Catalog of Control Systems Security: Recommendations for Standards Developers

April 2011

Homeland Security

Appendix A

Cross Reference of Standards

This cross reference mapping loosely correlates the requirements and guidance contained in the referenced source documents against the recommendations in the Catalog of Control Systems Security. This correlation depicts a general relationship between multiple documents in multiple industrial sectors. The cross reference cannot imply an exact matching between specific requirement details and multiple controls currently existing, but strives to implicitly address and associate specific controls across several standards and guidance documents.

The source documents in the cross reference are constantly evolving to address new and expanded understanding of security topics. Previous source documents have been deleted from this document as they are no longer relevant, or have been superseded by newer documents. This crosswalk attempts to use the most recent update of the source documents available at the time of publication, but availability, publishing and timing may result in older versions of source documents being referenced and used. Furthermore, it is not possible to determine the priority and baseline risk for each control family in every industrial facility and control system deployment.

Two reference sources were removed from the cross reference at this time. They are: (1) ChemITC—"Guidance for Addressing Cybersecurity in the Chemical Sector, Version 3.0; Chemical Sector Cyber Security Program May 2006"; This document has been superseded by "Guidance for Addressing Cyber Security in the Chemical Industry, Version 4, November 2009," and has not yet been reviewed; and (2) "NERC Security Guidelines—Security Guidelines for the Electricity Sector, Version 1.0 May 3, 2005," has been superseded by the NERC Critical Infrastructure Protection (CIP) reliability standards.

Two new additional reference sources were added at this time. They are (1) "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)," Version 2.3 November 13, 2009, and (2) U.S. Nuclear Regulatory Commission—Regulatory Guide 5.71—"Cyber Security Programs for Nuclear Facilities," January 2010. These two sources were added, as they are the latest cybersecurity standards released and provide a very good basis in industrial cybersecurity. The CAG, for instance, is broken down into four categories within each of the 20 critical controls. The first category is label "QW," which denotes a "quick win," action that will immediately improve the security posture, especially if addressed by the user. The second category is "Improved Visibility and Attribution," meant to increase monitoring, visibility and attribution, so organizations can better monitor network and computer systems. The third category is "Hardened Configuration and Improved Information Security Hygiene," and focuses on protecting against poor security practices by system administrators and end users. The final category is "Advanced" and identifies actions and items that further improve security beyond the other three categories. The CAG also lists functional/effectiveness testing to see how and if security functions are working. The NRC RG 5.71 takes elements from NIST SP 800-53 r3 and NIST SP 800-82 and focuses on how to use these elements in the operation of nuclear reactors. Most ICSs share similar layout, function and security. Three appendixes are in NRC 5.71. Appendix A is a generic Cyber Security Plan template for utilities to use. Appendix B contains Technical Security Controls, while Appendix C consists of Operational and Management Security Controls. The unique method on which roles, configuration, what to test, how to test, and periodic retesting provides an element lacking in current cybersecurity standards and guidelines.

The cross reference is accurate at the time of the most recent update. The reader is encouraged to confirm the currency, accuracy, and applicability of the source documents and obtain current copies of all

pertinent source documents as necessary. The versions of the documents used in the cross reference are listed below:

AGA 12-1	Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan, Draft 5, April 14, 2005.
AGA 12-2	Cryptographic Protection of SCADA Communications Part 2: Retrofit Link Encryption for Asynchronous Serial Communications, March 31, 2006.
FIPS 140-2	Security Requirements for Cryptographic Modules, issued May 25, 2001, updated December 3, 2002.
API 1164	Pipeline SCADA Security, Second Edition, June 2009.
API Security Guidelines	Security Guidelines for the Petroleum Industry, April 2005.
CAG	Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines, Version 2.3 November 13, 2009.
ChemITC	Guidance for Cyber Security in Chemistry, Version 4, November 2009.
ISO 17799	Information Technology—Security Techniques—Code of Practice for Information Security Management, Second Edition, 2005-06-15, superseded by ISO 27002.
ISO 27001	Information Technology—Security Techniques—Information Security Management Systems—Requirements, First Edition, October 15, 2005.
IEC 62351	Data and Communications Security—Introduction, Committee Draft Version 1, April 2005.
IEEE 1402	IEEE Guide for Electric Power Substation Physical and Electronic Security, January 30, 2000.
ISA 99-1	Manufacturing and Control Systems Security, Part 1: Models and Terminology, Draft 1, Edit, February 8, 2005.
ISA99-2	Manufacturing and Control System Security, Part 2: Establishing a Manufacturing and Control System Security Program, Draft 1, Edit 1, April 15, 2005.
NERC CIP	Cyber Security, 002-3 to 009-3: Approved by Board of Trustees: December 16, 2009.
NIST SP 800-53R3	NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009.
RG 5.71	U.S. Nuclear Regulatory Commission – Regulatory Guide 5.71 – "Cyber Security Programs for Nuclear Facilities", January 2010.

