PCSF Congress of Chairs

Cyber Security Combined Glossary Project

Terms From

Seventeen Cyber Security Glossaries

Version of

March 28, 2007

This list of cyber security terms will give you insight into one major activity of the Congress of Chairs, the Combined Glossary Project. The basic concept of this project is to collect glossaries from as many process control-related cyber security standards groups as possible and combine them. To date, we have posted on our Web site combined glossaries for seventeen groups:

- AGA 12
- API 1164
- CIDX Report on Cybersecurity Vulnerability Assessment Methodologies, version 2.0, November 2004
- FIPS Pub 200
- IEC TC57 WG15: IEC 62351-2 Data and Communications Security Glossary of Terms, 1st Committee Draft for Vote (CDV) Version 3 (not submitted yet), September 2006
- ISA Comprehensive Dictionary of Instrumentation and Control
- ISA SP99
- NERC Glossary of Terms Used in Reliability Standards, effective April 1, 2005
- NERC Cyber Security Standards Cip-002-009
- NERC Security Guidelines for the Electricity Sector: Physical Security – Substations, October 15, 2004
- NERC Threat Alert System and Cyber Response Guidelines for the Electricity Sector: Definitions of Cyber Threat Alert Levels, Version 2.0, October 8, 2002
- NERC Security Guidelines for the Electricity Sector: Patch Management for Control Systems, Version 1.0, May 5, 2005
- NERC Security Guidelines for the Electricity Sector: Control System – Business Network Electronic Connectivity, Version 1.0, May 3, 2005

- NIST SP800-53
- PCSRF Field Device Protection Profile
- SD6, SC 27 N 2776
- Microsoft Security Glossary, Published October 29, 2002, Updated December 19, 2005

Additional glossaries will be added as they are contributed. To see the most current version, visit the PCSF Congress of Chairs Web site at –

https://www.pcsforum.org/groups/59/

and click on “LIBRARY”.

This document identifies the terms that have been combined as of the date at the top of this page. Note that discussions are under way to align some of these terms and it is expected that many of the differences in duplicate terms will be eliminated in the near future. Any group that has a glossary that it would like to contribute should contact Bill Rush at -

William.Rush@comcast.net

Definitions of Process Control Terms and Acronyms

Using These Definitions to Save Effort and Simplify Standards Development

Some of the primary goals of the Congress of Chairs are to avoid duplication of effort, simplify standards development work, and to avoid the emergence of incompatible or conflicting standards. This document is designed to achieve these goals by providing a single collection of definitions of terms and acronyms drawn from a variety of sources. It is our hope that this collection will be useful to several groups, including the following:

- Standards groups that have not yet developed their own glossary. Using this collection will both save effort and assure agreement with the terminology used by other groups.
- Standards groups that have completed – or are developing – their glossary are invited to submit their definitions to the Congress of Chairs for inclusion of their work in this document. This will save others the effort of developing terms and reduce the odds of some other group's using these same terms in a different sense.
- Standards groups that have already developed and published terms that differ from those that are published by other groups in different documents will be made aware of the differences as a minimum. Identifying such instances allows people to recognize the differences as a minimum. The Congress of Chairs also provides a forum that may allow harmonization of terminology by jointly developing a single definition of the terms.

Please be certain that you are using the most recent version of this document, because new glossaries are added periodically and some terms that differed originally have been modified for agreement.

The Definitions Come From Several Sources

Below is a numbered list of sources from which the term/acronym was taken. Sources for definitions are shown in the third column of the table of Definition of Terms and Definition of Acronyms. If the same term has more than one definition, all definitions are given, along with the source. There is no significance to the order in which differing definitions of the same term are arranged. To provide a standard method of selecting which definition is given first, the terms are arranged in the order in which they were received. This list will expand as new glossaries are submitted to the Congress of Chairs for inclusion.

1 FIPS PUB 140-2, (2001): Security Requirements for Cryptographic Modules, Section 2, Glossary of terms and acronyms, National Institute of Standards and Technology.

2 IEEE 100: The Authoritative Dictionary of IEEE Standards Terms", 7th ed.: Institute of Electrical and Electronics Engineers.

3 DNP Technical Bulletin 2002-x, Message Authentication Object.

4 NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation.

5 RFC 793: Transmission Control Protocol, September 1981.

6 RFC 2828: Internet Security Glossary.

7 Menezes, Alfred J., van Oorschot, Paul C., and Vanstone, Scott A. (1997) Handbook of Applied Cryptography, CRC Press.

8 Schneier, Bruce: Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

9 FIPS PUB 198, (2002): The Keyed-Hash Message Authentication Code (HMAC).

10 AGA 12, Part 1, Cryptographic Protection of SCADA Communications

11 ISA-SP99, Manufacturing and Control System Security

12 CNSS Instruction No. 4009, National Information Assurance Glossary, May 2003

12* CNSS Instruction No. 4009, Adapted

13 API Standard 1164

14 FIPS PUB 200 (2005): Minimum Security Requirements for Federal Information and Information Systems

15 NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems

16 NIST SP 800-37

17 OMB Circular A-130, Appendix III

18 44 U.S.C., Sec. 3542

19 44 U.S.C., Sec. 5125(b)

20 41 U.S.C., Sec. 403

21 FEA Program Management Office

22 40 U.S.C., Sec. 11331

23 44 U.S.C., Sec. 3502

24 40 U.S.C., Sec. 1401

25 FIPS 199

26 NIST SP 800-18

27 47 C.F.R., Part 64, App A

28 OMB Memorandum 02-01

29 OMB Memorandum 03-22

30 NIST SP 800-30

31 44 U.S.C., Sec. 3544

31 NIST SP 800-53

32 CIDX Report on Cybersecurity Vulnerability Assessment Methodologies, version 2.0, November 2004

33 ISA Comprehensive Dictionary of Instrumentation and Control, edited by W. H. Cubberly, 1988

34 NERC Glossary of Terms Used in Reliability Standards (adopted by NERC Board of Trustees: February 8, 2005; effective date: April 1, 2005)

35 NERC Cyber Security Standards Cip-002-009, November 8, 2005

36 NERC Security Guidelines for the Electricity Sector: Physical Security – Substations, October 15, 2004

37 NERC Threat Alert System and Cyber Response Guidelines for the Electricity Sector: Definitions of Cyber Threat Alert Levels, Version 2.0, October 8, 2002

38 NERC Security Guidelines for the Electricity Sector: Patch Management for Control Systems, Version 1.0, May 5, 2005

39 NERC Security Guidelines for the Electricity Sector: Control System – Business Network Electronic Connectivity, Version 1.0, May 3, 2005

40 PCSRF Field Device Protection Profile

41 IEC 62351-2 Data and Communications Security Glossary of Terms, 1st Committee Draft for Vote (CDV) Version 3 (not submitted yet), September 2006 [Editor's note: This document draws definitions from ATIS/INFOSEC-99, FIPS 140-2, FS-1037C, IETF RFC2828, ISA SP99, ISO/IEC, NIST, and WIKI.]

