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

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)   1201     1301.a.5 Access Authorization   1202     1302.a.1 Critical Buk Electric System Assets   1302.a.2     1302.a.2 Critical Cyber Assets   1202     1303.a.1 Awareness   1211     1303.a.3 Records   1211     1303.a.4 Background Screening   1201     1304 Electronic Security   1201     1304 a.1 Electronic Security Perimeter   1203     1304 a.2 Electronic Access Controls   1204     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 a.2 Physical Security   1205     1305 a.2 Diging Physical Access   1206     1305 a.2 Countiation   1205     1305 a.4 Monitoring Physical Access   1206     1305 a.5 Logging Physical Access   1208     1305 a.5 Logging Physical Access   1208  1	Standard 1300 1301 Security Management Controls	Standard 1200
1301.a.2 information Protection (including identification and classification)12101301.a.3 Roles and Responsibilities (including access authorization)12011301.a.4 Governance (see joint task force report recommendations)1301.a.51301.a.5 Access Authorization1301.a.61302 Critical Cyber Assets12021303 Personnel & Training (including contractors, etc.)1303.a.11303.a.1 Awareness12011303.a.2 Training12111303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security Perimeter12031304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Access12091304.a.4 Documentation12051305.a.4 Documentation12051305.a.4 Monitoring Electronic Access12061305.a.4 Monitoring Physical Access12081305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12121306 Systems Security Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Nettrification of Logs (operator, application, intruston detection)12121306.a.1 Back-up and Recovery		1201
1301.a.3 Roles and Responsibilities (including access authorization)12011301.a.4 Governance (see joint task force report recommendations)1301.a.51301.a.5 Access Authorization1302.a.51302.a.1 Critical Bulk Electric System Assets12021303 Personnel & Training (including contractors, etc.)1203.a.11303.a.2 Training12111303.a.3 Records12111303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security12031304 Lectronic Security Perimeter12031304.a.2 Electronic Access12091304.a.4 Documentation12041304.a.3 Monitoring Electronic Access12091305 a.1 Documentation12051305.a.2 Physical Security12051305.a.4 Monitoring Perimeter12031304.a.4 Documentation12051305.a.5 Logging Physical Access12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12131306.a.1 Test Procedures12121306.a.3 Security Ata Management12121306.a.3 Locurity Management12121306.a.5 Logging Coperator, application, intrusion detection)12121306.a.6 Metention of Logs (operator, application, intrusion detection)12121306.a.6 Metention of Logs (operator, application, intrusion detection)12121306.a.6 Metention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Managem		
1301 a.4 Governance (see joint task force report recommendations) 1301 a.5 Access Authorization 1302 Critical Cyber Assets 1302.a.1 Critical Bulk Electric System Assets 1303.a.2 Critical Cyber Assets 1303.a.2 Critical Cyber Assets 1303 Personnel & Training (including contractors, etc.) 1303 Personnel & Training 1303.a.1 Awareness 1303.a.2 Training 1211 1303.a.3 Records 1211 1303.a.4 Background Screening 1207 1304 Lettertonic Security 1304.a.4 Electronic Security Perimeter 1304.a.1 Electronic Access 1209 1304 a.4 Documentation Review and Maintenance 1203/1204/1208/1209 1305 Physical Security 1305.a.1 Documentation 1305 a.1 Documentation 1305.a.2 Physical Access 1208 1305.a.5 Logging Physical Access 1306.a.5 Maintenance and Testing 1306 Systems Security Management 1306.a.5 Maintenance and Testing 1306 A.3 Security Perimeter 1306.a.1 Test Procedures 1212 1306.a.1 Test Procedures 1212 1306.a.5 Identification of Uninrabilities and Responses 1212 1306.a.5 Identification of Uninrabilities 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.7 Change Control and Configuration Management 1213 1306.a.7 Change Control and Configuration Management 1212 1306.a.6 Retention of Logs (operator, application, intrusion detection) 1212 1306.a.6 Retention of Logs (operator, application, intrusion detection) 1212 1306.a.7 Change Control and Configuration Management 1213 1306.a.6 Retention of Logs (operator, application, intrusion detection) 1212 1306.a.6 Retention of Logs (operator, application, intrusion detection) 1212 1306.a.1 Back-up and Recovery		
