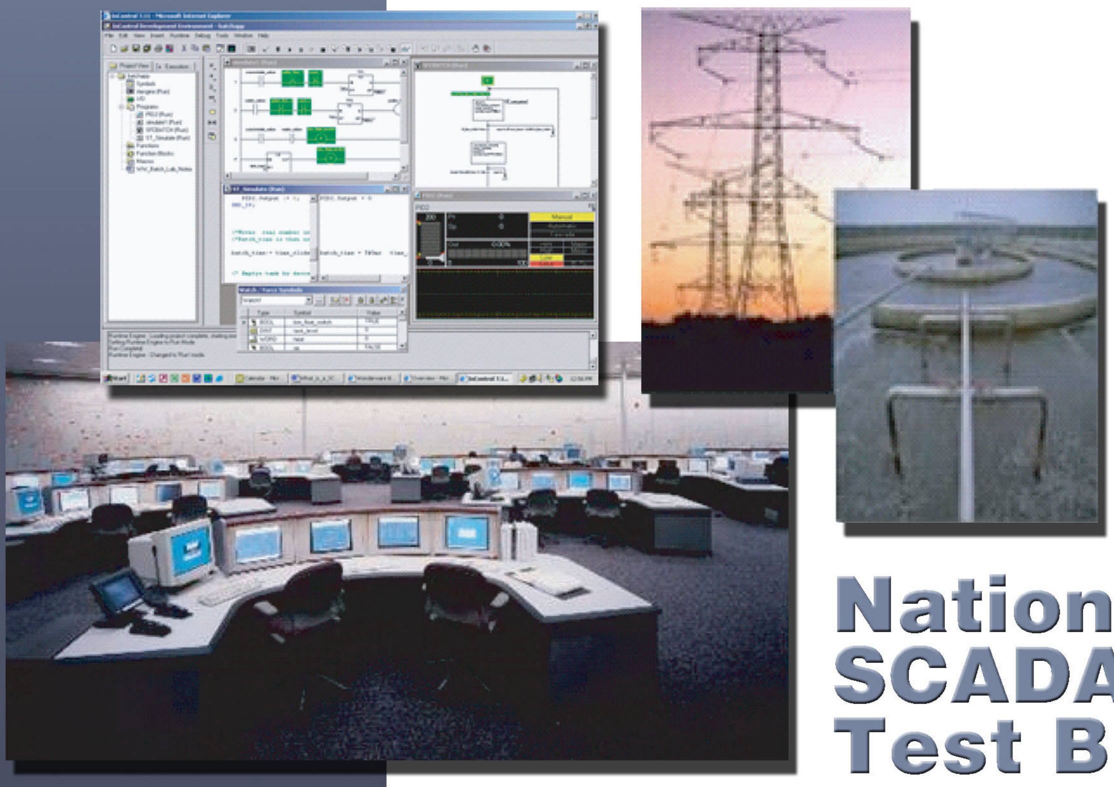
DOE Office of Electricity Delivery and Energy Reliability

A Summary of Control System Security Standards Activities in the Energy Sector

October 2005



National SCADA Test Bed

National SCADA Test Bed

A Summary of Control System Security Standards Activities in the Energy Sector

October 2005

Sandia National Laboratories
Idaho National Laboratory
Argonne National Laboratory
Pacific Northwest National Laboratory

Prepared for the
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

ABSTRACT

This document is a compilation of the activities and initiatives concerning control system security that are influencing the standards process in the development of secure communication protocols and systems. Also contained in this report is a comparison of several of the sector standards, guidelines, and technical reports, demonstrating standards coverage by security topic. This work focuses on control systems standards applicable to the energy (oil, gas, and electric, but not nuclear) sector.

AUTHOR CONTACTS

Rolf E. Carlson
Sandia National Laboratories[a]
Phone: 505.844.9476
E-mail: recarls@sandia.gov

Jeffery E. Dagle
Pacific Northwest National Laboratory[b]
Phone 509.375.3629
E-mail: jeff.dagle@pnl.gov

Shabbir A. Shamsuddin
Argonne National Laboratory[c]
Phone 630.252.6273
E-mail: shamsuddin@anl.gov

Robert P. Evans
Idaho National Laboratory[d]
Phone 208.526.0852
E-mail: Robert.Evans@inl.gov

[a] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

[b] The Pacific Northwest National Laboratory is operated by Battelle for the U.S. Department of Energy under Contract DE-AC05-76RL01830.

[c] Work supported by the U.S. Department of Energy under Contract No. W-31-109-ENG-38.

[d] Prepared for the U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability Under DOE Idaho Operations Office Contract DE-AC07-05ID14517.

ACKNOWLEDGMENTS

Department of Energy Laboratories

Thanks to Michael McLamore, Virgil Hammond, Victor Yarborough, and George Shaw from Argonne National Laboratories for their support of this effort.

Thanks to Kevin Robbins and Phillip Brittenham from Sandia National Laboratories for their contribution.

Industry

The CISSWG Team would like to thank the Standards and Industry Representatives for their candid comments and input to the report.

- American Gas Association – Kimberly Denbow, Engineering Services Director
- American Petroleum Institute – Thomas L. Frobase, Director, Network, SCADA & Automation Services, TEPPCO Partners
- Gas Technology Institute – Bill Rush
- International Electrotechnical Commission – Herb Falk, SISCO
- Instrumentation, Systems, and Automation Society – Joe Weiss, KEMA Consulting
- North American Electric Reliability Council – Thomas R. Flowers, Manager, Control Systems Division, Center Point Energy

University of Idaho

Thanks to Dr. Paul Oman and Jeannine Schmidt for initial research.

CONTENTS

ABSTRACT iii

ACKNOWLEDGMENTS vii

AUTHOR CONTACTS v

ACRONYMS xi

INTRODUCTION 1

SECTOR ORGANIZATIONS 3

Electric Power 3

Oil and Gas 3

Cross-Cut Organizations 3

CYBER AND CONTROL SYSTEM SECURITY STANDARDS 5

Electric Power 5

Oil and Gas 5

Cross-Cut Organizations 6

STATUS OF STANDARDS 7

IEEE 1402 – “IEEE Guide for Electric Power Substation Physical and Electronic Security” 7

IEC 62210 – “Data and Communication Security” 7

IEC 62351 – “Data and Communication Security” 7

IEC 62351-3 Security for Profiles Including TCP/IP 8
IEC 62351-4 Security for Profiles including MMS (ISO-9506) 8
IEC 62351-5 Security for IEC 60870-5 and Derivatives 8
IEC 62351-6 Security for IEC 61850 Profiles 8
IEC 62351-7 Objects for Network Management 9

NERC 1200 – “Urgent Action Standard 1200 – Cyber Security” 9

NERC 1300 – “Cyber Security” 9

NERC Security Guidelines – “Security Guidelines for the Electricity Sector” 10

FERC SSEMP – “Security Standards for Electric Market Participants” 10

API 1164 – “SCADA Security” 10

API – “Security Guidance for the Petroleum Industry” 11
API – “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries” 11

AGA 12 – “Cryptographic Protection for SCADA Communications General Recommendations” 11

AGA Report No. 12 Part 1. “Cryptographic Protection of SCADA Communications: Background, Policies & Test Plan” 11
AGA Report No. 12 Part 2. “Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications” 11
AGA Report No. 12 Part 3. “Cryptographic Protection of SCADA Communications: Protection of Networked Systems” 12
AGA Report No. 12 Part 4. “Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components” 12