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.1.1	Security Policy and Procedures	X	—	X	X	X	X	X	X	—	—	X	X	X	X	X
2.2.1	Management Policy and Procedures	—	—	—	X	X	—	X	X	—	—	X	X	X	X	X
2.2.2	Management Accountability	X	—	—	X	X	—	X	X	—	—	X	X	—	X	X
2.2.3	Baseline Practices	—	—	—	X	X	—	X	X	—	—	X	X	X	X	X
2.2.4	Coordination of Threat Mitigation	—	—	—	X	X	—	X	—	—	—	—	X	—	X	X
2.2.5	Security Policies for Third Parties	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.2.6	Termination of Third-Party Access	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.1	Personnel Security Policy and Procedures	—	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.3.2	Position Categorization	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.3.3	Personnel Screening	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.3.4	Personnel Termination	X	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.5	Personnel Transfer	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.6	Access Agreements	—	—	X	X	—	—	X	—	—	—	—	X	X	—	X
2.3.7	Third-Party Personnel Security	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.8	Personnel Accountability	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.3.9	Personnel Roles	—	—	—	X	X	—	X	—	—	X	—	X	X	X	X
2.4.1	Physical and Environmental Security Policy and Procedures	X	—	X	X	X	—	X	—	—	X	—	X	X	X	X
2.4.2	Physical Access Authorizations	—	—	X	X	—	—	X	—	—	X	—	X	X	X	X
2.4.3	Physical Access Control	—	—	—	X	X	—	X	—	—	X	—	X	X	X	X
2.4.4	Monitoring Physical Access	—	—	—	X	X	—	X	—	X	X	—	X	X	X	X
2.4.5	Visitor Control	—	—	—	X	X	—	X	—	—	X	—	—	X	X	X
2.4.6	Visitor Records		—	—	X	X	—	X	—	—	—	—	—	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.4.7	Physical Access Log Retention	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.4.8	Emergency Shutoff	—	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.4.9	Emergency Power	—	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.4.10	Emergency Lighting	—	—	—	X	X	—	X	—	—	—	—	X	X	—	X
2.4.11	Fire Protection		—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.4.12	Temperature and Humidity Controls	—	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.4.13	Water Damage Protection	—	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.4.14	Delivery and Removal	—	—	—	—	—	—	X	—	—	—	—	X	—	—	X
2.4.15	Alternate Work Site	—	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.4.16	Portable Media	X	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.4.17	Personnel and Asset Tracking	—	—	—	—	—	—	X	—	—	—	—	X	X	—	—
2.4.18	Location of Control System Assets	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.4.19	Information Leakage	—	—	—	X	X	—	X	X	—	—	—	—	X	—	X
2.4.20	Power Equipment and Power Cabling	—	—	—	X	—	—	—	—	—	—	X	—	X	—	X
2.4.21	Physical Device Access Control	X	—	X	X	X	—	—	—	—	—	X	—	X		X
2.5.1	System and Services Acquisition Policy and Procedures	—	—	—	X	X	X	X	X	—	—	—	—	X	—	X
2.5.2	Allocation of Resources	X	—	—	X	—	—	X	X	—	—	—	—	X	—	X
2.5.3	Life-Cycle Support	—	—	—	—		X	—	—	—	—	—	—	X	—	X
2.5.4	Acquisitions	—	—	X	—	—	X	X	—	—	—	—	—	X	—	X
2.5.5	Control System Documentation	X	—	X	X	—	—	X	X	—	—	—	—	X	X	X
2.5.6	Software License Usage Restrictions	—	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.5.7	User-Installed Software	X	—	—	X	X	X	X	—	—	—	—	—	X	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.5.8	Security Engineering Principles	X	—	—	X	X	X	X	X	—	—	—	—	X	—	X
2.5.9	Outsourced Control System Services	—	—	—	X	X	—	X	—	—	—	—	—	X	—	X
2.5.10	Developer Configuration Management	X	—	X	X	X	X	—	—	—	—	—	—	X	—	X
2.5.11	Developer Security Testing	—	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.5.12	Supply Chain Protection	X	—	X	—	X	—	X	—	—	—	—	—	X	—	X
2.5.13	Trustworthiness	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.5.14	Critical Information System Components	X	—	X	X	—	—	X	—	—	—	X	X	X		X
2.6.1	Configuration Management Policy and Procedures	X	—	X	X	—	X	X	—	—	—	X	X	X	X	X
2.6.2	Baseline Configuration	X	—	X	X	—	X	—	—	—	—	—	—	X	X	X
2.6.3	Configuration Change Control	X	—	X	X	—	X	X	—	—	—	X	X	X	X	X
2.6.4	Monitoring Configuration Changes	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.6.5	Access Restrictions for Configuration Change	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.6.6	Configuration Settings	—	—	—	—	X	X	X	—	—	—	—	X	X	X	X
2.6.7	Configuration for Least Functionality	—	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.6.8	Configuration Assets	—	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.6.9	Addition, Removal, and Disposal of Equipment	—	—	—	—	—	X	X	—	—	—	—	X	X	X	—