42 SD 6. SC 27 N 2776, Glossary of IT Security Terminology, March 31, 2002

43 Microsoft Security Glossary, Published October 29, 2002, Updated December 19, 2005

Definition of Terms

Term	Definition	Source
A priori	Latin phrase meaning "in advance;" "from something prior." Here it means the sender and recipient exchanged a common secret quantity (e.g., key) prior to exchanging encrypted messages.	10
Access	In respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of personnaly identifiable information collected about him or her. Access is an element of the Fair Information Practices.	43
Access Authority	An entity responsible for monitoring and granting access privileges for other authorized entities. [RFC2828]	41
Access Control	The restriction of entry or use, to all or part of, any physical, functional, or logical unit.	10
Access Control	1. Prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO/IEC 18028-2: 2006-02-01] 2. Protection of resources against unauthorized access; a process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy. [RFC 2828] 3. A service feature or technique used to permit or deny use of the components of a communication system. 4. A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device. 5. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device. 6. Limiting access to information system resources only to authorized users, programs, processes, or other systems. 7. That function performed by the resource controller that allocates system resources to satisfy user requests. [FS-1037C]	41
Access Control	The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based. See also access control list and accesscontrol entry.	43
Access Control Entry (ACE)	In Windows-based systems, an entry in an access control list containing the security identifier for a user or group and an access mask that specifies which operations by the user or group are allowed, denied, or audited.	43
Access Control List (ACL)	In Windows-based systems, a list of access control entries that apply to an entire object, a set of the object's properties, or an individual property of an object, and that define the	43

Term	Definition	Source
	access granted to one or more security principals.	
Access Mask	In Windows-based systems, a value that specifies the permissions that are allowed or denied in an access control entry of an access control list. The access mask is also used in an access request to specify the access permissions that the subject requires when accessing an object.	43
Access Token	A data structure that contains authorization information for a user or group. A system uses an access token to control access to securable objects and to control the ability of a user to perform various system-related operations on a local computer.	43
ACE	See access control entry.	43
ACL	See access control list.	43
Accountability	A property that ensures that the actions of an entity may be traced uniquely to that entity.	10
Accountability	1. The property that ensures that the actions of an entity may be traced uniquely to the entity [ISO/IEC 7498-2] 2. The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions. [RFC2828]	41
Accountability	The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	14, 15, 16
Accreditation	Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations. {ISO/IEC WD 15443-1 (11/2001)]	42
Accrediting Authority	See Authorizing Official.	15

Term	Definition	Source
Accreditation Authority	Entity trusted by all members of a group of entities for the purposes of the generation of private accreditation information. [ISO/IEC 9798-5; 1999]	42
Accreditation Boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.	15
Accreditation Multiplicity Parameter	Positive integer equal to the number of items of secret accreditation information provided to an entity by the accreditation authority. [ISO/IEC 9798-5: 1999]	42
ACL	Access Control List. The access control list (ACL) is a concept in computer security used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identity. [WIKI] Typically, it means that routers have only specific authorized ports enabled and that only specific IP addresses are permitted to be routed onward. {Common Usage]	41
ACSI	Abstract Communication Service Interface: A virtual interface to an IED providing abstract communication services, e.g. connection, variable access, unsolicited data transfer, device control and file transfer services, independent of the actual communication stack and profiles used. [IEC 61850]	41
Activities	An assessment object that includes specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).	15
Adequacy	The ability of the electric system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.	34
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.	14, 15, 17
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical	41

Term	Definition	Source
	controls. [NIST]	
Adjacent Balancing Authority	A Balancing Authority Area that is interconnected another [sic] Balancing Authority Area either directly or via a multi-party agreement or transmission tariff.	34
Administrative Vulnerablity	Failure to observe administrative best practices, such as using a weak password or logging on to an account that has more user rights than the user requires to perform a specific task.	43
Adversary	An individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities that may be detrimental to an industrial or manufacturing system. Adversaries may include disgruntled insiders or former insiders, hackers, crackers, computer criminals, terrorists, industrial espionage agents, foreign espionage agents, and cyber warriors.	11
Adware	Advertising that is integrated into software. Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware.	43
AES	Advanced Encryption Standard. 1. A symmetric encryption mechanism providing variable key length and allowing an efficient implementation specified as Federal Information Processing Standard (FIPS) 197. [ISO/IEC 18028-4: 2005-04-01] 2. In cryptography, the Advanced Encryption Standard (AES), based on Rijndael, is a block cipher adopted as an encryption standard by the US government. It is expected to be used worldwide and analysed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). AES was adopted by National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001 after a 5-year standardisation process. [WIKI]	41
AGA	American Gas Association	41

Term	Definition	Source
AGA 12 Series	A series of specifications and practices published by the American Gas Association, which comprise a series of documents. AGA 12, Part 1 includes background information, general security policies, and the cryptographic system test plan. AGA 12, Part 2 includes requirements to retrofit existing asynchronous serial communications. AGA 12, Part 3 and subsequent documents will address other configurations.	10
Agency	See Executive Agency.	15
Agency	Any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include: (i) the Government Accounting Office; (ii) the Federal Election Commission; (iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (iv) government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.	14, 23
Agreement	A contract or arrangement, either written or verbal and sometimes enforceable by law.	34
Ancillary Service	Those services that are necessary to support the transmission of capacity and energy from resources to loads while maintaining reliable operation of the Transmission Service Provider's transmission system in accordance with good utility practice. (*From FERC order 888-A*.)	34
Anonymity	A condition in which an individual's true identity is unknown.	43

Term	Definition	Source
Anti-Aliasing Filter	An analog filter installed at a metering point to remove the high frequency components of the signal over the AGC sample period.	34
Antivirus Software (AV)	A computer program designed to detect and respond to malicious software, such as viruses and worms. Responses may include blocking user access to infected files, cleaning infected files or systems, or informing the user that an infected program was detected.	43
Appendix	A string of bits formed by the signature and an optional text field. [ISO/IEC 14888-1: 1998]	42
Applicant	An entity (organization, individual etc.) which requests the assignment of a register entr and entry label. [ISO/IEC 15292: 2001]	42
Application (Software)	1. A loosely defined subclass of computer software that employs the capabilities of a computer directly to a task that the user wishes to perform. [WIKI] 2. Software computer program that performs a function. [Common Usage]	41
Application Layer	*See Open Systems Interconnection—Reference Model Layer 7*	41