ISA SP99 – “Manufacturing and Control System Security Standard” 12

NIST PCSRF – “Security Capabilities Profile for Industrial Control Systems” 13

ISO 15408 – “Common Criteria for Information Technology Security Evaluation” 13

ISO 17799 – “Information Technology – Code of practice for information security management” 13

CONCLUSIONS 19

REFERENCES 21

American National Standards Institute (ANSI) Standards 25

Federal Information Processing Standards (FIPS) 26

ISO/IEC Standards 27

IETF Request for Comments (RFC) 31

TABLES

1. Summary of Standards Status 14

2. Coverage of Each Standard. 15

ACRONYMS

AES	Advanced Encryption Standard
AGA	American Gas Association
AHWG06	Ad hoc working group 06
ASDU	Application-layer Service Data Unit
ANSI	American National Standards Institute
API	American Petroleum Institute
CIGRE	International Council on Large Energy Systems
CIP	Critical Infrastructure Protection
CISSWG	Critical Infrastructure Security Standards Working Group
CMIP	Common Management Information Protocol
COBIT	Control Objectives for Information and Related Technology
DCS	Distributed Control Systems
DHS	United States Department of Homeland Security
DNP	Distributed Network Protocol
DOE	United States Department of Energy
DoS	Denial-of-Service
DSS	Digital Signature Standard
FERC	Federal Energy Regulatory Commission
GOOSE	Generic Object Oriented Substation Event
GRI	Gas Research Institute
GSSE	Generic Substation Status Event
GTI	Gas Technology Institute
HAP	Host Access Protocol
HMAC	Hashed message authentication code

HV	High Voltage
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGT	Institute of Gas Technology
INEEL	Idaho National Engineering and Environmental Laboratory
INGAA	Interstate Natural Gas Association of America
INL	Idaho National Laboratory
ISA	Instrumentation, Systems, and Automation Society
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MAC	Message Authentication Codes
MIB	Management Information Base
MMS	ISO/IEC 9506 - Manufacturing Message Specification
NERC	North American Electric Reliability Council
NIST	National Institute of Standards and Technology
NSTB	National SCADA Test Bed
OE	Office of Electricity Delivery and Energy Reliability
PCSRF	Process Control Security Requirements Forum
PIN	Personal Identification Number
PSRC	Power Systems Relay Committee
SCADA	Supervisory Control and Data Acquisition
SMV	Sample Measured Values
SNMP	Simple Network Management Protocol

SPP	System Protection Profile
SSEMP	Security Standards for Electric Market Participants
TASE.2	Telecontrol Application Service Element Two
TC	Technical Committee
TC 57	Technical Committee 57 on Power System Control and Associated Communications
TLS	Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol
WAN	Wide Area Network
WG	Working Group
WG 15	Working Group 15 on Data and Communications Security

National SCADA Test Bed Program

A Summary of Control System Security Standards Activities in the Energy Sector

INTRODUCTION

In the U.S., systems that control critical energy infrastructure are vulnerable to physical and cyber attack, with potential consequences including significant interruption of economic activity or, even, to catastrophic loss of life. As the nation begins to take the necessary steps to remedy these vulnerabilities, a group is needed to assist in the shared understanding of standards activities in industry and in the standards-producing bodies. Without such shared understanding, results may be piecemeal, conflicting, and incomplete. It is also unlikely that adequate results could be accomplished in the time frame appropriate to the seriousness of the threat.

The National SCADA Test Bed (NSTB) Program, directed by the Department of Energy (DOE) – Office of Electricity Delivery and Energy Reliability (OE), is tasked with assisting industry and government in improving the security of energy sector control systems. As part of that mission, the NSTB Program funded the Critical Infrastructure Security Standards Working Group (CISSWG) to identify industry standards applicable to control system security and to perform an initial evaluation of the scope and status of those standards. The CISSWG is DOE-sponsored working group composed of representatives of four national laboratories. It has a charter to consider energy sector cyber security standards. Included in this sector are electrical power and oil and gas. There are many professional bodies that represent interests in the energy sector, but only a few have been identified as dealing with cyber or control system security. There are also other professional bodies that represent interests that complement those in the energy sector.

This report documents the current state of information within the CISSWG concerning cyber and control system security standards. This report endeavors to answer four questions:

1. Which standards organizations or professional bodies are documenting work that could eventually contribute to a standard for the cyber security of communication and control in the energy sector?

2. Which standards documents that address cyber security for the energy sector are of greatest interest?

3. What is the status of each document, i.e., in process, in review, completed, etc.?

4. How do these standards documents compare to one another?

The CISSWG recognizes that additional information is needed to fill in many of the gaps concerning these control system cyber security standards. This information will be gathered through continued review of the standards, interfacing with the standards organizations, and through interviewing subject-matter experts.

Several previous authors have looked into identifying the activities of the standards community. Singer[1] identified a collection of standards organizations and noted that most of the documents were in the formative stages, with difficult, unresolved technical problems, including: electronic perimeter security, periodic assessments, personnel background checks, control system security policies, event identification and disclosure, and recovery plans. Idaho National Laboratory (INL) produced four reports covering standards in the electric power sector,[2] oil and gas sector,[3] cross-sector,[4] and 13 critical infrastructures identified by the Department of Homeland Security (DHS).[5] Preparation of this report has been fully integrated with these related efforts at INL to preclude redundant actions and ensure maximum sharing of standards-related information. In the Sector Organizations section of this document, we identify the organizations most active in the standards process for energy communications and control security. In the subsequent section on Cyber and Control System Security Standards, we identify the documents most relevant for the standards process associated with communication and control security in energy. In the third major section, titled: Status of Standards, an overview is provided, initially in paragraph form, and then as tables, of the status and relative state of each standard.

SECTOR ORGANIZATIONS

The professional organizations that deal with cyber or control system security standards considered in this report are grouped by sector, followed by those that cross-cut several sectors.

Electric Power

In the electric power sector, excluding nuclear power and distributed energy, there are several organizations that are involved in cyber security standards:

IEEE	Institute of Electrical and Electronic Engineers
IEC	International Electrotechnical Commission
NERC	North American Electric Reliability Council
CIGRE	International Council on Large Energy Systems
FERC	Federal Energy Regulatory Commission
PSRC	Power Systems Relay Committee

Oil and Gas

In the oil and gas sector, several organizations that are involved with cyber security standards were identified:

API	American Petroleum Institute
AGA	American Gas Association
IGT*	Institute of Gas Technology
GRI*	Gas Research Institute
GTI	Gas Technology Institute
INGAA	Interstate Natural Gas Association of America

* Note that IGT and GRI are no longer in existence, and some former roles of the organization are now handled by GTI.

Cross-Cut Organizations

There are several professional organizations that cut across multiple sectors:

ANSI	American National Standards Institute
ISA	Instrumentation, Systems, and Automation Society
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology

CYBER AND CONTROL SYSTEM SECURITY STANDARDS

Standards for this analysis were selected based on the best available knowledge of the CISSWG at the time. No effort was made to rank these standards as to usefulness to industry or to the type of standard. There are recognized differences in standards aimed at the manufacturing section, as opposed to those for energy distribution. There are also differences between technical and operating standards, and most of the cyber security standards fall into the operating standards category. Most good standards are based on best practices developed by asset owners/operators.

The following standards and guidelines deal with cyber or control system security. Because, in many cases, guidelines published by an organization are considered comparable in significance to published standards, they are included here as well. A brief description of each of these standards is presented, along with the current position of the standard. This is not an exhaustive list of the standards, but it is believed to include those that are most relevant to energy sector control system security. These standards are listed by sector.