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.6.10	Factory Default Authentication Management	—	—	X	X	—	X	X	—	—	—	—	X	X	X	X
2.6.11	Configuration Management Plan	—	—	—	X	—	—	—	—	—	—	—	—	X	X	X
2.7.1	Strategic Planning Policy and Procedures	—	—	—	—	X	—	X	X	—	X	—	X	X	X	X
2.7.2	Control System Security Plan	X	—	—	X	X	—	X	X	—	X	—	X	X	X	X
2.7.3	Interruption Identification and Classification	—	—	—	—	X	X	X	X	—	—	—	X	X	X	X
2.7.4	Roles and Responsibilities	X	—	—	X	X	X	X	X	—	X	—	X	X	X	X
2.7.5	Planning Process Training	X	—	—	X	X	X	X	X	—	—	X	X	X	X	X
2.7.6	Testing	X	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.7.7	Investigation and Analysis	—	—	—	X	X	—	X	X	—	—	—	X	X		X
2.7.8	Corrective Action	—	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.7.9	Risk Mitigation	—	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.7.10	System Security Plan Update	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.7.11	Rules of Behavior	—	—	X	X	X	—	X	—	—	—	—	X	X	X	X
2.7.12	Security-Related Activity Planning	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.8.1	System and Communication Protection Policy and Procedures	X	—	X	X	X	—	X	—	—	—	—	X	X	X	X
2.8.2	Management Port Partitioning	X	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.8.3	Security Function Isolation	—	—	X	X	—	X	X	—	—	—	—	—	X	X	X
2.8.4	Information in Shared Resources	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.8.5	Denial-of-Service Protection	—	X	—	X	X	—	—	—	X	—	—	X	X	—	X
2.8.6	Resource Priority	X	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.8.7	Boundary Protection	—	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.8.8	Communication Integrity	X	—	—	X	X	—	X	—	—	—	—	—	X	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.8.9	Communication Confidentiality	X	—	X	X	X	X	X	—	—	—	—	X	X	—	X
2.8.10	Trusted Path	X	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.8.11	Cryptographic Key Establishment and Management	X	—	X	—	—	—	X	—	—	—	—	—	X	—	X
2.8.12	Use of Validated Cryptography	X	—	X	—	—	X	X	—	—	—	—	—	X	—	X
2.8.13	Collaborative Computing Devices	—	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.8.14	Transmission of Security	X	—	—		—	—	X	—	—	—	—	—	X	—	X
2.8.15	Public Key Infrastructure Certificates	X	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.8.16	Mobile Code	—	—	—	—	—	X	X	—	—	—	—	—	X	—	X
2.8.17	Voice-Over Internet Protocol	—	—	—	X	—	—	—	—	—	—	—	—	—	—	X
2.8.18	System Connections	X	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.8.19	Security Roles	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.8.20	Session Authenticity	X	—	—	X	—	—	X	X	X	—	X	—	X	—	X
2.8.21	Architecture and Provisioning for Name/Address Resolution Service	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.22	Secure Name/Address Resolution Service (Authoritative Source)	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.24	Fail in Known State	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.25	Thin Nodes	—	—	—		—	—	—	—	—	—	—	—	X	—	X
2.8.26	Honeypots	—	—	—	—	—	X	—	—	—	—	—	—	—	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.8.27	Operating System-Independent Applications	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.8.28	Confidentiality of Information at Rest	—	—	—	X	—	X	—	—	—	—	—	—	X	—	X
2.8.29	Heterogeneity	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.8.30	Virtualization Techniques	—	—	—	—	—	—	—	—	—	—	—	—	—	—	X
2.8.31	Covert Channel Analysis	—	—	—	—	—	X	—	—	—	—	—	—	—	—	X
2.8.32	Information System Partitioning	—	—	—	X	—	—	X	—	—	—	—	X	X		X
2.8.33	Transmission Preparation Integrity	—	—	—	—	X	—	X	—	—	—	—	X	X		X
2.8.34	Non-Modifiable Executable Programs	—	—	—	X	—	—	X	—	—	—	—	X	—	—	X
2.9.1	Information and Document Management Policy and Procedures	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.9.2	Information and Document Retention	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.9.3	Information Handling	X	—	—	X	—	—	X	X	—	—	—	X	X	X	X
2.9.4	Information Classification	X	—	X	X	X	X	X	—	—	—	—	X	X	X	X
2.9.5	Information Exchange	X	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.9.6	Information and Document Classification	X	—	X	X	—	X	X	—	—	—	—	X	X	X	X
2.9.7	Information and Document Retrieval	X	—	—	X	—	—	X	X	—	—	—	X	X	—	X
2.9.8	Information and Document Destruction	X	—	—	X	—	—	X	X	—	—	—	X	X	—	—
2.9.9	Information and Document Management Review	X	—	—	X	—	—	X	—	—	—	—	X	X	X	—