Term	Definition	Source
Approach	The method used or steps taken in setting about a task, problem, etc. [ISO/IEC WD 15443-1 (11/2001)]	42
Approved	FIPS-Approved and/or NIST-recommended.	1, 10
Approved Security Function	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either specified in an approved standard, or adopted in an approved standard and specified either in an annex of the approved standard or in a document referenced by the approved standard, or specified in the list of approved security functions.	1, 10
Archive	See key management archive.	10
Area Control Error (ACE)	The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias and correction for meter error.	34
Assessment	Verification of a deliverable against a standard using the corresponding method to establish compliance and determine the assurance. [ISO/IEC WD 15443-1 (11/2001)]	42
Asset	An entity that may have value to someone. Assets may be tangible or intangible. Examples are people, a facility, materials, equipment, information, business reputation, an activity or operation such as manufacturing, the environment, and the community.	32
Asset	Anything that has value to the organization. [ISO/IEC PDTR 13335-1 (11/2001)] Anything that has value to the organization, its business operations and theoir continuity. [ISO/IEC 17799: 2000]	42
Assets	Information or resources to be protected by the countermeasures of a TOE. [ISO/IEC 15408-1: 1999]	42
Assignment	A data item which is a function of the witness and possibly of a part of the message, and forms part of the input to the signature function. [ISO?IEC 14888-1: 1998, ISO/IEC 9796-3: 2000] The specification of an identified parameter in a component. [ISO/IEC 15408-1:1999]	42

Term	Definition	Source
Assurance	In the context of security: Grounds for confidence that a deliverable meets its security objectives. [ISO/IEC 15408-1] Note: this definition is generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfils specified requirements. [ISO/IEC Guide 2]	41
Assurance	Grounds for confidence that an entity meets its security objectives. [ISO/IEC 15408-1: 1999] Performance of appropriate activities or processes to instil confidence that a deliverable meets its security objectives. [ISO/IEC WD 15443-1 (11/2001)]	42
Assurance Approach	A grouping of assurance methods according to the aspect examined. [ISO/IEC WD 15443-1 (11/2001)]	42
Assurance Authority	A person or body responsible (accountable) for the selection, implementation and acceptance of assurance. NOTE – In specific schemes or organisations, the term for assurance authority may be different such as evaluation authority. [ISO/IEC WD 15443-1 (11/2001)]	42
Assurance Element	A process or activity of an assurance method, in itself recognised to provide reproducible assurance results. [ISO/IEC WD 15443-1 (11/2001)]	42
Assurance Level	The amount of assurance obtained according to the specific scale used by the assurance method. The amount of assurance obtained generally is related to the effort expended on the activities performed. NOTE – The assurance level may not be measurable in quantitative terms. [ISO/IEC WD 15443-1 (11/2001)]	42
Assurance Method	Documented set of assurance elements recognised to obtain reproducible assurance results. [ISO/IEC WD 15443-1 (11/2001)]	42

Term	Definition	Source
Assurance Results	Documented numerical or qualitative assurance statement obtained by applying an assurance method. [ISO/IEC WD 15443-1 (11/2001)]	42
Assurance Scheme	The administrative and regulatory framework under which an assurance method is applied by an assurance authority within a specific community or organisation. [ISO/IEC WD 15443-1 (11/2001)]	42
Assurance Stage	The deliverable life cycle stage on which a given assurance method is focused. The overall deliverable assurance takes into account the results of the assurance methods applied throughout the deliverable life cycle. [ISO/IEC WD 15443-1 (11/2001)]	42
Asymmetric	Having unequal shape or weight on either side. In communications, refers to a protocol exchange where one device is known to be the master, as opposed to communications between equal peers. In cryptography, refers to “public key” cryptography where one key may be published while the other remains secret. [Common Usage]	41
Asymmetric cipher	Cipher based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption [ISO/IEC 18033-1].	41
Asymmetric Cipher	Alternative term for asymmetric encipherment system. [ISO/IEC WD 18033-1 (12/2001)]	42
Asymmetric Cryptographic Algorithm	A cryptographic formula that uses two related keys—a public key and a private key —each of which has the characteristic algorithm that, given the public key, it is computationally infeasible to derive the private key. [After X9.62] [ATIS]	41

Term	Definition	Source
Asymmetric Cryptographic Technique	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. NOTE - A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature systems encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this is not the general case, throughout ISO/IEC 9798 the four elementary transformations and the corresponding keys are kept separate. [ISO/IEC 9798-1: 1997] A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. [ISO/IEC 11770-1: 1996, ISO/IEC FDIS 15946-3 (02/2001)] A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. NOTE - A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature systems, encipher and decipher for encipherment systems. The signature and the decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary	42

Term	Definition	Source
	functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this does not conform to the principle of key separation, throughout this part of ISO/IEC 11770 the four elementary transformations and the corresponding keys are kept separate. [ISO/IEC 11770-3: 1999] Cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. [ISO/IEC WD 18033-1 (12/2001)]	
Asymmetric Encipherment System	A system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] System based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment. NOTE - An asymmetric encipherment system is an asymmetric cryptographic technique that is also an encryption algorithm. [ISO/IEC WD 18033-1 (12/2001)]	42
Asymmetric Encryption Algorithm	Alternative term for asymmetric encipherment system. [ISO/IEC WD 18033-1 (12/2001)]	42
Asymmetric Key Algorithm	*See Public Key Cryptographic Algorithm.* [RFC2828]	41

Term	Definition	Source
Asymmetric Key Pair	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC 9798-1: 1997-08-01]	41
Asymmetric Key Pair	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] Pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC WD 18033-1 (12/2001)]	42
Asymmetric Signature System	A system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification. [ISO/IEC 9798-1: 1997]	42
Attack	Attempt to gain unauthorized access to a system's services, resources, or information, or the attempt to compromise an Information System's integrity, availability, or confidentiality. [CNSS]	12
Attack	Hostile action taken by an adversary to obtain access to an asset and use it to achieve their objectives.	32
Attack	1. An attempt to destroy, expose, alter, or disable an Information System and/or information within it or otherwise breach the security policy. [ISO/IEC FDIS 18043: 2006-03-14] 2. An attempt to violate computer security. Note: An example of an attack is malicious logic. [2382-pt.8] 3. [An] intentional act of attempting to bypass one or more of the following security controls of an information system (IS): non-repudiation, authentication, integrity, availability, or confidentiality. [INFOSEC-99]	41

Term	Definition	Source
Attack	An attempt to exploit an IT system vulnerability. [ISO/IEC DTR 15947 (10/2001)]	42
Attack	A deliberate attempt to compromise the security of a computer system or deprive others of the use of the system.	43
Attack Potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation. [ISO/IEC 15408-1: 1999]	42
Attribute Authority (AA)	An entity trusted by one or more entities to create and sign attribute certificates. Note that a CA may also be an AA. [ISO/IEC TR 14516; 2000]	42
Audit	1. Formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity. [ISO/IEC 18028-3: 2005-12-15] 2. To conduct an independent review and examination of system records and activities in order to test the adequacy and effectiveness of data security and data integrity procedures, to ensure compliance with established policy and operational procedures, and to recommend any necessary changes. 3. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [FS-1037C]	41

