

Summary

Invensys has the products and the skills to meet all of your Cyber Security Compliance needs. Our products and security consultant teams can meet the changing NERC CIP requirements as well as those being driven by your internal organization.

Business Value

Invensys understands that the security of your control system and data is paramount to your organization. We can help you protect those assets in the most cost-effective manner to meet your business needs. We are able to supply strategies and software to meet industry requirements surrounding topics such as plant-wide patch management, change control, loggings services, access control and backup and recovery.

Invensys Cyber Security

CIP Compliance Services

INVENSYS CYBER SECURITY CONSULTING

Invensys Cyber Security Consulting has the resources, know-how, and implementation skills to assist a company in becoming CIP compliant. Our security experts will design a security solution specifically for your situation. Our team of professionals offers plantwide, platform independent solutions through a project-oriented or ongoing service delivery as well as master plan development and rollout.

BENEFITS

- Meet and maintain CIP compliance
- Reduced workload for the internal staff
- Lower and more predictable cost of implementation and maintenance
- Maximized reliability and uptime of control networks
- Enforced policy management and change control
- Skilled security practitioners
- Leverage pre-qualified Electronic Perimeter

CHALLENGES

In today's business environment, cyber security has become a key focus for all industries. Within the Power industry the Federal Energy Regulatory Commission (FERC) is adopting cyber security standards defined by the North American Electric Reliability Corporation (NERC) known as CIP-001 through CIP-009. Companies now face the challenge of becoming NERC compliant by the year 2010. This means having to learn the requirements, design and implement the policies and procedures, install additional equipment, and maintain all of it.



STAYING CURRENT – AND COMPLIANT

Invensys is committed to maintaining currency with regulatory standards, Cyber Security technology, evolving threats and solutions. Our solutions-oriented approach ensures that we consider YOUR needs in developing a solution that fits YOUR unique situation. As CIP regulations evolve, as other standards are implemented, and as Cyber Security protocols mature, Invensys will be there to develop solutions that work – for you.

OUR OFFERING

- **Hardware Independence** – we work with any vendor’s control system and any type of security technology.
- **Regulation Knowledge** – our subject matter experts understand not only CIP regulations, but other regulatory requirements as well. We actively participate in a number of industry and government groups.
- **Technical Knowledge** – our consultants are well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, network architecture, etc.
- **Industry Knowledge** – with more than 100 years experience, Invensys understands all aspects of the power industry.
- **Proven Methodology** – Invensys follows a proven methodology for implementing a cyber security solution, customized for your particular needs.

CIP-002 CRITICAL CYBER ASSET IDENTIFICATION STANDARD

- R1 Critical Asset Identification Method
- R2 Critical Asset Identification
- R3 Critical Cyber Asset Identification
- R4 Annual Review and Approval

ACHIEVE COMPLIANCE

- > Baseline the current methods for identifying critical assets and perform a gap analysis against a proven risk-based methodology to create a comprehensive identification methodology specific to the client’s needs.
- > Apply the identification methodology to requirements R2 and R3 to create a list of critical assets and critical cyber security assets.

MAINTAIN COMPLIANCE

- > Perform annual reviews of the methodology and the list to ensure they are accurate and continue to meet CIP requirements.

CIP-003 SECURITY MANAGEMENT CONTROLS STANDARD

- R1 Cyber Security Policy in Place
- R2 Leadership Assignments
- R3 Policy Exception Handling
- R4 Information Protection
- R5 Access Control
- R6 Change Control and Configuration Management

ACHIEVE COMPLIANCE

- > Review current policies and procedures and deliver a detailed report with current status and recommendations for improvement.
- > Together with the customer, create the appropriate policies and procedures that specify:
 - How the various networks and systems will be accessed, supported, maintained and updated
 - How the information about the cyber security assets will be classified, protected, and accessed
 - How change control and configuration management of the cyber security assets will be accomplished
- > Create the lists of information classified as protected and those who have access.
- > Recommend changes to electronic access that meet requirements R4, R5, and R6.

MAINTAIN COMPLIANCE

- > Perform annual reviews of the methodology and the list to ensure they are accurate and continue to meet CIP requirements.
- > Provide Managed Security Services to monitor all security related equipment and manage change and configurations.

CIP-004 PERSONNEL AND TRAINING

- R1 Awareness
- R2 Training
- R3 Personnel Risk Assessment
- R4 Access

ACHIEVE COMPLIANCE

- > Establish, maintain and document employee training and awareness programs.
- > Ensure all personnel with access to Cyber Assets are trained on security practices.
- > Create documented personnel risk assessment program for background checks that include at the very least Social Security Number verification and criminal check.
- > Documentation of cyber access privilege and physical access type for authorized personnel.

MAINTAIN COMPLIANCE

- > Maintain updated documentation for personnel for training, background checks, program reviews, and new hires.
- > Review documentation list and update documentation on cyber access privileges, physical access privileges and access revocation.