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.9.10	Media Marking	—	—	—	X	—	X	—	—	—	—	—	—	X	—	X
2.9.11	Security Attributes	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.10.1	System Maintenance Policy and Procedures	X	—	X	X	—	—	X	X	—	X	—	X	X	X	X
2.10.2	Legacy System Upgrades	X	—	X	X	—	X	—	—	—	—	—	X	X		X
2.10.3	System Monitoring and Evaluation	X	—	X	X	X	X	X	—	—	—	X	X	X	X	X
2.10.4	Backup and Recovery	X	—	X	X	X	X	X	—	—	—	X	X	X	X	X
2.10.5	Unplanned System Maintenance	X	—	—	X	—	—	X	—	—	—	X	X	X		—
2.10.6	Periodic System Maintenance	X	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.10.7	Maintenance Tools	X	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.10.8	Maintenance Personnel	—	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.10.9	Non-Local (Remote) Maintenance	—	—	X	X	—	—	X	—	—	—	X		X	—	X
2.10.10	Timely Maintenance	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.11.1	Security Awareness and Training Policy and Procedures	—	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.11.2	Security Awareness	X	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.11.3	Security Training	—	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.11.4	Security Training Records	—	—	X	X	—	—	—	X	—	—	—	X	X	X	X
2.11.5	Contact with Security Groups and Associations	X	—	X	X	X	—	X	—	—	—	—	—	X	X	X
2.11.6	Security Responsibility Testing	—	—	—	X	X	—	—	X	—	—	—	X	X	—	—
2.12.1	Incident Response Policy and Procedures	X	—	—	X	X	X	X	X	—	X	—	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.12.2	Continuity of Operations Plan	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.12.3	Continuity of Operations Roles and Responsibilities	—	—	X	X	X	—	X	X	—	—	—	X	X	X	X
2.12.4	Incident Response Training	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.12.5	Continuity of Operations Plan Testing	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.12.6	Continuity of Operations Plan Update	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.12.7	Incident Handling	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.12.8	Incident Monitoring	—	—	—	X	X	X	X	X	—	—	—	—	X	X	X
2.12.9	Incident Reporting	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.12.10	Incident Response Assistance	—	—	—	—	X	—	X	—	—	—	—	—	X		X
2.12.11	Incident Response	—	—	—	X	—	—	X	X	—	—	—	X	X	X	X
2.12.12	Corrective Action	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.12.13	Alternate Storage Sites	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.12.14	Alternate Command/Control Methods	—	—	—	X	X	—	X	—	—	X	—	X	X	—	X
2.12.15	Alternate Control Center	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.12.16	Control System Backup	—	—	—	X	X	X	—	—	—	—	—	X	X	X	X
2.12.17	Control System Recovery and Reconstitution	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.12.18	Fail-Safe Response	—	—	—	X	—	—	—	—	—	—	—	—	—	—	—
2.13.1	Media Protection Policy and Procedures	X	—	—	X	—	—	—	X	—	—	—	—	X	X	X
2.13.2	Media Access	—	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.13.3	Media Classification	—	—	—	X	X	X	X	X	—	—	—	—	X	X	X
2.13.4	Media	—	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.13.5	Media Storage	—	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.13.6	Media Transport	—	—	—	—	—	—	X	X	—	—	—	—	X	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.13.7	Media Sanitization and Disposal	X	—	—	X	—	—	X	X	—	—	—	—	X	X	X
2.14.1	System and Information Integrity Policy and Procedures	—	—	—	—	X	—	—	X	—	—	—	—	X	X	X
