

Cross-Reference of (proposed) Standard 1300 to Standard 1200
 (Requirements shown in Red indicate they are new to 1300)

Standard 1300	Standard 1200
1301 Security Management Controls	
1301.a.1 Cyber Security Policy	1201
1301.a.2 Information Protection (including identification and classification)	1210
1301.a.3 Roles and Responsibilities (including access authorization)	1201
1301.a.4 Governance (see joint task force report recommendations)	
1301.a.5 Access Authorization	
1301.a.6 Authorization to Place into Production	
1302 Critical Cyber Assets	
1302.a.1 Critical Bulk Electric System Assets	
1302.a.2 Critical Cyber Assets	1202
1303 Personnel & Training (including contractors, etc.)	
1303.a.1 Awareness	
1303.a.2 Training	1211
1303.a.3 Records	1211
1303.a.4 Background Screening	1207
1304 Electronic Security	
1304.a.1 Electronic Security Perimeter	1203
1304.a.2 Electronic Access Controls	1204
1304.a.3 Monitoring Electronic Access	1209
1304.a.4 Documentation Review and Maintenance	1203/1204/1208/1209
1305 Physical Security	
1305.a.1 Documentation	1205
1305.a.2 Physical Security Perimeter	1205
1305.a.3 Physical Access Controls	1206
1305.a.4 Monitoring Physical Access	1208
1305.a.5 Logging Physical Access	
1305.a.6 Maintenance and Testing	
1306 Systems Security Management	
1306.a.1 Test Procedures	1213
1306.a.2 Account and Password Management	1212
1306.a.3 Security Patch Management	1212
1306.a.4 Integrity Software	1212
1306.a.5 Identification of Vulnerabilities and Responses	1212
1306.a.6 Retention of Logs (operator, application, intrusion detection)	1212
1306.a.7 Change Control and Configuration Management	1213
1306.a.8 Disabling Unused Network Services/Ports	1212
1306.a.9 Dial-up Modems	
1306.a.10 Operating Status Monitoring Tools	
1306.a.11 Back-up and Recovery	
1307 Incident Response Planning	
1307.a.1 Incident Response Plan Documented	1214/1215
1307.a.2 Incident Classification	
1307.a.3 Electronic and Physical Incident Response Actions	1214/1215
1307.a.4 Incident and Cyber Security Incident Reporting	1214/1215
1308 Recovery Plans (with linkage to Incident Response)	
1308.a.1 Recovery Plan Document	1216
1308.a.2 Event Response	1216
1308.a.3 Update Recovery Plans	
1308.a.4 Train on Recovery Plans	

Cross-Reference of Standard 1200 to (proposed) Standard 1300

Standard 1200	Standard 1300
1201 Cyber Security Policy	1301.a.1/1301.a.3
1202 Critical Cyber Assets	1302.a.2
1203 Electronic Security Perimeter	1304.a.1/1304.a.4
1204 Electronic Access Controls	1304.a.2/1304.a.4
1205 Physical Security Perimeter	1305.a.1/1305.a.2
1206 Physical Access Controls	1305.a.3
1207 Personnel	1303.a.4
1208 Monitoring Physical Access	1305.a.4
1209 Monitoring Electronic Access	1304.a.3/1304.a.4
1210 Information Protection	1301.a.2
1211 Training	1303.a.2/1303.a.3
1212 Systems Management	1306.a.2/1306.a.3/1306.a.4/1306.a.5/1306.a.6/1306.a.8
1213 Test Procedures	1306.a.1/1306.a.7
1214 Electronic Incident Response Actions	1307.a.1/1307.a.3/1307.a.4
1215 Electronic Incident Response Actions	1307.a.1/1307.a.3/1307.a.4
1216 Recovery Plans	1308.a.1/1308.a.2