1301.a.5 Access Authorization 1302.a.6 Authorization to Place into Production1302. Critical Cyber Assets1302.a.1 Critical Bulk Electric System Assets1302.a.2 Critical Cyber Assets1303 Personnel & Training (including contractors, etc.)1303.a.1 Awareness1303.a.2 Training1303.a.3 Records1304 Electronic Security1304 Electronic Security1304.a.1 Electronic Security Perimeter1304.a.2 Electronic Access Controls1305 a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security1305 a.5 Logging Physical Access1305 a.6 Maintenance and Testing1305 a.7 System Access1305 a.6 Maintenance12071305 a.7 Documentation1305 a.6 Maintenance and Testing1305 a.6 Maintenance and Testing1306 Systems Security Management1306 a.7 Caccourt and Password Management1306 a.7 Caccourt and Password Management1306 a.6 Maintenance and Testing1306 a.7 Change Control and Configuration, intrusion detection)12121306 a.6 Retention of Logs (operator, application, intrusion detection)12121306 a.6 Retention of Logs (operator, application, intrusion detection)12121306 a.7 Change Control and Configuration Management12121306 a.6 Retention of Logs (operator, application, intrusion detection)12121306 a.6 Detail Modems1306 a.7 Danage Control and Configuration Management12121306 a.6 Detail Modems1306 a		
1302 Critical Cyber Assets1302.a.11302.a.2 Critical Cyber Assets12021303 Personnel & Training (including contractors, etc.)1303.a.11303.a.1 Awareness12111303.a.2 Training12111303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security12031304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Security Perimeter12041304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security12051305 a.2 Physical Security Perimeter12051305 a.3 Physical Access Controls12061305 a.3 Physical Access Controls12061305 a.3 Physical Access Controls12061305 a.3 Physical Access Controls12061305 a.4 Monitoring Physical Access12081305 a.5 Logging Physical Access12081305 a.6 Maintenance and Testing12121306 Systems Security Management12121306 a.7 Change Control and Configuration Management12121306 a.6 Identification of Logs (operator, application, intrusion detection)12121306 a.7 Change Control and Configuration Management12131306 a.8 Disabiling Unused Network Services/Ports12121306 a.9 Dial-up Modems12131306 a.9 Dial-up Modems12121306 a.9 Dial-up Modems12121306 a.1 Bask-up and Recovery1212		
1302.a.1 Critical Bulk Electric System Assets12021303 Personnel & Training (including contractors, etc.)1303.a.1 Awareness1303.a.1 Awareness12111303.a.2 Training12111303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security12031304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Access Controls12041304.a.3 Monitoring Electronic Access12091305 Physical Security12051305 A.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security12051305.a.1 Documentation12051305.a.2 Dysical Access12061305.a.3 Physical Access12081305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081306.a.1 Test Procedures12121306.a.3 Excurity Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabiling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.1 Back-up and Recovery1212	1301.a.6 Authorization to Place into Production	
1302.a.2 Critical Cyber Assets12021303 Personnel & Training (including contractors, etc.)1303.a.1 Awareness1303.a.1 Awareness12111303.a.2 Training12111303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security12031304.a.1 Electronic Access Controls12041304.a.2 Electronic Access Controls12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security12051305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.4 Monitoring Physical Access12061305.a.5 Logging Physical Access12081306 Systems Security Management12121306.a.1 Test Procedures12121306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Ohange Control and Configuration Management12131306.a.8 Disabiling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.10 Operating Status Monitoring Tools12121306.a.11 Back-up and Recovery1212		
1303 Personnel & Training (including contractors, etc.)1303.a.1 Awareness1303.a.2 Training1303.a.2 Training1303.a.2 Training1303.a.3 Records12111303.a.4 Background Screening1304.a.1 Electronic Security1304.a.2 Electronic Coress Controls1304.a.2 Electronic Access Controls1304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security1305.a.1 Documentation12051305.a.2 Physical Security1305.a.3 Documentation12051305.a.4 Monitoring Physical Access1305.a.5 Logging Physical Access1305.a.6 Maintenance and Testing1306.a.6 Maintenance and Testing1306.a.1 Test Procedures1306.a.2 Ideging Physical Access1306.a.3 Steurity Patch Management1306.a.4 Integrity Software1306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management1306.a.8 Disabiling Unused Network Services/Ports1306.a.1 Deprating Status Monitoring Tools1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery	•	1202
1303.a.1 Awareness12111303.a.2 Training12111303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security12031304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Access Controls12041304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security12051305.a.2 Physical Security Perimeter12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12061305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12111306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.3 Security Path Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabiling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.10 Operating Status Monitoring Tools12121306.a.11 Back-up and Recovery1212	1302.a.2 Chucai Cyber Assets	1202