2.14.2	Flaw Remediation	—	—	—	X	X	—	X	X	—	—	—	—	X	X	X
2.14.3	Malicious Code Protection	X	—	—	X	X	X	X	—	—	—	—	—	X	X	X
2.14.4	System Monitoring Tools and Techniques	X	—	—	X	—	X	X	—	—	—	—	—	X	X	X
2.14.5	Security Alerts and Advisories and Directives	X	—	—	X	X	—	X	—	—	—	—	—	X	X	X
2.14.6	Security Functionality Verification	—	X	X	X	—	—	X	—	—	—	—	—	X	—	X
2.14.7	Software and Information Integrity	—	X	X	X	—	X	X	—	—	—	—	—	X	—	X
2.14.8	Spam Protection	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.14.9	Information Input Restrictions	—	—	—	X	X	—	X	—	—	—	—	—	X	X	X
2.14.10	Information Input	—	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.14.11	Error Handling	—	X	—	X	—	—	X	—	—	—	—	—	X	—	X
2.14.12	Information Output Handling and Retention	—	—	—	X	X	—	X	X	—	—	—	—	X	X	X
2.14.13	Predictable Failure Prevention	—	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.15.1	Access Control Policy and Procedures	X	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.15.2	Identification and Authentication Policy and Procedures	X	X	X	—	X	—	X	X	—	X	—	X	X	X	X
2.15.3	Account Management	X	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.15.4	Identifier Management	X	—	X	X	X	—	X	—	—	—	—	X	X	X	X
2.15.5	Authenticator Management	—	—	X	X	—	X	X	—	—	—	—	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.15.6	Account Review	X	—	X	X	—	X	X	X	—	—	—	X	X	X	X
2.15.7	Access Enforcement	X	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.15.8	Separation of Duties	X	—	X	X	—	—	X	—	—	—	—	X	X	X	X
2.15.9	Least Privilege	X	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.15.10	User Identification and Authentication	X	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.15.11	Permitted Actions without Identification or Authentication	—	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.15.12	Device Identification and Authentication	—	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.15.13	Authenticator Feedback	—	—	X	X	—	—	X	—	—	—	—	—	X	X	X
2.15.14	Cryptographic Module Authentication	X	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.15.15	Information Flow Enforcement	—	—	X	X	—	X	X	—	—	—	—	—	X	X	X
2.15.16	Passwords	X	—	X	X	—	X	X	—	—	—	—	X	X	X	X
2.15.17	System Use Notification	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.15.18	Concurrent Session Control	X	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.15.19	Previous Logon (Access) Notification	—	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.15.20	Unsuccessful Login Attempts	—	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.15.21	Session Lock	—	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.15.22	Remote Session Termination	X	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.15.23	Remote Access Policy and Procedures	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.15.24	Remote Access	X	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.15.25	Access Control for Mobile Devices	—	—	—	X	X	X	X	—	—	—	—	X	X	—	X
2.15.26	Wireless Access Restrictions	X	—	—	X	—	X	X	—	—	—	—	—	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.15.27	Personally Owned Information	—	—	—	X	—	X	—	—	—	—	—	—	X	—	X
2.15.28	External Access Protections	—	—	—	X	X	X	X	—	—	—	—	—	X	X	X
2.15.29	Use of External Information Control Systems	X	X	—	X	X	X	—	—	—	—	—	X	X	X	X
2.15.30	User-Based Collaboration and Information Sharing	X	X	—	X	—	—	—	—	—	—	—	X	—	X	X
2.15.31	Publicly Accessible Content	X	X	—	X	—	—	—	—	—	—	—	X	X	X	X