Electric Power

IEEE 1402	"IEEE Guide for Electric Power Substation Physical and Electronic Security"
IEC 62210	"Initial Report from IEC TC 57 ad-hoc WG06 on Data and Communication Security"
IEC 62351	"Data and Communication Security"
NERC 1200	"Urgent Action Standard 1200 – Cyber Security"
NERC 1300	"Cyber Security," also known as CIP-002-1 through CIP-009-1
NERC Security Guidelines	"Security Guidelines for the Electricity Sector"
FERC SSEMP	"Security Standards for Electric Market Participants (SSEMP)."

Oil and Gas

API 1164	"SCADA Security"
API	"Security Guidance for the Petroleum Industry"
API	"Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries"
AGA Report No. 12 Part 1	"Cryptographic Protection of SCADA Communications Background, Policies & Test Plan"
AGA Report No. 12 Part 2	"Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications"
AGA Report No. 12 Part 3	"Cryptographic Protection of SCADA Communications: Protection of Networked Systems"
AGA Report No. 12 Part 4	"Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components."

Cross-Cut Organizations

ISA SP99	“Manufacturing and Control System Security Standard”
NIST PCSRF	“Security Capabilities Profile for Industrial Control Systems”
ISO 15408	“Common Criteria for Information Technology Security Evaluation”
ISO 17799	“Information Technology – Code of practice for information security management.”

STATUS OF STANDARDS

IEEE 1402 – "IEEE Guide for Electric Power Substation Physical and Electronic Security"

IEEE 1402-2000 is a guide sponsored by the Power Engineering Society/Substations of IEEE. It was approved June 7, 2000. The guide identifies and discusses security issues related to human intrusion at electric power supply substations. Various methods and techniques that are being used to mitigate both physical and electronic intrusions are also presented.[6]

IEC 62210 – "Data and Communication Security"

IEC report 62210, "Data and Communications Security," was developed and circulated in 1999 throughout the IEC as the initial report of IEC TC 57 AHWG06. As a result of the report, AHWG06 was formalized into Working Group (WG) 15 on Data and Communications Security. The report was published in the IEC as technical report 62210 in April, 2003.

The report was broad in scope, including security definitions, stakeholder identification, consequence analysis, threats and prioritization of threats, attacks, policy, a "Common Criteria" protection profile, and consequence analysis. Consequence analysis was adopted in the report as the security methodology for prioritization of assets and threats to the security of the TC 57 protocols. Consequence analysis was combined with "Common Criteria," ISO/IEC 15408 to develop an example protection profile for a cryptographic communications channel between a master station and a substation that served to illustrate the development of a security specification.

AHWG06 issued the report, making the recommendation to establish a permanent WG 15 with the following tasks:

1. Use consequence analysis combined with ISO 15408 to develop security specifications

2. Focus on the application layer

3. Address key management

4. Address end-to-end security.

It was later discovered that key management and end-to-end security, or system-level security, were difficult topics that were not resolvable with the resources available at the time. The recent WG15 activities found in IEC 62351, "Data and Communication Security," are beginning to remedy some of these deficiencies.

IEC 62351 – "Data and Communication Security"

Many of the new work items currently under development by IEC TC 57 WG 15 are being incorporated into a document known as IEC 62351. There are seven sections to IEC 62351: "Data and Communications Security," with sections 3-7 containing the new work items.

Part 1: Introduction

Part 2: Glossary

Part 3: Security for profiles including TCP/IP

Part 4: Security for profiles including MMS

Part 5: Security for IEC 60870-5 and derivatives (DNP)

Part 6: Security for IEC 61850 profiles

Part 7: Objects for Network Management

IEC 62351-3 Security for Profiles Including TCP/IP

Because many TC 57 communication profiles are based on the Transmission Control Protocol/Internet Protocol (TCP/IP), a common security solution is being investigated. The use of Transport Layer Security (TLS) in order to secure IEC TC57 protocols and their derivatives is being considered. Issues include roles in renegotiation of keys, certificate revocation, certificate sizes, and certificate field. These will be standardized to ensure interoperability.

IEC 62351-4 Security for Profiles including MMS (ISO-9506)

Two protocols make use of the Manufacturing Message Specification (MMS), ISO/IEC 9506, as the application-level protocol: (1) IEC 60870-6, “Telecontrol Application Service Element 2,” (TASE.2) (IEC TC57 WG15 and IEC TC57 WG07 are standardizing their security) and (2) IEC 61850. The consistent use of security across these two standards is being developed and supported through IEC 62351-4, building upon IEC 62351-3 by adding application-level authentication.

IEC 62351-5 Security for IEC 60870-5 and Derivatives

IEC 62351-5 is a standard that is being developed to secure IEC 60870-5 and its derivatives. Derivates, in this case, means DNP3. The threats to be addressed include spoofing, modification of packets, message replay, and to some extent denial of service. Primary design principles are that authentication of the communication is done at the application layer only, authentication is bi-directional, a challenge/response model will be followed, default pre-shared keys will be used when necessary, and non-secure systems will be supported. Authentication will be provided by HMAC (hashed message authentication code). The hash will be based upon the entire length of the message, protocol-specific addressing information, challenged ASDU, HMAC session key, and padding data as required by the protocol. The direction in which the working group is headed implies: 1) that TCP/IP will be used natively for DNP3, and 2) that an out-of-band network will exist to support cryptographic key exchanges. The work order is approaching committee draft form. 62351-5 builds upon IEC 62351-3, adding application-level authentication capability.

IEC 62351-6 Security for IEC 61850 Profiles

IEC 61850 is an emerging standard entitled: “Communication networks and systems in substations.” The standard consists of 14 sections, each in various stages of approval/release. One of the effects of this standard, when a complete set of IEC 61850 products is available, is that all the substation equipment will form one integrated system. This system comprises, for example, instrument transformers, protective relays, control systems, and also HV-switchgear that is controlled and supervised using the IEC 61850 process and station bus. Measurements from the instrument transformers, as well as trip commands from the protection relays, will make use of the communication network. There is discussion within the IEC that 61850 should be expanded beyond the substation in order to serve communication and control needs of the power system from the master station down to the switchgear.

The object-oriented data model of IEC 61850 defines all objects in the substation that communicate with each other. These so-called Logical Nodes contain the data and attributes of the respective objects. In addition, this part contains a device model that describes the function allocation, as well as the properties, of each physical device. Clear rules facilitate extensions in applications.[7]

To implement and use communication profiles of IEC 61850 in nonsecure environments, security enhancements are required. Security for five IEC 61850 profiles is being developed and packaged into IEC 62351-6: Client/Server (using TLS and MMS), GOOSE (analogue and digital multicast primarily for protective relaying), GSSE, GSSE Management, and Sample Measured Values (SMV). IEC 62351-6 references IEC 62351-5.

IEC 62351-7 Objects for Network Management

IEC 62351-7 is being developed to support management information base (MIB) requirements for end-to-end network management, a step towards system-level security. Standardized network management object definitions will facilitate intrusion detection, security infrastructure management, and audit capabilities. End-to-end security requires management of communication networks, network devices, and end devices. MIB data will support the monitoring of network state-of-health through the ISO Common Management Information Protocol (CMIP) and the Internet Engineering Task Force (IETF) Simple Network Management Protocol (SNMP) standards for network management. Utility power system operations will be supported through the development of MIB data that is mapped to IEC 61850, IEC 60970-5, and IEC 60970-6.