Term	Definition	Source
Audit Record Field	A field containing information regarding all entities in a transaction, and indicators of the types of processing performed by those entities. [After X9.17/95] [ATIS]	41
Audit Trail	1. A record of both completed and attempted accesses and service. 2. Data in the form of a logical path linking a sequence of events, used to trace the transactions that have affected the contents of a record. 3. [In INFOSEC, a] chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. *Note:* Audit trail may apply to information in an information system (IS), to message routing in a communications system, or to the transfer of COMSEC material. [INFOSEC-99] [FS-1037C]	41
Augmentation	The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package. [ISO/IEC 15408-1: 1999]	42
Authenticate	1. To establish, usually by challenge and response, that a transmission attempt is authorized and valid. 2. Verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an automated information system, or establish the validity of a transmitted message. [NIS] 3. A challenge given by voice or electrical means to attest to the authenticity of a message or transmission. [JP1] [FS-1037C]	41

Term	Definition	Source
Authentication	A process that establishes the origin of information, or validates an entity's identity[1].	10
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSS]	12
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.	14, 15
Authentication	The process used to verify user identity.	39
Authentication	1. [Any] Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [INFOSEC-99] [After JP 1-02] 2. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. [JP 1-02] 3. Evidence by proper signature or seal that a document is genuine and official. [JP 1-02] [FS-1037C] 4. A process that establishes the origin of information, or determines an entity's identity. [RFC2828] 5. the provision of assurance of the claimed identity of an entity [ISO/IEC 10181-2:1996]	41
Authentication	The provision of assurance of the claimed identity of an entity. [ISO/IEC TR 13335-4: 1999]	42

[1] The AGA 12 Task Group found that "Authentication" has two distinct meanings. One is authentication of one cryptographic module (CM) to another, simply establishing that the module is talking to the module to which it believes it is talking. The other meaning of authentication is establishing that the CM indeed is really associated with domain (i.e., user defined name) identity with which it is claimed to be associated.

Term	Definition	Source
Authentication	The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital signatures, smart cards, biometric data, and a combination of user names and passwords.	43
Authentication Code	A cryptographic checksum based on an approved security function (also known as a Message Authentication Code).	1, 10
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.	15
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information. [ISO/IEC TR 13335-1:1996 (3.3) monolingual (English) only]	41
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Authorization	The right or a permission that is granted to a system entity to access a system resource.	10, 12
Authorization	(1.) An “authorization” is a right or a permission that is granted to a system entity to access a system resource. (2.) An “authorization process” is a procedure for granting such rights. (3.) To “authorize” means to grant such a right or	41

Term	Definition	Source
	permission. (See: privilege.) [RFC2828]	
Authorization	The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, which is verified through authentication.	43
Authorize Processing	See Accreditation.	15
Authorized User	In security, a user who may, according to an organization's security policy, perform an operation. [After CC-99] [FS-1037C]	41
Authorised User	A user who may, in accordance with the TSP, perform an operation. [ISO/IEC 15408-1: 1999]	42
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	14, 15, 16
Automated Information System	A computer system that is used to process and transmit data.	11
Automatic Generation Control (AGC)	Equipment that automatically adjusts generation in a Balancing Authority Area from a central location to maintain the Balancing Authority's interchange schedule plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction.	34
AV	See antivirus software.	43
Availability	The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.	10, 11
Availability	Ensuring timely and reliable access to and use of	14, 15, 18

Term	Definition	Source
	information.	
Availability	The number of hours in the reporting period less the total downtime for the reporting period divided by the number of hours in the reporting period (expressed in percent).	33
Availability	1. the property of being accessible and usable upon demand by an authorized entity [ISO/IEC 13335-1:2004] 2. The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them. [RFC2828]	41
Availability	The property of being accessible and usable upon demand by an authorized entity. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Availability	The property of a system or a system resource that ensures it is accessible and usable upon demand by an authorized system user. Availability is one of the core characteristics of a secure system.	43
Available Transfer Capability (ATC)	A measure of the transfer capability remaining in the physical transmission network for further commercial activity over and above already committed uses. It is defined as Total Transfer Capability less existing transmission commitments (including retail customer service), less a Capacity Benefit Margin, less a Transmission Reliability Margin.	34
b-bits	block of length ‘b’ bits	
Back Door	*Synonym* for Trapdoor. A hidden software or hardware mechanism, usually created for testing and troubleshooting,	41

Term	Definition	Source
	that may be used to circumvent computer security. [ATIS]	
Back Door	A hardware or software-based hidden entrance to a computer system that can be used to bypass the system's security policies.	43
Backup	A copy of information to facilitate recovery, if necessary.	10
Back-up	1. Equipment which is available to complete an operation in the event that the primary equipment fails. 2. A copy of a computer diskette which protects against destruction or loss of the original.	33
Balancing Authority (BA)	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.	34
Balancing Authority Area	The collection of generation, transmission, and loads within the metered boundaries of the Balancing Authority. The Balancing Authority maintains load-resource balance within this area.	34
Bandwidth	The rate at which a data path (e.g., a channel) carries data, measured in bits per second.	10
Bandwidth	1. A group of consecutive frequencies constituting a band that exists between limits of stated frequency attenuation. A band is normally defined as more than 3.0 decibels greater than the mean attenuation across the band. 2. A group of consecutive frequencies constituting a band that exists between limits of stated frequency delay.	33
Bandwidth	Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second. [RFC2828]	41
Base Load	The minimum amount of electric power delivered or required over a given period at a constant rate.	34
Baseline Controls	A minimum set of safeguards established for a system or organization. [ISO/IEC PDTR 13335-1 (11/2001)]	42

Term	Definition	Source
BBBOnLine	A privacy seal program established by the Better Business Bureau which certifies that certain Web sites conform to baseline privacy standards. Microsoft is a sponsor of BBBOnLine.	43
Big-endian	A method of storage of multi-byte numbers with the most significant bytes at the lowest memory addresses. [ISO/IEC 10118-1: 2000]	42
Blackstart Capability Plan	A documented procedure for a generating unit or station to go from a shutdown condition to an operating condition delivering electric power without assistance from the electric system. This procedure is only a portion of an overall system restoration plan.	34
Block	A group of contiguous characters formed for transmission purposes.	10
Block	1. A set of things, such as words, characters, or digits, handled as a unit. 2. A collection of contiguous records recorded as a unit, blocks are separated by interblock gaps, and each block may contain one or more records. 3. In data communication, a group of contiguous characters formed for transmission purposes. The groups are separated by interblock characters. 4. A group of physically adjacent words or bytes of a specified size particular to a device. The smallest system-addressable segment on a mass-storage device in reference to I/O. See also cylinder block; block-and-tackle.	33
Block	A bit-string of length L_1, i.e., the length of the first input to the round-function. [ISO/IEC FDIS 9797-2 (09/2000), ISO/IEC CD 10118-3 (11/2001)] A string of bits of length $L_{\bullet}$·, which shall be an integer multiple of 16. [ISO/IEC 10118-4: 1998] A bit-string of length *n*. [ISO/IEC 9797-1: 1999] String of bits of defined length. [ISO/IEC WD 18033-1 (12/2001)]	42
Block Chaining	The encipherment of information such that each block of ciphertext is cryptographically dependent upon the preceding ciphertext block. [ISO 8372: 1987] The encipherment of information such that each block of ciphertext is cryptographically dependent upon a preceding ciphertext block. [ISO/IEC CD 10116 (12/2001)]	42

