



The
**NERC CIP
Compliance
Guide**
3rd Edition

**Now including CIP-014, FERC Orders 791, 802,
and updates from the July 16, 2015 NOPR RM15-14-000**

Table of Contents

Introduction	5
Features	11
CIP-002-5.1 BES Cyber System Categorization	13
CIP-003-6 Security Management Controls	31
CIP-004-6 Personnel & Training	55
CIP-005-5 Electronic Security Perimeter(s)	81
CIP-006-6 Physical Security of BES Cyber Systems	93
CIP-007-6 Systems Security Management	117
CIP-008-5 Incident Reporting and Response Planning	151
CIP-009-6 Recovery Plans for BES Cyber Systems	166
CIP-010-2 Configuration Change Management and Vulnerability Testing	187
CIP-011-2 Information Protection	215
CIP-014-2 Physical Security	225
Appendix A: IRA and ICE	253
Appendix B: CRSI Definitions	255
Appendix C: CRSI Compliance Tips	263
Appendix D: Document Retention	267
Appendix E: SME Testimony Tips	269
Appendix F: Exemplars	273
Appendix G: References	279



Attachments: These are attachments or additional information from NERC outside of the Standards themselves but concerning a specific Standard.



Measures: These are the Measures included in the standard providing guidance on the types of evidence that can demonstrate compliance to the requirements.



Additional Supporting Evidence Guidance: This section provides additional guidance on what types of evidence can demonstrate compliance to the requirements.



Auditor Expectations: This is NERC guidance provided to the auditors as documented in the Reliability Standard Audit Worksheets (RSAWs).



NERC Guidelines and Technical Basis: This is the verbatim guidance provided by NERC and the standard Drafting Team. It provides insight, guidance and rationale to support the registered entities' understanding in the standard.



NERC Rationale: This section describes the reasoning that NERC used in formulating the Standards and Requirements in NERC's own words.



Problem Areas: These are concerns or deficiencies frequently identified by CRSI with respect to compliance to the specific requirement.

SAMPLE

CIP-002-5.1 R2: The Responsible Entity shall:

- R2.1:** Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and
- R2.2:** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

VRF: Lower/Time Horizon: Operations Planning



MEASURES

M2

Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.



ADDITIONAL SUPPORTING EVIDENCE GUIDANCE

- Effective change management will be key to an effective and efficient review of assets and BES Cyber Systems.
- Plan for sufficient review time to ensure completing annual reviews and obtaining approvals within the 15 month window. Sufficient review time should include time for investigation and resolution of any identified data discrepancies.



AUDITOR EXPECTATIONS

- Verify the reviews of the identifications in Requirement R1 have occurred at least once every 15 calendar months.
- Verify the approvals by the CIP Senior Manager or delegate of the identifications in Requirement R1 have occurred at least once every 15 calendar months.



NERC GUIDELINES AND TECHNICAL BASIS

NERC does not provide any Guidelines and Technical Basis specific to R2.

NERC CIP Compliance Guide Order Form

Ask about our "NERC CIP Compliance Guide User Listing" for additional order fields!

CRSI's NERC CIP Compliance Guide is the first ever, holistic, abridged "Go-to" source for all NERC CIP Compliance questions.

Expanding on FERC Orders 706 and 791, our new Guide provides insight into FERC Order 802 and the soon to be approved 'Version 6' changes. Our NERC CIP Compliance Guide references every NERC document published for guidance and the interpretation or application for each CIP Standard. Additionally, the Guide provides what documentation is needed per Requirement and Sub-Requirement and then details additional evidence that must be provided during an audit. Then, we provide best practice recommendations and problem areas to avoid that CRSI has identified from working with over 200 electric utility companies over the past 15 years. This guide was developed using Version 5 (FERC Order 791) of the CIP Standards, the July 16, 2015 FERC Notice of Proposed Rulemaking (NOPR), FERC Order 802 (CIP-014), and includes mapping charts for Version 5 to 6. Reliability Assurance Initiative (RAI) and FERC NOPR are addressed, as supplements within the Guide.

Who is the NERC CIP Compliance Guide for?

CRSI's NERC CIP Compliance Guide is designed for all members of your company. Those that will benefit the most from the Guide are Subject Matter Experts, members of your internal Compliance Team, Senior Executives, Management and employees dealing with NERC CIP on a daily basis. The Guide is designed as a stand-alone reference source for all NERC CIP compliance questions.

Quantity:	\$600 per book [<input type="checkbox"/> PDF / <input type="checkbox"/> Hardcopy]	Order Total: \$
Billing and Shipping Information		
Name and Company:		
Billing Address:		
City, State, ZIP:	Phone #:	
Shipping Address:	<input type="checkbox"/> Check if Same as Billing Address	
City, State, ZIP:		
Method of Payment		
<input type="checkbox"/> Check/ACH (include check with order)	<input type="checkbox"/> VISA	<input type="checkbox"/> MasterCard
Credit/Debit Card No.	Exp. Date	CVS#
Signature	Date	

Terms and Conditions

- A limited distribution agreement is provided with each sale as identified in the CRSI NERC CIP Compliance Guide. Beyond this limited distribution agreement, no transfer of intellectual property rights are made with the purchase.
- Purchases of the CRSI NERC CIP Compliance Guide Book are exclusive of any former, current, or future contract with CRSI for professional services.
- Payment via accepted payment processes is required at the time of order and in advance of product shipping and delivery, or access being granted to PDF versions of the Compliance Guide. Payment is in U.S. Dollars.
- This book is presented solely for educational and informational purposes. The author and publisher are not offering it as legal, accounting or other professional services advice. While best efforts have been used in preparing this book, it may contain errors, omissions or information that was accurate as of its publication but has subsequently become outdated. The author or publisher shall not be liable or responsible to any person or entity with respect to any loss or incidental or consequential damages caused, or alleged to have been caused, directly or indirectly, by the information contained herein.
- No warranty may be created or extended by sales representatives or written sales materials.
- The DRM for PDF guides expires every two years and must be renewed for continued access.
- Purchase of the CRSI NERC CIP Compliance Guide Book represents acceptance of these terms and conditions.

Signature _____

Date _____

Corporate Risk Solutions, Inc.
11900 W. 87th St Pkwy
Suite 120
Lenexa, KS 66215

CRSI Sales Department
Phone: 913-422-0410
Fax: 913-948-8364 Email:
info@corprisk.net

Corporate Risk[®]
SOLUTIONS

The NERC CIP Compliance Guide 3rd Edition User Listing

Provide the name and email address for each user to whom you would like a protected PDF to be issued. Please write legibly for accurate processing. Thank you!

NAME

EMAIL

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____
22. _____
23. _____
24. _____
25. _____