NERC 1200 – "Urgent Action Standard 1200 – Cyber Security"

North American Electric Reliability Council (NERC), recognized as the energy sector coordinator by FERC, DOE, and DHS, developed the "Urgent Action Cyber Security Standard" (NERC 1200) as a temporary standard to establish a set of defined security requirements related to the energy industry and to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets. This standard was adopted August 13, 2003, for a one-year period. It has received an extension, until August, 2006,[e] at which point permanent Cyber Security Standards, CIP-002-1 through CIP-009-1 (previously identified as [draft] NERC 1300) are expected to be released.[8,9]

NERC 1200 applies to entities performing various electric system functions, as defined in the functional model approved by the NERC Board of Trustees in June, 2001. NERC is now developing standards and procedures for the identification and certification of such entities. Until the identification and certification are complete, these standards apply to the existing entities (such as control areas, transmission owners and operators, and generation owners and operators) that are currently performing the defined functions.[10]

NERC 1300 – "Cyber Security"

At the start of this project, the current draft NERC standard was Draft Version 1 of NERC 1300. This is the document that was reviewed. The current draft NERC cyber security standard, CIP-002

[e] On August 2, 2005, NERC 1200 was extended until August 13, 2006, or until CIP-002 – CIP-009 takes effect.

through CIP-009, when released, will replace NERC 1200, “Urgent Action Cyber Security Standard.” These standards are in the review process by the North American Electric Reliability Council. The first drafts of these standards were released for review on September 15, 2004; review comments submitted on the third draft are now in review by the standards committee. These standards are expected to cover essentially the same material as NERC 1200, but in more detail.[11]

NERC Security Guidelines – “Security Guidelines for the Electricity Sector”

The “NERC Security Guidelines for the Electrical Sector” is a 73-page document published by the North American Electric Reliability Council. Version 1.0 was released on June 14, 2002. The guideline consists of 14 sections addressing both physical and cyber security.[12]

These guidelines describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems. These guidelines are advisory in nature, and each user determines how they will be used.[13]

FERC SSEMP – “Security Standards for Electric Market Participants”

The “Federal Energy Regulatory Commission (FERC) Security Standards for Electric Market Participants (SSEMP) Notice of Proposed Rulemaking[14]” was published in July of 2002. Currently, there is uncertainty as to when the final rule will be published and what the implementation schedule will be; however, it is mandated for all electric market participants. FERC SSEMP establishes minimum standards focusing on “electronic systems, which include hardware, software, data, related communication networks, control systems as they impact the grid market, and personnel[15].” Since this standard does not address either control systems or critical infrastructure, it is not addressed further.

API 1164 – “SCADA Security”

The SCADA security standard, API 1164, first edition was released in September, 2004, and is available to the industry. This standard on SCADA security provides guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document is not limited to pipelines regulated under Title 49 CFR 195.1, but should be viewed as a long listing of best practices to be employed when reviewing and developing standards for a SCADA system.[16]

The API standard, to date, applies only to pipeline operators and does not cover refineries. Previously released cyber-security guidelines are considered by API to be adequate for refineries at this time. Although the standard does address physical security, the primary thrust of this document is cyber security and access control. This document embodies "API Security Guidelines for the Petroleum Industry," and is specifically designed to provide the operators with a description of industry practices in SCADA security and to provide the framework needed to develop sound security practices within the operator’s individual companies.

API 1164 addresses access control, communication security (including encryption), information distribution classification, physical issues (including disaster recovery and business continuity plans), operating systems, network design, data interchange between enterprise and third-party support/customers, management systems, and field devices configuration and local access.[17]

API – “Security Guidance for the Petroleum Industry”

API’s second edition of “Security Guidance for the Petroleum Industry” is now in use at oil and gas facilities around the world to help managers decide how to deter terrorist attacks. Covering all segments of the industry, this guidance builds on the existing solid foundation of design and operational regulations, standards, and recommended practices, which relate to facility design and safety, environmental protection, emergency response, and protection from theft and vandalism.[18]

API – “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries”

The American Petroleum Institute and the National Petrochemical & Refiners Association jointly developed a new methodology for evaluating the likelihood and consequences of terrorist attacks against refineries and petrochemical facilities. “Security Vulnerability Assessment Methodology for Petroleum and Petrochemical Facilities” is designed for companies to use in assessing vulnerabilities and potential damages from different kinds of terrorist attacks.[19]

AGA 12 – “Cryptographic Protection for SCADA Communications General Recommendations”

AGA Report No. 12 is a series of documents recommending practices designed to protect SCADA communications against cyber attacks. AGA Report No. 12 is the result of the combined efforts of several gas-related organizations: Institute of Gas Technology, Gas Research Institute, Gas Technology Institute, and American Gas Association. The AGA 12 Part 1 (draft 3 revision 6) report was released on August 14, 2004, for industry review and comments.[20] A final version is expected to be out by the end of 2005. Work on subsequent parts is pending public and private research funding.

AGA 12 focuses on securing the communication link between the field devices and the control servers in the control center. The recommended practices are designed to provide confidential and authentic SCADA communications.

Note that AGA 12 is a voluntary standard and does not mandate any companies to install encryption technology as recommended in the standard. Recommendations included in this report apply to some Distributed Control Systems (DCS). Because gas, water, wastewater, electric, and pipeline SCADA systems have many commonalities, most of the recommendations of the AGA 12 series apply to all of these systems.

AGA Report No. 12 Part 1. “Cryptographic Protection of SCADA Communications: Background, Policies & Test Plan”

This document contains the background, security policy fundamentals, and a test plan that generally apply to all areas of cryptographic protection of SCADA systems.

AGA Report No. 12 Part 2. “Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications”

This document focuses on retrofit link encryption for asynchronous serial communications. It contains the functional requirements and detailed technical specifications for AGA-12-compliant retrofit devices.

AGA Report No. 12 Part 3. “Cryptographic Protection of SCADA Communications: Protection of Networked Systems”

This document will focus on high-speed communication systems, including the Internet.

AGA Report No. 12 Part 4. “Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components”

This document will focus on protecting SCADA systems by incorporating cryptography into system components at the time of manufacture. Work on this standard is expected to begin in late 2005.[17,21]

AGA 12 standards do not protect against an attack from a compromised field site or control center if the attack takes place outside the limits of the encrypting/decrypting software. The encryption module would treat spurious data as legitimate, and the attack would be encrypted. The standard does protect against someone hijacking or modifying the communication channel.

The standards group is still working on defining key management, including key generation and destruction.

Requirements for the layers of security not addressed by the AGA 12 series consist of the following:

1. Protect the operating system files.

2. Protect the application code that interacts with the database.

3. Control connections to the database.

AGA 12 does not address the interdependencies of networks—interdependencies of one network (e.g., a gas system) on another network (such as an electric grid or a communication network) are a very broad and complex problem. The complete treatment of this set of questions is beyond the current scope of the AGA 12 series.

AGA 12 series does not address denial-of-service (DoS) caused by cyber attack because the cryptographic solutions cannot mitigate this attack. The standard does provide guidelines for SCADA cyber security and security of the SCADA integration with corporate WAN/LAN systems. The standard provides best practices of cyber security, social engineering, physical security, and developing security policies and procedures.