Term	Definition	Source
Block Cipher	Symmetric encryption algorithm with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 18033-1]	41
Block Cipher	Symmetric encryption algorithm with the property that the encryption process operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 18033-1 (02/2001)]	42
Block Cipher Key	A key that controls the operation of a block cipher. [ISO/IEC 9797-1: 1999]	42
Broadcast Mode	Concurrent transfer mode of information to all connected receivers with one message from the information source. Contrast: unicast and multicast modes	10
Buddy Fix	See private fix.	43
Buffer	A region of memory reserved for use as an intermediate repoitory in which data is temporarily held before it is transferred between two locations or devices.	43
Buffer Overrun	A condition that results from adding more information to a buffer than it was designed to hold. An attacker may exploit this vulnerability to take over a system.	43
Bug	1. A concealed microphone or listening device or other audio surveillance device. [JP 1-02] 2. A mistake in a computer program. 3. To install means for audio surveillance. [JP 1-02] 4. A semiautomatic telegraph key. 5. A mistake or malfunction. [ATIS]	41

Term	Definition	Source
Bulk Electric System	As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.	34
Bump-in-the-Wire	In security, the addition of encryption boxes at either end of a communications link, just after the connection of the devices/system. One encryption box takes the plain text messages from one device and encrypts them, while the other box receives the encrypted messages and decrypts them back into plain text, and vice versa. This approach provides external encryption and avoids the need to embed an encryption function within the device. [Common usage]	41
Burden	Operation of the Bulk Electric System that violtes or is expected to violate a System Operating Limit or Interconnection Reliability Operating Limit in the Interconnection, or that violates any other NERC, Regional Reliability Organization, or local operating reliability standards or criteria.	34
Business Network	An entity's communication network, used for general purpose business activities, typically connecting a wide variety of non-critical assets and non-safety related business applications.	38, 39
Can	The word "can," equivalent to "is able to," is used to indicate possibility and capability, whether material or physical.	10
Capacity	Positive integer indicating the number of bits available within the signature for the recoverable part of the message. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Capacity Benefit Margin (CBM)	The amount of firm transmission transfer capability preserved by the transmission provider for Load-Serving Entities (LSEs), whose loads are located on that Transmission Service Provider's system, to enable access by the LSEs to generation from interconnected systems to meet generation reliability requirements. Preservation of CBM for an LSE allows that entity to reduce its installed generating capacity below that which may otherwise have been necessary without interconnections to meet its generation reliability requirements. The transmission transfer capability preserved as CBM is intended to be used by the	34

Term	Definition	Source
	LSE only in times of emergency generation deficiencies.	
Capacity Emergency	A capacity emergency exists when a Balancing Authority Area's operating capacity, plus firm purchases from other systems, to the extent available or limited by transfer capability, is inadequate to meet its demand plus its regulating requirements.	34
Cascading	The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.	34
Certificate	See "public key certificate."	10
Certificate	1. In cryptography, the public key and the identity of an entity, with other information, rendered unforgeable by digitally signing the entire information with the private key of the issuing certification authority. [After X9.42] Synonym digital certificate. 2. [A] record holding security information about an information-system (IS) user and vouches to the truth and accuracy of the information it contains. [INFOSEC-99] [ATIS]	41
Certificate	An entity's data rendered unforgeable with the private or secret key of a certification autority. [ISO/IEC WD 13888-1 (11/2001)] A declaration by an independent authority operating in accordance with ISO Guide 58, Calibration and testing laboratory accreditation systems – General requirements for operation and recognition, confirming that an evaluation pass statement is valid. [ISO/IEC 15292: 2001]	42
Certificate	An encrypted file containing user or server identification information, which is used to verify identity and to help establish a security-enhanced link.	43
Certificate Authority	The entity in a PKI that is responsible for issuing certificates and exacting compliance to a PKI policy.	10
Certificate Directory	A directory containing a well defined (sub)set of public key certificates. This directory can contain certificates from different Certification Authorities. [ISO/IEC FDIS 15945 (10/2000)]	42
Certificate Domain	Collection of entities using public key certificates created by a single Certification Authority (CA) or a collection of CAs operating under a single security policy. [ISO/IEC FDIS 9796-2 (12/2001)]	42

Term	Definition	Source
Certificate Domain Parameters	Cryptographic parameters specific to a certificate domain and which are known and agreed by all members of the certificate domain. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Certificate Management	[The] process whereby certificates . . . are generated, stored, protected, transferred, loaded, used, and destroyed. [ATIS]	41
Certificate Management Services	All services needed for the maintenance of the lifecycle of certificates, including registration, certification, distribution, and revocation of certificates. [ISO/IEC FDIS 15945 (10/2000)]	42
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	14, 15
Certification	[The] comprehensive evaluation of the technical and nontechnical security features of an AIS [automated information system] and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NIS] [FS-1037C]	41
Certification	Procedure by which a third party gives written assurance that a deliverable (product, system or service) conforms to specified requirements. [ISO/IEC WD 15443-1 (11/2001)]	42

Term	Definition	Source
Certification Agent	The individual, group, or organization responsible for conducting a security certification.	15, 16
Certification Authority (CA)	1. An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users‘ keys. [ISO/IEC 13888-1: 2004-06-01] 2. In cryptography, a centre trusted by one or more agencies or individuals to create and assign certificates and, optionally, to create user’s keys. [After X9.31] 3. In secure communications, a trusted person or entity who issues certificates (also called “public-key certificates”) for encryption purposes. 4. An independent party identifying and certifying payers and payees for real-time credit card transactions in electronic commerce. [Mattila] 5. Third level of the Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by-the parent Policy Creation Authority (PCA). [INFOSEC-99] [ATIS] 6. The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates, and exacting compliance to a PKI policy. [RFC2828]	41
Certification Authority (CA)	A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities. [ISO/IEC 9796-3: 2000, ISO/IEC 11770-1: 1996, ISO/IEC 11770-3: 1999]	42
Certification Service	The service of creating and assigning certificates performed by a CA and described in ISO/IEC 9594-8: 1995. [ISO/IEC FDIS 15945 (10/2000)]	42
Challenge	A data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier. [ISO/IEC 9798-1:	42