2.16.1	Audit and Accountability Policy and Procedures	X	—	X	X	X	—	X	X	—	X	—	X	X	X	X
2.16.2	Auditable Events	X	—	X	X	X	X	X	—	—	—	—	—	X	X	X
2.16.3	Content of Audit Records	X	—	X	X	—	X	X	—	—	—	—	—	X	X	X
2.16.4	Audit Storage Capacity	—	—	—	—	—	X	X	—	—	—	—	—	X	—	X
2.16.5	Response to Audit Processing Failures	—	—	—		—	X	X	—	—	—	—	—	X	X	X
2.16.6	Audit Monitoring, Analysis, and Reporting	X	—	X	X	X	X	X	X	—	—	—	—	X	X	X
2.16.7	Audit Reduction and Report Generation	X	—	X	X	—	X	X	X	—	—	—	—	X	X	X
2.16.8	Time Stamps	—	—	—	—	—	X	X	—	—	—	—	—	X	X	X
2.16.9	Protection of Audit Information	X	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.16.10	Audit Record Retention	X	—	—	X	—	—	X	X	—	—	—	—	X	X	X
2.16.11	Conduct and Frequency of Audits	X	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.16.12	Auditor Qualification	—	—	—	X	—	X	—	—	—	—	—	X	X	—	X
2.16.13	Audit Tools	X	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.16.14	Security Policy Compliance	—	—	—	X	—	—	X	X	—	—	—	—	X	X	X
2.16.15	Audit Generation	—	—	—	—	—	—	—	—	—	—	—	—	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.16.16	Monitoring for Information Disclosure	—	—	—	—	—	—	—	—	—	—	—	—	—	X	X
2.16.17	Session Audit	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.17.1	Monitoring and Reviewing Control System Security Management Policy and Procedures	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.17.2	Continuous Improvement	—	—	—	X	—	X	X	X	—	—	X	X	X	X	X
2.17.3	Monitoring of Security Policy	—	—	—	X	—	X	—	X	—	—	—	X	X	X	X
2.17.4	Best Practices	—	—	—	X	X	X	—	X	—	—	—	X	X	X	X
2.17.5	Security Accreditation	X	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.17.6	Security Certification	X	—	—	X	X	—	—	X	—	—	—	—	—	—	X
2.18.1	Risk Assessment Policy and Procedures	X	—	—	X	X	—	X	X	—	X	X	X	X	X	X
2.18.2	Risk Management Plan	X	—	—	X	X	X	X	X	—	X	—	X	X	X	X
2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures	X	—	—	X	X	—	X	—	—	X	—	X	X	—	X
2.18.4	Security Assessments	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.18.5	Control System Connections	—	—	—	X	X	X	X	—	—	—	—	—	—	X	X
2.18.6	Plan of Action and Milestones	—	—	—	X	X	—	—	X	—	—	—	X	—	X	X
2.18.7	Continuous Monitoring	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.18.8	Security Categorization	—	—	—	X	—	X	X	—	—	—	—	X	—	X	X
2.18.9	Risk Assessment	—	—	—	X	X	X	X	X	—	X	X	X	X	X	X
2.18.10	Risk Assessment Update	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.18.11	Vulnerability Assessment and Awareness	—	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.18.12	Identify, Classify, Prioritize, and Analyze Potential Security Risks	—	—	—	X	—	X	—	—	—	—	—	—	X	X	X
2.19.1	Information Security Program Plan	—	—	—	X	—	—	—	—	—	—	—	—	X	X	X
2.19.2	Senior Information Security Officer	—	—	—	X	—	—	—	—	—	—	—	—	X	X	X
2.19.3	Information Security Resources	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.4	Plan of Action and Milestones Process	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.5	Information System Inventory	—	—	—	X	—	X	—	—	—	—	—	—	X	X	X
2.19.6	Information Security Measures of Performance	—	—	—	X	—	X	—	—	—	—	—	—	—	X	X
2.19.7	Enterprise Architecture	—	—	—	X	—	X	—	—	—	—	—	—	—	X	X
2.19.8	Critical Infrastructure Plan	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.9	Risk Management Strategy	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.10	Security Authorization Process	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.11	Mission/Business Process Definition	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X