ISA SP99 – “Manufacturing and Control System Security Standard”

The ISA-SP99 Committee was formed in October, 2002, and to date has issued two technical reports dealing with control system security. The committee, comprised of four working groups, is in the process of preparing a standard for manufacturing and control system security. There is no publication date forecast at this time. The committee’s focus is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and provide criteria for procuring and implementing secure control systems. The committee plans to establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices, and for assessing electronic security performance.[22]

The technical reports incorporate a great deal of information from other security standards and publications and add information specific to control systems. These technical reports are useful for identifying issues to consider and security options. They are not standards with well defined requirements that can be tested, certified, or included in RFPs.[23]

NIST PCSRF – "Security Capabilities Profile for Industrial Control Systems"

The Process Control Securities Requirements Forum (PCSRF) has prepared a System Protection Profile (SPP) to formally state security requirements associated with industrial control systems (ICS). This document discusses security issues and capabilities relevant to those regarded as components of the national critical information infrastructure. The document defines security capabilities that would exist in electronic programmable components that comprise an industrial control system.[24]

The document is intended to provide an ISO 15408-based starting point in formally stating security requirements associated with ICS. It directs users to review the "Common Criteria" document (ISO 15408, see below) for further guidance in securing control systems. The SPP has been written in such a way that it may be used as the basis for preparing a system security target for a specific ICS or as the basis for a more detailed SPP for a sub-class of ICS, such as a SCADA.

ISO 15408 – "Common Criteria for Information Technology Security Evaluation"

Version 2.2 of the "Common Criteria for Information Technology Security Evaluation" was published in January, 2004, by ISO. The Common Criteria are presented as a set of three distinct but related parts: the Introduction and General Model (Part 1), the Security Functional Requirements (Part 2), and the Security Assurance Requirements (Part 3). These define general concepts and principles of information technology (IT) security evaluation and a general model of evaluation. They also set out a standard way of expressing functional requirements and a set of assurance components as a way of expressing assurance requirements.[25]

The standard does not particularly discuss cryptographic designs and uses in terms of communication and control applications.

ISO 17799 – "Information Technology – Code of practice for information security management"

The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799: "Information Technology – Code of Practice for Information Security Management," (ISO 17799)[26] is an international guideline addressing organizational information security management. The intent of ISO/IEC 17799 is to give direction to organizations in developing their own proprietary security guidelines.

ISO 17799 is employed later in Tables 2 and 3 as a metric to support comparison of the coverage of various standards.

Table 1 summarizes the status and the focus of the various documents described in this section.

Table 1. Summary of Standards Status

	Standard	Final	Control System Focus	Detailed Technical Specifications
IEEE 1402		✓	✓	
IEC 62210		✓	✓	
IEC 62351	✓		✓	✓
NERC 1200	✓	✓	✓	
NERC 1300	✓		✓	
NERC Security Guidelines		✓	✓	
API 1164	✓	✓	✓	
AGA 12	✓		✓	✓
ISA TR99	✓		✓	✓
NIST PCSRF		✓	✓	
ISO 17799	✓	✓		
ISO 15408	✓	✓		

The standards, guidelines, and technical reports (documents) considered in this report provide recommendations for information/control system security management for use by those responsible for initiating, implementing, or maintaining security in their organization.

Table 2 provides a comparison of several of the documents considered in this report. By examining this table, it is possible to see which section of a particular document addresses which recommendation. International Standard ISO/IEC 17799 was used as the baseline because it has been considered as a baseline by others[1,2,3] and is the starting point for other cyber security standards. Three reports,[2,3,4] along with information received from organization reviewers, were used to populate this table. Since all the documents do not address the same recommendations, it is recognized that there will be areas where there are no comparisons. For example, AGA 12 is geared more toward encryption for the purpose of authenticating data transfer within the (SCADA) control system network, while the API 1164 focus is on pipeline control system security by listing the processes used to identify and analyze the SCADA system vulnerabilities, providing a comprehensive list of practices to harden the core architecture, and providing examples of industry best practices. The ISO/IEC standard considers the network, operating system, and application separately, and looks at recommendations such as passwords for each of these individually. These varying areas of content and focus among the standards required judgment in making the comparisons summarized in Table 2.

Table 2. Coverage of Each Standard.

	ISO 17799	API 1164	IEEE 1402	AGA Report No. 12[f]	NERC Security Guideline	NERC 1200	NERC 1300[g]	ISA TR99-01	ISA TR99-02	PCSRF	IEC 62210	IEC 62351
SECURITY POLICY												
Information security policy.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VULNERABILITY AND RISK ASSESSMENT												
Vulnerability and risk assessment.				✓	✓		✓	✓	✓	✓		
ORGANIZATIONAL SECURITY												
Information security infrastructure.	✓		✓	✓	✓	✓	✓		✓	✓	✓	
Security of third party access.	✓	✓		✓	✓		✓		✓	✓	✓	
Outsourcing.	✓				✓		✓				✓	
ASSET CLASSIFICATION AND CONTROL												
Accountability for assets.	✓					✓	✓	✓	✓	✓	✓	
Information classification.	✓	✓						✓	✓		✓	
PERSONNEL SECURITY												
Security in job definition and resourcing.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
User training.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Responding to security incidents and malfunctions.	✓	✓		✓	✓	✓	✓		✓	✓		
Threat response (enhanced security) related to announced threat levels.					✓		✓					✓
Personnel Qualifications		✓										

[f] Draft 3 , August 14, 2004

[g] Draft 1.0, Sept. 15, 2004

	ISO 17799	API 1164	IEEE 1402	AGA Report No. 12[f]	NERC Security Guideline	NERC 1200	NERC 1300[g]	ISA TR99-01	ISA TR99-02	PCSRF	IEC 62210	IEC 62351
PHYSICAL AND ENVIRONMENTAL SECURITY												
Secure areas.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Other physical security methods.		✓	✓		✓		✓					
Equipment security.	✓	✓			✓		✓	✓	✓	✓		
General controls (information and information processing facilities).	✓				✓			✓				
COMMUNICATIONS AND OPERATIONS MANAGEMENT												
Operational procedures and responsibilities.	✓	✓		✓	✓		✓	✓	✓		✓	
System planning and acceptance.	✓					✓	✓		✓		✓	
Protection against malicious software.	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Housekeeping.	✓				✓		✓		✓			
Network management.	✓	✓		✓	✓	✓	✓	✓	✓		✓	
Media handling and security.	✓	✓		✓		✓	✓	✓	✓			
Exchanges of information and software.	✓	✓			✓				✓			
Availability		✓			✓		✓			✓	✓	✓
ACCESS CONTROL												
Business requirements for access control.	✓	✓			✓			✓		✓		
User access management.	✓	✓		✓	✓	✓	✓	✓	✓	✓		
User responsibilities.	✓	✓	✓	✓	✓		✓		✓	✓		
Network access control.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Operating system access control.	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Application access control.	✓								✓			

	ISO 17799	API 1164	IEEE 1402	AGA Report No. 12[f]	NERC Security Guideline	NERC 1200	NERC 1300[g]	ISA TR99-01	ISA TR99-02	PCSRF	IEC 62210	IEC 62351
Monitoring system access and use.	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Mobile computing and teleworking considerations.	✓	✓			✓			✓	✓			
Field Device Access		✓			✓			✓	✓		✓	
SYSTEMS DEVELOPMENT AND MAINTENANCE												
Security requirements of systems.	✓	✓			✓	✓	✓	✓	✓		✓	✓
Security in application systems.	✓					✓	✓	✓	✓		✓	✓
Cryptographic controls.	✓	✓	✓	✓	✓			✓	✓		✓	✓
SCADA Cryptographic system component requirements				✓				✓			✓	✓
SCADA Cryptographic system performance requirements				✓								✓
SCADA Cryptographic system design goals				✓				✓			✓	✓
Key management.				✓	✓		✓	✓			✓	✓
Security of system files.	✓			✓			✓					✓
Security in development and support processes.	✓					✓	✓	✓	✓			
Security patch management.	✓	✓			✓		✓	✓	✓			
BUSINESS CONTINUITY MANAGEMENT												
Aspects of business continuity management.					✓		✓			✓		
SCADA System Compliance Requirements.	✓	✓			✓	✓	✓		✓	✓		

