ul>

## Section 1214: Electronic Response Incident Procedures

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall define electronic incident response actions, including roles and responsibilities assigned by individual or job function.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document defining the electronic incident response action, including actions, roles and responsibilities.</p> <p>2.2. The document in 1214.2.1 shall require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the <i>NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure</i>.</p>	<p>Assess</p> <p>Manage and Support</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA Systems</li> <li>• Security Awareness Program</li> <li>• Incident Response Planning</li> <li>• Emergency Response Services</li> <li>• Documentation</li> </ul> <p><b>Managed Services:</b></p> <ul style="list-style-type: none"> <li>• Managed Protection Services</li> <li>• Managed Firewall Service</li> <li>• Managed Intrusion Detection and Prevention Services</li> <li>• Vulnerability Management</li> <li>• Customer Portal</li> </ul>

## Section 1215: Physical Incident Response Actions

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall define physical incident response actions, including roles and responsibilities assigned by individual or job function.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document defining the physical incident response action, including actions, roles and responsibilities.</p> <p>2.2. The document in 1215.2.1 shall require that incidents involving physical assets used to protect critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the <i>NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure</i>.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA Systems</li> <li>• Security Awareness Program</li> <li>• Incident Response Planning</li> <li>• Emergency Response Services</li> <li>• Documentation</li> </ul>

## Section 1216: Recovery Plans

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall create action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Each responsible entity shall exercise these plans at least annually. The plans and procedures shall define roles and responsibilities by individual or job function.

Description	ISS Program Phases	ISS Solutions to Achieve NERC Compliance
<p>2.1. The responsible entity shall maintain a document defining the action plan and procedures used to recover or re-establish critical cyber assets following a cyber security event, including actions, roles and responsibilities.</p> <p>2.2. The responsible entity shall maintain a document verifying that the action plan is exercised via drill at least annually.</p>	<p>Assess and Design</p>	<p><b>Professional Security Services:</b></p> <ul style="list-style-type: none"> <li>• Policy and Procedures Design</li> <li>• Best Practices for SCADA Systems</li> <li>• Security Awareness Program</li> <li>• Incident Response Planning</li> <li>• Emergency Response Services</li> <li>• Documentation</li> </ul>

#### GLOBAL HEADQUARTERS

6303 Barfield Road  
Atlanta, GA 30328  
United States  
Phone: (404) 236 2600

#### REGIONAL HEADQUARTERS

##### **Australasia**

Internet Security Systems Pty Ltd.  
Level 6, 15 Astor Terrace  
Spring Hill Queensland 4000  
Australia  
Phone: +61 (0)7 3838 1555  
Fax: +61 (0)7 3832 4756  
e-mail: aus-info@iss.net  
Support e-mail: support@iss.net

##### **Asia Pacific**

Internet Security Systems K. K.  
JR Tokyu Meguro Bldg. 3-1-1  
Kami-Osaki, Shinagawa-ku  
Tokyo 141-0021  
Japan  
Phone: +81 (3) 5740-4050  
Fax: +81 (3) 5487-0711  
e-mail: sales@isskk.co.jp  
Support e-mail: support@isskk.co.jp

##### **Europe, Middle East and Africa**

Ringlaan 39 bus 5  
1853 Strombeek-Bever  
Belgium  
Phone: +32 (2) 479 67 97  
Fax: +32 (2) 479 75 18  
e-mail: isseur@iss.net

##### **Latin America**

6303 Barfield Road  
Atlanta, GA 30328  
United States  
Phone: 404 236 2790  
Fax: 404 236 2629  
e-mail: isslatam@iss.net