1303.a.2 Training12111303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security12031304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Access Controls12041304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12121306.a.1 Test Procedures12131306.a.3 Security Management12121306.a.4 count and Password Management12121306.a.3 Security Software12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabiling Unused Network Services/Ports12121306.a.10 Operating Status Monitoring Tools12121306.a.11 Back-up and Recovery1212		
1303.a.3 Records12111303.a.4 Background Screening12071304 Electronic Security12031304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Access Controls12041304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security12051305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12061305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12121306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Cest Control of Vulnerabilities and Responses12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabiling Unused Network Services/Ports12121306.a.9 Dial-up Modems12131306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery		
1303.a.4 Background Screening12071304 Electronic Security12031304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Access Controls12041304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security1305 a.1 Documentation1305.a.1 Documentation12051305.a.2 Physical Security Perimeter12061305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12131306.a.7 Chage Control Management12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Chage Control and Configuration Management12131306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Chage Control and Configuration Management12131306.a.9 Dial-up Modems12131306.a.9 Dial-up Modems12121306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery	•	
1304 Electronic Security12031304.a.1 Electronic Access Controls12041304.a.2 Electronic Access Controls12041304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security1305.a.1 Documentation1305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12061305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12121306.a.1 Test Procedures12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.10 Operating Status Monitoring Tools12021306.a.11 Back-up and Recovery1212		
1304.a.1 Electronic Security Perimeter12031304.a.2 Electronic Access Controls12041304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security12051305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12121306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.9 Dial-up Modems12131306.a.11 Back-up and Recovery1212	1303.a.4 Background Screening	1207
1304.a.2 Electronic Access Controls12041304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security1305.a.1 Documentation1305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12061305.a.5 Logging Physical Access12081306.a.6 Maintenance and Testing12131306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.9 Dial-up Modems12131306.a.10 Operating Status Monitoring Tools12021306.a.11 Back-up and Recovery1205		
1304.a.3 Monitoring Electronic Access12091304.a.4 Documentation Review and Maintenance1203/1204/1208/12091305 Physical Security1305.a.1 Documentation1305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12131306.a.1 Test Procedures12121306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.11 Back-up and Recovery		1203
1304.a.4 Documentation Review and Maintenance1203/1204/1208/120913051305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12131306 Systems Security Management12121306.a.1 Test Procedures12121306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.7 Change Control and Configuration Management12121306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.11 Back-up and Recovery1305		
1305 Physical Security12051305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12131306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.7 Change Control and Configuration, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.1 Back-up and Recovery1212		
1305.a.1 Documentation12051305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12131306.a.1 Test Procedures12131306.a.1 Test Procedures12121306.a.3 Security Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabiling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.11 Back-up and Recovery1306	1304.a.4 Documentation Review and Maintenance	1203/1204/1208/1209