	ISO 17799	API 1164	IEEE 1402	AGA Report No. 12[f]	NERC Security Guideline	NERC 1200	NERC 1300[g]	ISA TR99-01	ISA TR99-02	PCSRF	IEC 62210	IEC 62351
COMPLIANCE												
Compliance monitoring process (compliance with standard).						✓	✓		✓			
Inspection of facilities.						✓	✓		✓			
Compliance with legal requirements.			✓				✓	✓		✓		
Reviews of security policy and technical compliance.	✓						✓	✓	✓	✓		
System audit considerations.	✓						✓	✓	✓	✓	✓	✓
CRYPTOGRAPHIC SYSTEM TEST PLAN												
Cryptographic System Test Plan.			✓	✓								✓

CONCLUSIONS

We identified a mosaic of security coverage areas for communication and control standards and guidelines in energy. Contributing to this mosaic, the CISSWG found 16 organizations of primary interest that were documenting work that would eventually contribute to a standard for cyber security of communication and control in the energy sector. Associated with these 16 organizations, are 12 sets of documents, in various stages of development that are of greatest interest to the energy sector.

When the documents were summarized in Table 1, we determined that the documents were either detailed technical descriptions, or final, but not both. This may suggest that there are technical issues that require resolution prior to finalizing each standard. One future activity could be to isolate the technical problems that most need to be solved by the standards community, and support the development of solutions to these problems so that the standards can be finalized. Technology gaps will sometimes need to be addressed before policy and best practices can be put in place, for example the development of protocol-aware firewalls for communication and control.

These documents were compared in Table 2 against a superset of ISO 17799 for coverage and completeness. From Table 2, it appears that similar problems are being addressed by different organizations. An important future activity could be to isolate the commonalities between problems that are being addressed by the identified standards organizations and look for areas of overlap and mutual support. Joint standards teams focused on the solution to a common problem might be more effective than a single organization alone. One mechanism for achieving the twin goals of precise problem identification and standards activity overlap could be an industry road-mapping process. It is recommended that such an activity be undertaken for industry.

Because the liaison activity of each standards organization has historically been limited, the CISSWG could support the activities of these joint technical teams as a catalyst for better communication, as well as being able to reach into the National Laboratories for support in solving difficult technical problems.

There are several additional questions that could be answered in follow-on activity:

Question 1: In what ways do system-level communication and control security standards depend on other standards, such as those listed in Appendix B? A systems-level communication and control security standard will rely upon other documents, such as cryptographic standards and media standards used in wireless communications, and may draw from other well developed security architectures from other fields, such as banking and finance. The universe of applicable standards that can be drawn from and their associated assurance levels needs to be identified.

Question 2: What is the best metric for comparing standards? ISO 17799 may not be the best metric for comparison; a revised metric that includes contributions from COBIT (Control Objectives for Information and Related Technology) might serve as well or better. Further work could include the development of such a metric.

Question 3: What are the assurance levels (i.e., assurance requirements as defined by Common Criteria) needed to mitigate the threats faced by communication and control systems and how do these assurance levels meet the needs of business and government?. It is recommended that once a precise problem set has been identified for communication and control standards, that associated assurance levels be developed.

Question 4: What is the business case for security and assurance of communication and control standards? Having the business case and a cost/benefit methodology for security investment will be important to justify increasing the security level.

Question 5: What is the method for a system-of-systems description in support of security specification development, such as common criteria protection profiles? One hypothesis for the difficulty in gaining greater acceptance with the common criteria is the lack of a generally agreed upon system description by the stakeholders, some of whom are non-technical. An improved system description may make it easier to apply diverse teams of analysts to solve assurance problems for communication and control.

Question 6: What is the means for specifying and measuring end-to-end, or system-level, security? IEC TC 57 WG 15 is starting to answer this question with IEC 62351; however, there is currently no agreed-upon definition of a systems-level solution for security in communication and control standards. The development of a common-criteria protection profile that packages many of the requirements from the standards identified in this document might be a means for developing such a system-level description.

Question 7: How will the trend towards automation affect the security process? It is not clear which requirements are most important to support the trend towards fully automated communication and control networks for energy. Plug and Play and seamless security are two often discussed requirements, but little attention has been given to investigating the security implications of these directions.

Question 8: Can a security standard be developed for heterogeneous legacy systems? Control systems are engineered on site over many years, so the requirements must reflect the age and implementation restrictions. Most standards are forward-looking, however, given that the installed base of communication and control systems has a lifespan of 10-15 years, sometimes as long as 25 years, is there a mechanism for addressing the security of older systems?

REFERENCES

1. Singer, Bryan L., "Security Standards, Those Available Today and Future Directions," *ISA Expo 2004, Houston, Texas, October 4, 2004*

2. INEEL, *A Comparison of Electrical Sector Cyber Security Standards and Guidelines*, Idaho National Engineering and Environmental Laboratory, INEEL/EXT-04-02428, November 2, 2004

3. INEEL, *A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment*, Idaho National Engineering and Environmental Laboratory, INEEL/EXT-04-02462, November 5, 2004

4. INL, *A Comparison of Cross-Sector Cyber Security Standards*, Idaho National Laboratory, INL/EXT-05-00656, September, 2005

5. INEEL, *Standards – Status and Path Forward*, Idaho National Engineering and Environmental Laboratory, INEEL/EXT-04-02425, October 19, 2004

6. IEEE, IEEE Standard 1402-2000, IEEE Guide for Electric Power Substation Physical and Electronic Security. New York: IEEE, Inc.

7. IEC TC 57 Power System Control and Associated Communications, Draft IEC 61850, Communication Networks and Systems in Substations, http://www.nettedautomation.com/standardization/IEC_TC57/WG10-12/iec61850/61850_on_a_page.html

8. NERC, Urgent Action Standard 1200 Cyber Security, ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStnd-3-3121.pdf

9. NERC, "NERC Approves Extension of Urgent Action Cyber Security Standard," *NERC News*, September 8, 2004, http://www.nerc.com/~filez/nercnews/news-0804c.html

10. Breakwater Security, "Key Energy and Utility Security Questions, What is the NERC 1200 Urgent Action Cyber Security Standard?," Breakwater Security Associates, http://www.breakwatersecurity.com/energy/key_questions.html?id=2

11. Standard 1300 — "Cyber Security," ftp://ftp.nerc.com/pub/sys/all_updl/standards/sar/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf

12. NERC, "Securing Remote Access to Electronic Control and Protection Systems," NERC Security Guideline (10 June 2003, Version 1.0), http://www.esisac.com/library-guidelines.htm

13. NERC, "Security Guidelines for the Electricity Sector, Overview, Version 1.0," http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf

14. U.S. Federal Energy Regulatory Commission, *Security Standards for Electric Market Participants,* 18 CFR Part 35, Docket No. RM01-12-000, Notice of Proposed Rulemaking, Appendix G.