Term	Definition	Source
	1997]	
Challenge and Reply Authentication	[A] prearranged procedure in which a subject of another, and the latter establishes validity with a correct reply. [ATIS]	41
Change Management	The practice of administering changes with the help of tested methods and techniques in order to avoid new errors and minimize the impact of changes.	43
Check Character	Added character which may be used to verify the accuracy of a string by a mathematical relationship to that string. [ISO/IEC FCD 7064 (09/2000)]	42
Check Character System	Set of rules for generating check characters and checking strings incorporating check characters. [ISO/IEC FCD 7064 (09/2000)]	42
Checksum	1. The sum of a group of data items, which sum is used for checking purposes. Note 1: A checksum is stored or transmitted with the group of data items. Note 2: The checksum is calculated by treating the data items as numeric values. Note 3: Checksums are used in error detecting and correcting. 2. [The] value computed on data to detect error or manipulation during transmission. See hash total. [INFOSEC-99] [FS-1037C]	42
Chemical Industry Data Exchange (CIDX)	A chemicals sector trade organization that owns the Chem eStandards®.	32
Chief Information Officer	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.	14, 15, 19
Chief Information	See Senior Agency Information Security Officer.	14

Term	Definition	Source
Security Officer		
Children's Online Privacy Protection Act (COPPA)	A U.S. law that took effect on April 21, 2000, and requires parental consent for certain Web sites to knowingly collect personally identifiable information on children under the age of 13.	43
Choice	An individual's ability to determine whether and how personally identifiable information collect from him or her may be used, especially for purposes beyond those for which the information was originally provided. Choice is an element of the Fair Information Practices.	43
Cipher	1. Cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys [ISO/IEC 18033-1] 2. A cipher is any cryptographic system in which arbitrary symbols, or groups of symbols, represent units of plain text of regular length, usually single letters, or in which units of plain text are rearranged, or both, in accordance with certain predetermined rules. 2. The result of using a cipher. *Note:* An example of a cipher is an enciphered or text. [FS-1037C]	41
Cipher	Alternative term for encryption algorithm. [ISO/IEC WD 18033-1 (12/2001)]	42
Cipher	The method used to transform a readable message (called plaintext or cleartext) into an unreadable, scrambled or hidden message (called ciphertext).	43
Cipher Block Chaining (CBC)	An encryption mode in which the plaintext of the current block is XORed with the previous ciphertext block before it is encrypted.	8, 10
Cipher Text	Enciphered information. [ISO 8372: 1987]	42
Ciphertext	Data in its encrypted form.	10
Ciphertext	Data which has been transformed to hide its information	41

Term	Definition	Source
	content [ISO/IEC 10116:1997]	
Ciphertext	Data which has been transformed to hide its information content. [ISO/IEC 9791-1: 1999, ISO/IEC 9798-1: 1997, ISO/IEC CD 10116 (12/2001), ISO/IEC WD 18033-1 (12/2001)]	42
Ciphertext	Data that has been encrypted. Ciphertext is the output of the encryption process and can be transformed back into a readable form plaintext with the appropriate decryption key.	43
Ciphertext Port	The CM communications port connected to a protected communication link. Communication on this port may be in plaintext or ciphertext.	10
Claimant	An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal. [ISO/IEC 9798-1: 1997]	42
Class	A grouping of families that share a common focus. [ISO/IEC 15408-1: 1999]	42
Cleared Personnel/Person	A person that has received an appropriate review, according to corporate policy. This could include background screening, and other periodic reviews.	13
Cleartext	Unencrypted data without format additions or changes, such as framing or padding.	10
Cleartext	*Synonym*: *Plaintext*. Unencrypted information. [INFOSEC-99] [FS-1037C]	41

Term	Definition	Source
Cleartext	Alternative term for plaintext. [ISO/IEC WD 18033-1 (12/2001)]	42
Cleartext	See plaintext.	43
Clickstream Data	Information that users generate as they move from page to page and click on items within a Web site, usually stored in log files. Web site designers can use clickstream data to improve users' experiences with a site.	43
Client	A device or program requesting a service.	10
Client	A device or application receiving or requesting services or information from a server application. [ATIS]	41
Clock Hour	The 60-minute period ending at :00. All surveys, measurements, and reports are based on Clock Hour periods unless specifically noted.	34
Closed Session	The session has been terminated and a new key is required for the next session.	10
Cogeneration	Production of electricity from steam, heat, or other forms of energy produced as a by-product of another process.	34
Collision-resistant Hash-function	A hash-function satisfying the following property: o it is computationally infeasible to find any two distinct inputs which map to the same output. NOTE - Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1: 2000, ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC WD 15946-4 (10/2001)] Hash-function satisfying the following property. o It is computationally infeasible to find any two distinct inputs which map to the same output. [ISO/IEC FDIS 9796-2 (12/2001), ISO/IEC FDIS 9797-2 (09/2000)]	42

Term	Definition	Source
Commissioning	The process of installing cryptographic protection on a system or portion of a system that has not been previously protected by cryptography.	10
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.	15
Common Security Control	Security controls that can be applied to one or more organizational information systems and have the following properties: (i) the development, implementation, and assessment of the controls can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the controls can be used to support the security certification and accreditation processes of organizational information systems where those controls have been applied.	14
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.	15
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization under strict terms and conditions in lieu of the prescribed security controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system.	14
Compliance Monitor	The entity that monitors, reviews, and ensures compliance of responsible entities with reliability standards.	34
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package. [ISO/IEC 15408-1: 1999]	42
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs).	1, 10
Computer Security	The protection of information assets through the use of technology, processes, and training.	43

Term	Definition	Source
Confidence	A belief that a deliverable will perform in the way expected or claimed (i.e. properly, trustworthy, enforce security policy, reliably, effectively). [ISO/IEC WD 15443-1 (11/2001)]	42
Confidential	Spoken, written, or electronic information that must be kept secret or in the confidence of a trusted employee; secret; private, entrusted with another's confidence or secret affairs, kept hidden or separate from the knowledge of others. Information that if released could case harm to the operator and that is only supplied on a need-to-know basis. (See Information Distribution for more details.)	13
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.	1, 10, 12
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	14, 15, 18
Confidentiality	1. Of classified or sensitive data, the degree to which the data have not been compromised; i.e., have not been made available or disclosed to unauthorized individuals, processes, or other entities. [After 2382-pt.8] 2. Assurance that information is not disclosed to unauthorized persons, processes, or devices. [INFOSEC-99] 3. A property by which information relating to an entity or party is not made available or disclosed to unauthorized individuals, entities, or processes. [T1.Rpt22-1993] [ATIS] 4. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST] 5. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 7498-2]	41
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation.	12, 15