1305.a.2 Physical Security Perimeter12051305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access12081305.a.6 Maintenance and Testing12131306.a.1 Test Procedures12131306.a.1 Test Procedures12121306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.9 Dial-up Modems12121306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery	1305 Physical Security	
1305.a.3 Physical Access Controls12061305.a.4 Monitoring Physical Access12081305.a.5 Logging Physical Access1305.a.6 Maintenance and Testing1306 Systems Security Management12131306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery		1205
1305.a.4 Monitoring Physical Access 1305.a.5 Logging Physical Access 1305.a.6 Maintenance and Testing12081306 Systems Security Management 1306.a.1 Test Procedures1213 1306.a.2 Account and Password Management1212 1212 1306.a.3 Security Patch Management1306.a.4 Integrity Software1212 1306.a.5 Identification of Vulnerabilities and Responses1212 1212 1306.a.6 Retention of Logs (operator, application, intrusion detection)1306.a.7 Change Control and Configuration Management1213 1213 1306.a.8 Disabling Unused Network Services/Ports1212 1213 1306.a.10 Operating Status Monitoring Tools 1306.a.11 Back-up and Recovery		
1305.a.5 Logging Physical Access 1305.a.6 Maintenance and Testing1306 Systems Security Management 1306.a.1 Test Procedures1213 1306.a.2 Account and Password Management1306.a.2 Account and Password Management1212 1212 1306.a.3 Security Patch Management1306.a.4 Integrity Software1212 1212 1306.a.5 Identification of Vulnerabilities and Responses1306.a.6 Retention of Logs (operator, application, intrusion detection)1212 1212 1306.a.7 Change Control and Configuration Management1306.a.8 Disabling Unused Network Services/Ports1212 1306.a.9 Dial-up Modems 1306.a.10 Operating Status Monitoring Tools 1306.a.11 Back-up and Recovery		
1305.a.6 Maintenance and Testing1306 Systems Security Management1306.a.1 Test Procedures1306.a.2 Account and Password Management1306.a.2 Account and Password Management1306.a.3 Security Patch Management1306.a.4 Integrity Software1306.a.5 Identification of Vulnerabilities and Responses1306.a.6 Retention of Logs (operator, application, intrusion detection)1306.a.7 Change Control and Configuration Management1306.a.8 Disabling Unused Network Services/Ports1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery		1208
1306 Systems Security Management12131306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery1306		
1306.a.1 Test Procedures12131306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery1306.a.11 Back-up and Recovery	1305.a.6 Maintenance and Testing	
1306.a.2 Account and Password Management12121306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery1306		
1306.a.3 Security Patch Management12121306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery		
1306.a.4 Integrity Software12121306.a.5 Identification of Vulnerabilities and Responses12121306.a.5 Identification of Logs (operator, application, intrusion detection)12121306.a.6 Retention of Logs (operator, application Management12131306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems12121306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery		
1306.a.5 Identification of Vulnerabilities and Responses12121306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery1306.a.11 Back-up and Recovery		
1306.a.6 Retention of Logs (operator, application, intrusion detection)12121306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery1306.a.11 Back-up and Recovery		
1306.a.7 Change Control and Configuration Management12131306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery1306.a.11 Back-up and Recovery		
1306.a.8 Disabling Unused Network Services/Ports12121306.a.9 Dial-up Modems1306.a.10 Operating Status Monitoring Tools1306.a.11 Back-up and Recovery1306.a.11 Back-up and Recovery		
1306.a.9 Dial-up Modems 1306.a.10 Operating Status Monitoring Tools 1306.a.11 Back-up and Recovery		
1306.a.10 Operating Status Monitoring Tools 1306.a.11 Back-up and Recovery		1212
1306.a.11 Back-up and Recovery		
1307 Incident Response Planning		
	1307 Incident Response Planning	
1307.a.1 Incident Response Plan Documented 1214/1215		1214/1215
1307.a.2 Incident Classification		
1307.a.3 Electronic and Physical Incident Response Actions 1214/1215	1307.a.3 Electronic and Physical Incident Response Actions	1214/1215
1307.a.4 Incident and Cyber Security Incident Reporting1214/1215	• •	1214/1215
1308 Recovery Plans (with linkage to Incident Response)	1308 Recovery Plans (with linkage to Incident Response)	
1308.a.1 Recovery Plan Document 1216		1216
1308.a.2 Event Response 1216		
1308.a.3 Update Recovery Plans		
1308.a.4 Train on Recovery Plans	1308.a.4 Train on Recovery Plans	

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

Standard 1200 1201 Cyber Security Policy	<b>Standard 1300</b> 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.a8
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