15. U.S. Federal Energy Regulatory Commission, *Security Standards for Electric Market Participants,* 18 CFR Part 35, Docket No. RM01-12-000, Notice of Proposed Rulemaking, Appendix G.: National Security Telecommunications Advisory Committee Information Assurance Task Force, *Electric Power Risk Assessment*, March 1997, http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html (5 March 2004)

16. API Publications Catalog, pg. 53 (copyright 2005) http://api-ep.api.org/filelibrary/Catalog_web.pdf

17. Fisher. R, July 29, 2004, “Supervisory Control and Data Acquisition (SCADA) Systems White Paper,” prepared by Argonne National Laboratory for DPO.

18. API Publications Catalog, pg. 54 (copyright 2005) http://api-ep.api.org/filelibrary/Catalog_web.pdf

19. API Publications Catalog, pg. 54 (copyright 2005) http://api-ep.api.org/filelibrary/Catalog_web.pdf

20. AGA 12 Working Document Collaboration Area, http://www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml (2 of 2), 9/22/2004 11:26:54 AM

21. Website: AGA 12 Working Document Collaboration Area -*Welcome to your AGA 12 Cryptographically Protected SCADA Communications Working Document Collaboration Area* (Source: http://www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml [8/18/2004 2:02:03 PM]

22. ISA web page, www.isa.org

23. ISA SP99, http://www.digitalbond.com/SCADA_security/SP99.htm

24. Process Control Security Requirements Forum (PCSRF), http://www.isd.mel.nist.gov/projects/processcontrol/

25. The Common Criteria, Evaluation and Validation Scheme, http://niap.nist.gov/cc-scheme/cc_docs/index.html

26. ISO/IEC 17799:2000, Information Technology – Code of Practice for Information Security Management. <http://www.iso.ch/iso/en/prods-services/ISOstore/store.html> (5 March 2004).

Appendix A

Related Information Technology Standards

Appendix A

Related Information Technology Standards

The following references are examples of additional information technology documents and standards that should be considered for a more complete communication and control standards-based solution. Many of these standards may be employed as foundational elements in developing systems-level specifications. As such, the assurance levels accorded to the system specification will depend upon the assurance levels provided by the constituent components. It will, therefore, be necessary to eventually consider the appropriateness of many of these standards in developing standards-based system solutions for communication and control security.

American National Standards Institute (ANSI) Standards

ANSI standards may be ordered online at http://webstore.ansi.org/ansidocstore/

Designation	Title
ANSI X3.92	"Data Encryption Algorithm."
ANSI X3.106	"Data Encryption Algorithm – Modes of Operation."
ANSI X9.8	"Banking - Personal Identification Number Management and Security; Part 1: Pin Protection Principles and Techniques for Online Pin Verification in ATM & POS Systems."
ANSI X9.17	"Financial Institution Key Management (Wholesale)."
ANSI X9.19	"Financial Institution Retail Message Authentication."
ANSI X9.23	"Financial Institution Encryption of Wholesale Financial Messages."
ANSI X9.24	"Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques."
ANSI X9.26	"Financial Institution Sign-On Authentication for Wholesale Financial Transactions."
ANSI X9.28	"Financial Institution Multiple Center Key Management (Wholesale)."
ANSI X9.30.1	"Public Key Cryptography for the Financial Services Industry – Part 1. The Digital Signature Algorithm (DSA)."
ANSI X9.30.2	"Public Key Cryptography for the Financial Services Industry – Part 2. The Secure Hash Algorithm (SHA)."
ANSI X9.31	"Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (RDSA)."
ANSI X9.42	"Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography."
ANSI X9.45	"Enhanced Management Controls Using Digital Signatures and Attribute Certificates."
ANSI X9.52	"American National Standard for Financial Services - Triple Data Encryption Algorithm Modes of Operation."
ANSI X9.57	"Public Key Cryptography for the Financial Services Industry - Certificate Management."

Federal Information Processing Standards (FIPS)

Copies of FIPS publications can be obtained from the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to the publication number, e.g. (FIPS-PUB-74), and title. For more information, see their www site at http://www.itl.nist.gov/fipspubs/

Designation	Title
FIPS PUB 31	“Guidelines to ADP Physical Security and Risk Management.”
FIPS PUB 39	“Glossary for Computer Systems Security (withdrawn).”
FIPS PUB 41	“Computer Security Guidelines for Implementing the Privacy Act of 1974 (withdrawn).”
FIPS PUB 46-3	“Data Encryption Standard.”
FIPS PUB 48	“Guidelines on Evaluation of Techniques for Automated Personal Identification.”
FIPS PUB 74	“Guidelines for Implementing and Using, NBS Data Encryption Standard.”
FIPS PUB 81	“DES Modes of Operation.”
FIPS PUB 112	“Password Usage.”
FIPS PUB 113	“Computer Data Authentication.”
FIPS PUB 140-1	“Security Requirements for Cryptographic Modules.”
FIPS PUB 171	“Key Management Using ANSI X9.17.”
FIPS PUB 180	“Secure Hash Standard.”
FIPS PUB 185	“Escrowed Encryption Standard.”
FIPS PUB 186	“Digital Signature Standard (DSS).”
FIPS PUB 190	“Guideline for the use of Advanced Authentication Technology Alternatives.”
FIPS PUB 196	“Entity Authentication using Public Key Cryptography.”
FIPS PUB 197	“Advanced Encryption Standard (AES).”
FIPS PUB 198	“The Keyed-Hash Message Authentication Code (HMAC).”

ISO/IEC Standards

Designation	Title
ISO 7498-2:1989	"Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture."
ISO/IEC 7816	"Smart Card Standard: Overview."
INCITS/ISO 8372-1987	"Information Processing – Modes of Operation for a 64-Bit Block Cipher Algorithm (formerly ANSI/ISO 8372-1987)."
ISO 8732:1988	"Banking – Key Management (wholesale)."
ISO 9564-1:2002	"Banking – Personal Identification Number (PIN) Management and Security – Part 1: Basic Principles and Requirements for Online PIN Handling in ATM and POS Systems."
ISO 9564-2:1991	"Banking – Personal Identification Number Management and Security – Part 2: Approved Algorithm(s) for PIN Encipherment."
ISO 9564-3:2003	"Banking – Personal Identification Number Management and Security – Part 3: Requirements for Offline PIN Handling in ATM and POS Systems."
ISO/IEC 9594	"The Directory: Authentication Framework."
ISO 9735	"Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) – Application Level Syntax Rules (first edition 1988, amended 1990)."
ISO/IEC 9796-2:2002	"Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 2: Integer Factorization Based Mechanisms."
ISO/IEC 9796-3:2000	"Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 3: Discrete Logarithm Based Mechanisms."
ISO/IEC 9797-1:1999	"Information Technology – Security Techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms Using a Block Cipher."
ISO/IEC 9797-2:2002	"Information Technology – Security Techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms Using a Dedicated Hash-Function."
ISO/IEC 9798	"Security Techniques – Entity Authentication Mechanism."
ISO/IEC 9979	"Security Techniques – Procedures for the Registration of Cryptographic Algorithms."
ISO/IEC 10116	"Security Techniques – Modes of Operation for an *n*-bit Block Cipher Algorithm."
ISO/IEC 10181	"Open Systems Interconnection – Security Frameworks for Open Systems."
ISO/IEC 10118-1:2000	"Information Technology – Security Techniques – Hash-Functions – Part 1: General."