Term	Definition	Source
Conformance test	A test performed by an independent body to determine if a particular piece of equipment satisfies the criteria in a specified controlling document, such as a Federal standard, an American National Standard, a Military Standard, or a Military Specification. Contrast with acceptance test. [FS-1037C]	41
Congestion Management Report	A report that the Interchange Distribution Calculator issues when a Reliability Coordinator initiates the Transmission Loading Relief procedure. This report identifies the transactions and native and network load curtailments that must be initiated to achieve the loading relief requested by the initiating Reliability Coordinator.	34
Congruence	Property of a set of integers which differ from each other by a multiple of the modulus. Congruence is indicated by the symbol ●●●●●●. For example, 39●●●●●● 6 (mod 11) indicates that 39 and 6 are congruent with respect to the modulus 11, i.e., 39 - 6 = 33, which is a multiple of 11. [ISO/IEC FCD 7064 (09/2000)]	42
Connectivity	The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration. [ISO/IEC 1548-1: 1999]	42
Constrained Facility	A transmission facility (line, transformer, breaker, etc.) that is approaching, is at, or is beyond its System Operating Limit or Interconnection Reliability Operating Limit.	34
Content Advisor	A tool in Microsoft Internet Explorer that lets you control which sites users on your computer can visit. This is particularly helpful for parents who want to control the content their children view on the Web.	43
Contingency	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element.	34
Contingency Reserve	The provision of capacity deployed by the Balancing Authority to meet the Disturbance Control Standard (DCS) and other NERC and Regional Reliability Organization contingency requirements.	34
Contract Path	An agreed upon electrical path for the continuous flow of electrical power between the parties of an Interchange	34

Term	Definition	Source
	Transaction.	
Control	In the context of information technology security, the term 'control' is normally considered to be synonymous with 'safeguard'. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Control Information	Information that is entered into a cryptographic module for the purposes of directing the operation of the module.	1, 10
Control Performance Standard (CPS)	The reliability standard that sets the limits of a Balancing Authority's Area Control Error over a specified time period.	34
Control System	Those facilities, systems, and equipment that comprise the operational real-time control environment, services, diagnostics, and functional capabilities necessary for the effective and reliable operation of the bulk electric system.	38, 39
Control System	A control system is a device or set of devices that manage the behaviour of other devices. Some devices or systems are not controllable. A control system is an interconnection of components connected or related in such a manner as to command, direct, or regulate itself or another system. There are two common types of controllers, with many variations and combinations: logic controls, and feedback or linear controls. There is also fuzzy logic, which attempts to combine the easy design of logic with the real-world utility of feedback controls. [WIKI]	41
Control System Operations	Control system operations encompass the collection of production, maintenance, and quality assurance operations with other activities of a manufacturing facility. Control system operations include: • facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials into end-products • functions that may be performed by physical equipment, human effort, and information systems • managing information about the schedules, use, capability, definition, history, and status of all of resources (personnel, equipment, and material) within the facility. [ISA SP99]	42

Term	Definition	Source
Controlled Access	Access in which the resources of an area or system is limited to authorized personnel, users, programs, processes, or other systems, and denied to all others.	13
Controlled Interface	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).	12, 14, 15
Cookie	A small data file that is stored on a user's local computer for record-keeping purposes and which contains information about the user that is pertinent to a Web site, such as user preferences.	43
COPPA	See Children's Online Privacy Protection Act.	43
Cost	Value impact to the organization or person that can be measured.	11
Counter (CTR)	An encryption mode, in which a set of input blocks, called counters, is fed to the cipher to produce a sequence of output blocks that are XORed with the plaintext to produce the ciphertext.	10
Counter	1. A device or register in a digital processor for determining and displaying the total number of occurrences of a specific event. 2. In the opposite direction. 3. Device or PC program element that can total binary events and perform ON/OFF actions based on the value of the total. 4. A device, register, or location in storage for storing numbers or number representations in a manner which permits these numbers to be increased or decreased by the value of another number, or to be changed or reset to zero or to an arbitrary value.	33
Counter	A bit array of length *n* bits which is used in the Counter Mode; its value when considered as the binary representation of an integer increases by one (modulo 2<SUPn) after each block of plaintext is processed [ISO/IEC CD 10116 (12/2001)]	42
Countermeasure	An action taken in opposition to a threat, or to reduce or eliminate vulnerabilities. They may be safeguards or secureguards.	32
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.	12, 14, 15

Term	Definition	Source
CRC	Cyclic Redundancy Check. A cyclic redundancy check (CRC) is a type of hash function used to produce a checksum – which is a small number of bits – against a byte or a larger block of data, such as a packet of network traffic or a block of a computer file. The checksum is used to detect and correct errors after transmission or storage. A CRC is computed and appended before transmission or storage, and verified afterwards by recipient to confirm that no changes occurred on transit. Correction can also be done if information lost is lower than information held by the checksum. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channels. [WIKI]	41
Credentials	Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names and passwords, smart cards, and certificates.	43
Critical Asset	Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.	36
Critical Assets	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System	35
Critical Assets	Those facilities, systems, and equipment, which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the bulk electric system, or would cause significant risk to public health and safety.	38, 39

Term	Definition	Source
Critical Cyber Assets	Cyber Assets essential to the reliable operation of Critical Assets.	35
Critical Cyber Assets	Those cyber assets essential to the reliable operation of critical assets.	39
Critical Security Parameter (CSP)	Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.	1, 10
Critical Update	A broadly released fix for a specific problem addressing a critical, non-security-relatedbug.	43
Crypto-algorithm	[A] well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc. [INFOSEC-99] [ATIS]	41
Cryptographic Algorithm for Confidentiality	A cryptographic algorithm for confidentiality is defined as an algorithm which transforms data in order to hide or reveal its information content and which uses at least one secret parameter. This definition includes both symmetric algorithms (e.g. DES and FEAL) and asymmetric algorithms (e.g. RSA and Rabin). In the case of a symmetric algorithm the data is hidden and revealed using a secret parameter. In the case of an asymmetric algorithm the data is hidden using a public parameter and revealed using a secret parameter. [ISO/IEC 9979: 1999]	42
Cryptographic Boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.	1, 10
Cryptographic Check Function	A cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall be infeasible. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Cryptographic Check Value	Information which is derived by performing a cryptographic transformation on the data unit. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999]	42