CIP-005 ELECTRONIC SECURITY PERIMETER(S) STANDARD

- R1 Establish Electronic Security Perimeter
- R2 Electronic Access Controls
- R3 Monitoring Electronic Access
- R4 Cyber Vulnerability Assessment
- R5 Documentation Review and Maintenance

ACHIEVE COMPLIANCE

- > Establish the electronic security perimeter based on the identification of critical cyber assets and analyze current access controls and monitoring capability.
- > Establish the appropriate policies for access and monitoring.
- > Perform a vulnerability assessment based on proven procedures. Procedures will be documented for CIP compliance.
- > Recommend design changes to the system that will 'harden' it from attacks using a layered approach known as defense in depth. This may include firewalls, Intrusion.
- > Detection / Prevention devices, DMZ, network architecture changes, etc.
- > Implement the design changes to the system.

MAINTAIN COMPLIANCE

- > Perform annual reviews of the security perimeter, access controls and access monitoring.
- > At a minimum, perform annual vulnerability assessments.
- > Provide Managed Security Services to monitor the perimeter on a 365 x 24 x 7 basis including access, intruder detection and prevention, system health, etc.
- > Remotely change system configuration based on new technologies or system health.

CIP-006 PHYSICAL SECURITY STANDARD

- R1 Physical Security Plan
- R2 Physical Access Controls
- R3 Monitor Physical Access
- R4 Logging Physical Access
- R5 Access Log Retention
- R6 Maintenance and Testing

ACHIEVE COMPLIANCE

- > Identify scope of critical assets within defined physical security perimeter.
- > Identify existing procedures, review and augment to ensure comprehensive documentation and procedures to monitor and record aspects of physical security.
- > Review, develop and recommend appropriate security controls.
- > Ensure capability and procedures exist for periodic testing and maintenance.

MAINTAIN COMPLIANCE

- > Perform annual reviews of security plan and procedures to ensure they are accurate and continue to meet CIP requirements.
- > Update security plan as appropriate to incorporate new technology and measures.

CIP-007 SYSTEMS SECURITY MANAGEMENT STANDARD

R1 Test Procedures
R2 Ports and Services
R3 Security Patch Mgmt
R4 Malicious Software Prevention
R5 Account Mgmt
R6 Security Status Monitoring
R7 Disposal or Redeployment
R8 Cyber Vulnerability Assessment
R9 Documentation Review and Maint

ACHIEVE COMPLIANCE

- > Assess the cyber assets within the perimeter and current methodologies used to test, upgrade, patch, etc.
- > From the assessment, create the appropriate policies for each asset type for maintaining and updating security.
- > Establish procedures to create procedures, documentation and logs for each subject area and ensure procedures are developed to monitor and maintain.

MAINTAIN COMPLIANCE

- > Perform annual reviews of the methodology and the lists to ensure they are accurate and continue to meet NERC requirements.
- > Provide Managed Security Services to monitor all security related equipment and manage change and configurations.

CIP-008 INCIDENT REPORTING AND RESPONSE PLANNING STANDARD

R1 Cyber Security Incident Response Plan
R2 Incident Documentation

ACHIEVE COMPLIANCE

- > Provide guidance and recommendation in both Incident reporting and response.
- > Develop & ensure strong Reporting Functionality and Response alerting.
- > Establish requirement within Cyber Security Policy for reporting and response planning.
- > Ensure procedures and ownership for Response testing and Validation.

MAINTAIN COMPLIANCE

- > Develop and recommend procedures to ensure that the Response Plan and documentation are reviewed annually and updated to remain current.

CIP-009 RECOVERY PLANS FOR CRITICAL CYBER ASSETS

R1 Recovery Plans
R2 Exercises
R3 Change Control
R4 Backup and Restore
R5 Testing Backup

ACHIEVE COMPLIANCE

- > Provide guidance and recommendation in developing a Recovery plan.
- > Establish requirement within Cyber Security Policy for a Recovery plan.
- > Ensure ownership and procedures exist to test the Recovery plan.

MAINTAIN COMPLIANCE

- > Develop and recommend procedures to ensure that the Recovery Plan and documentation are reviewed annually and updated to remain current.

INVENSYS ACTIVE GROUP PARTICIPATION

NIST National Institute of Standards
ISASP99 Control System Security
Technical reports and standard
MSMUG Microsoft Manufacturing User Group
DOE Department of Energy
DHS Department of Homeland Security
INL Idaho National Laboratory
CPNI Centre for Protection of National Infrastructure

ISCI ISA Security Compliance Institute
SANDIA Sandia National Laboratories
NERC North American Electric Reliability Corporation
IAEA International Atomic Energy Agency
U.S. NRC U.S. Nuclear Regulatory Commission
ICSJWG Industrial Control Systems Joint Working Group
I3P Institute for Information Infrastructure Protection
And more!



Invensys Operations Management • 5601 Granite Parkway III, #1000, Plano, TX 75024 • Tel: (469) 365-6400 • Fax: (469) 365-6401 • iom.invensys.com

Invensys, the Invensys logo, ArchestrA, Avantis, Eurotherm, Foxboro, IMServ, InFusion, SimSci-Esscor, Skelta, Triconex, and Wonderware are trademarks of Invensys plc, its subsidiaries or affiliates. All other brands and product names may be the trademarks or service marks of their representative owners.

© 2010 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by any information storage and retrieval system, without permission in writing from Invensys Systems, Inc.

Rev. 08/10 PN IN-0103