Designation	Title
ISO/IEC 10118-2:2000	"Information Technology – Security Techniques – Hash-Functions – Part 2: Hash-Functions using an n-bit Block Cipher."
ISO/IEC 10118-3:1998	"Information Technology – Security Techniques – Hash-Functions – Part 3: Dedicated Hash-Functions."
ISO/IEC 10118-4:1998	"Information Technology – Security Techniques – Hash-Functions – Part 4: Hash-Functions Using Modular Arithmetic."
ISO 10126-1:1991	"Banking – Procedures for Message Encipherment (Wholesale) – Part 1: General Principles."
ISO 10126-2:1991	"Banking – Procedures for Message Encipherment (Wholesale) – Part 2: DEA Algorithm."
ISO 10164-1	"Object Management Function."
ISO 10164-2	"State Management Function."
ISO 10164-3	"Attributes for Representing Relationships."
ISO 10164-4	"Alarm Reporting Function."
ISO 10164-5	"Event Report Management Function."
ISO 10164-6	"Log Control Function."
ISO 10164-7	"Security Alarm Reporting Function."
ISO 10164-14	"Confidence and Diagnostic Test Categories."
ISO 10164-13	"Summarization Function."
ISO 10164-11	"Metric Objects and Attributes."
ISO 10164-8	"Security Audit Trail Function."
ISO 10164-9	"Objects and Attributes for Access Control."
ISO 10164-10	"Usage Metering Function for Accounting Purposes."
ISO 10164-12	"Test Management Function."
ISO 10164-15	"Scheduling Function."
ISO 10164-16	"Management Knowledge Management Function."
ISO 10164-17	"Changeover Function."
ISO 10202-1:1991	"Financial Transaction Cards - Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 1: Card Life."
ISO 10202-2:1996	"Financial Transaction Cards – Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 2 : Transaction Process."
ISO 10202-3:1998	"Financial Transaction Cards – Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 3: Cryptographic Key Relationships."

Designation	Title
ISO 10202-4:1996	“Financial Transaction Cards – Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 4: Secure Application Modules.”
ISO 10202-5:1998	“Financial Transaction Cards – Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 5: Use of Algorithms.”
ISO 10202-6:1994	“Financial Transaction Cards - Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 6: Cardholder Verification.”
ISO 10202-7:1998	“Financial Transaction Cards – Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 7: Key Management.”
ISO 10202-8:1998	“Financial Transaction Cards – Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards – Part 8: General Principles and Overview.”
ISO 11131:1992	“Banking and Related Financial Services – Sign-on Authentication.”
ISO 11166: 1994	“Banking – Key Management by means of Asymmetric Algorithms (withdrawn).”
ISO 11568-5: 1998	“Banking – Key Management (Retail).”
ISO/IEC 11770-1:1996	“Information Technology – Security Techniques – Key Management – Part 1: Framework.”
ISO/IEC 11770-2:1996	“Information Technology – Security Techniques – Key Management – Part 2: Mechanisms Using Symmetric Techniques.”
ISO/IEC 11770-3:1999	“Information Technology – Security Techniques – Key Management – Part 3: Mechanisms Using Asymmetric Techniques.”
ISO/TR 13335-1: 1996	“Information Technology – Guidelines for the Management of IT Security – Part 1: Concepts and Models for IT Security.”
ISO/FCD 13335-1: 200x	“Information Technology – Management of Information and Communications Technology Security – Part 1: Concepts and Models for Information and Communications Technology Security Management.”
ISO/TR 13335-2: 1997	“Information Technology – Guidelines for the Management of IT Security – Part 2: Managing and Planning IT Security.”
ISO/TR 13335-3: 1998	“Information Technology – Guidelines for the Management of IT Security – Part 3: Techniques for the Management of IT Security.”
ISO/TR 13335-4: 2000	“Information Technology – Guidelines for the Management of IT Security – Part 4: Selection of Safeguards.”
ISO/TR 13335-5: 2001	“Information Technology – Guidelines for the Management of IT Security – Part 5: Management Guidance on Network Security.”

Designation	Title
ISO/TR 13335-2: 1997	“Information Technology – Guidelines for the Management of IT Security – Part 2: Managing and Planning IT Security.”
ISO/IEC 13888	“Security Techniques – Non-repudiation.”
ISO/IEC 14888-1:1998	“Information technology - Security Techniques – Digital Signatures with Appendix – Part 1: General.”
ISO/IEC 14888-2:1999	“Information Technology – Security Techniques – Digital Signatures with Appendix – Part 2: Identity-Based Mechanisms.”
ISO/IEC 14888-3:1998	“Information Technology – Security Techniques – Digital Signatures with Appendix – Part 3: Certificate-Based Mechanisms.”
ISO/IEC 15408	“Information Technology – Security Techniques – Evaluation Criteria for IT Security.”
ISO/IEC 15946-1:2002	“Information Technology – Security Techniques – Cryptographic Techniques Based on Elliptic Curves – Part 1: General.”
ISO/IEC 15946-2:2002	“Information Technology – Security Techniques – Cryptographic Techniques Based on Elliptic Curves – Part 2: Digital Signatures.”
ISO/IEC 15946-3:2002	“Information Technology – Security Techniques – Cryptographic Techniques Based on Elliptic Curves – Part 3: Key Establishment.”
ISO/IEC 15946-4:2004	“Information Technology – Security Techniques – Cryptographic Techniques Based on Elliptic Curves – Part 4: Digital Signatures Giving Message Recovery.”
ISO/IEC 17799	“Information Technology – Code of Practice for Information Security Management.”
ISO/IEC 18014	“Time Stamping.”

IETF Request for Comments (RFC)

IETF documents can be viewed and downloaded directly from the IETF www site at http://www.ietf.org/rfc.html.

Designation	Title
RFC 1102	“Policy Routing in Internet Protocols.”
RFC 1004	“A Distributed-Protocol Authentication Scheme.”
RFC 1221	“Host Access Protocol (HAP) Specification - Version 2.”
RFC 1305	“Network Time Protocol (Version 3): Specification, Implementation and Analysis.”
RFC 1319	“The MD2 Message-Digest Algorithm.”
RFC 1320	“The MD4 Message-Digest Algorithm.”
RFC 1321	“The MD5 Message-Digest Algorithm.”
RFC 1322	“A Unified Approach to Inter-Domain Routing.”
RFC 1351	“SNMP Administrative Model.”
RFC 1352	“SNMP-SEC SNMP Security Protocols.”
RFC 1424	“Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.”
RFC 1507	“DASS - Distributed Authentication Security Service.”
RFC 1508	“Generic Security Service Application Program Interface.”
RFC 1510	“The Kerberos Network Authentication Service (V5).”
RFC 1579	“Firewall-Friendly FTP.”
RFC 1750	“Randomness Recommendations for Security.”
RFC 1826	“IP Authentication Header.”
RFC 1827	“IP Encapsulating Security Payload (ESP).”
RFC 1828	“IP Authentication using Keyed MD5.”
RFC 1847	“Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted.”
RFC 1848	“MIME Object Security Services.”
RFC 1938	“A One-Time Password System.”
RFC 1968	“The PPP Encryption Control Protocol (ECP).”
RFC 2196	“Site Security Handbook.”
RFC 2040	“The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms.”
RFC 2093	“Group Key Management Protocol (GKMP) Specification.”
RFC 2228	“FTP Security Extensions.”

Designation	Title
RFC 2244	“ACAP -- Application Configuration Access Protocol.”
RFC 2246	“The TLS Protocol Version 1.0.”
RFC 2350	“Expectations for Computer Security Incident Response.”
RFC 2401	“Security Architecture for the Internet Protocol.”
RFC 2527	“Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.”
RFC 2725	“Routing Policy System Security.”
RFC 2993	“Architectural Implications of NAT.”