Term	Definition	Source
	Information which is derived by performing a cryptographic transformation on the data unit. NOTE - The cryptographic check value is the output of the cryptographic check function. [ISO/IEC FDIS 15946-3 (02/2001)]	
Cryptographic hash	1. Function that maps octet strings of any length to octet strings of fixed length, such that it is computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infeasible to predict any bit of the remaining output. The precise security requirements depend on the application. [ISO/IEC FDIS 18033-2: 2005-11-29] 2. A mathematical function that maps values from a large (or even very large) domain into a smaller range, and is (a) one-way in that it is computationally infeasible to find any input which maps to any pre-specified output; and (b) collision-free in that it is computationally infeasible to find any two distinct inputs which map to the same output. [After X9.31] [ATIS]	41
Cryptographic Key (key)	A parameter used in conjunction with a cryptographic algorithm that defines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret.	1, 10
Cryptographic key	A mathematical value that is used (a) in an algorithm to generate cipher text from plain text or vice versa, and (b) to determine the operation of a cryptographic function (e.g., the synchronized generation of keying material), or a digital signature computation or validation. [After X9.31] [ATIS]	41
Cryptographic Key Component (key component)	One of two or more secret numbers that are combined to produce a key using split knowledge procedures.	10
Cryptographic Module (CM)	The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is	10

Term	Definition	Source
	contained within the cryptographic boundary.	
Cryptographic Module	The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and are contained within the cryptographic boundary.	1
Cryptographic module security policy	A precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor. [1]	10
Cryptographic Module Security Policy	A precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this standard and additional rules imposed by the vendor.	1
Cryptographic Synchronization	The co-ordination of the encipherment and decipherment processes. [ISO 8372: 1987, ISO/IEC CD 10116 (12/2001)]	42
Cryptography	The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.	7, 10
Cryptography	1. [The] art or science concerning the principles, means, and methods for rendering plain information unintelligible, and for restoring encrypted information to intelligible form. [INFOSEC-99] 2. The branch of cryptology that treats of the principles, means, and methods of designing and using cryptosystems. [ATIS] 3. The discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [ISO/IEC 2nd WD 18014-2: 2006-04-04]	41
Cryptography	The study or analysis of codes and encoding methods used to secure information. Cryptographic techniques can be used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation.	43

Term	Definition	Source
Cryptoperiod	The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect.	10
Cryptosystem	A collective of keys, algorithms, hardware, software and security policies that are employed to provide cryptographic services to an organization.	10
Curtailment	A reduction in the scheduled capacity or energy delivery of an Interchange Transaction.	34
Curtailment Threshold	The minimum Transfer Distribution Factor which, if exceeded, will subject an Interchange Transaction to curtailment to relieve a transmission facility constraint.	34
Cyber	Of, relating to, or involving computers or computer networks.	32
Cyber	*Loosely,* a prefix referring to anything related to computers or networking. *Note 1:* For example, a “cyber I” is a coffee shop that offers computer terminals for customers to browse the Internet while sipping coffee, and a “cyber sleuth” is an investigator who researches and attempts to solve or find the cause of, unusual Internet occurrences. *Note 2:* While “cyber” is listed herein as colloquial, its use has become ubiquitous and it is rapidly becoming accepted as formal language. [ATIS]	41
Cyber Assets	Programmable electronic devices and communication networks including hardware, software, and data.	35
Cyber Attack	Exploitation of the software vulnerabilities of information technology-based control components.	10
Cyber Attack	*See Attack*	41
Cyber Security	*Synonym: Information Security.* The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [ATIS]	41
Cybersecurity	The protection of digital systems and their support systems from threats of:	32

Term	Definition	Source
	• Cyberspace attack by adversaries who wish to disable or manipulate them. • Physical attack by adversaries who wish to disable or manipulate them. • Access by adversaries who want to obtain, corrupt, damage or destroy sensitive information. This is an aspect of information security. Electronic data can be obtained by theft of computer storage media or by hacking into the computer system. Note that a cyberspace attack may be mounted to obtain sensitive information to plan a future physical or cyberspace attack.	
Cyber Security Incident	Any malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.	35
Cybersecurity Vulnerability Assessment Methodology (Cybersecurity VAM)	The methodology used to identify and analyze cyber threat scenarios.	32
Cyclic Redundancy Check (CRC)	A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected. Sometimes called "cyclic redundancy code".	10
Cyclic Redundancy Check Character (CRC)	A character used in a modified cyclic code for error detection and correction.	33
Data	Information stored on a computer, usually formatted in a special way.	32
Data	1. Information of any type. 2. A common term used to indicate the basic elements that can be processed or produced by a computer.	33
Data Authentication	A process used to verify data integrity, e.g., verification that data received are identical to data sent, or verification that a program is not infected by a virus. [After 2382-pt.8] [ATIS]	41

Term	Definition	Source
Data Corruption	An accidenAn accidental or intentional violation of data integrity. [2382-pt 8 [ATIS [AT [ATIS]	41
Data Encryption Standard (DES)	1. [A] cryptographic algorithm for the protection of unclassified computer data and published by the National Institute of Standards and Technology in Federal Information Processing Standard Publication 46-1. [NIS] Note: DES is not approved for protection of national security classified information. [FS-1037C] 2. A well-known symmetric encryption mechanism using a 56 bit key. Due to its short key length DES was replaced by the AES, but is still used in multiple encryption mode, e.g., 3DES or Triple DES (FIPS 46-3). [ISO/IEC 18028-4: 2005-04-01]	41
Data Input	A data item which depends on the entire message and forms a part of the input to the signature function. [ISO/IEC 9796-3: 2000] A data item which depends on the entire message and forms a part of the input to the signature function. NOTE – Signature generation function is the signature process which is determined by signature key and the domain parameter. [ISO/IEC WD 15946-4 (10/2001)]	42
Data Integrity	1. [The] condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [NIS] 2. The condition in which data are identically maintained during any operation, such as transfer, storage, and retrieval. [FIPS 140-2]88) 3. The preservation of data for their intended use. 4. Relative to specified operations, the a priori expectation of data quality. [FS-1037C]	41
Data Integrity	The property that data has not been altered or destroyed in an unauthorized manner. [ISO/IEC 9797-1; 1999]	42
Data Items' Representation	A data item or some representation thereof such as a cryptographic hash value. [ISO/IEC FDIS 18014-1 (02/2002)]	42
Data Object (DO)	Part of a logical node object representing specific information, e.g., status or measurement. From an object-oriented point of view a data object is an instance of a class data object. Dos are normally used as transaction objects; i.e., they are data structures. [IEC 61850]	41
Data Security	[The] protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. [INFOSEC-99]	41
Data Storage	A means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority. [ISO/IEC WD 13888-1 (11/2001)]	42

Term	Definition	Source
Data String (Data)	String of bits which is theinput to a hash-function. [ISO/IEC FDIS 9797-2 (09/2000)] A string of bits which is the input to a hash-function. [ISO/IEC 10118-1: 2000]	42
Data Transfer	As a key principle of privacy, the movement of personally indentifiable information between entities, such as a customer list being shared between two different companies.	43
Datagram	In packet switching, a self-contained packet, independent of other packets, that contains information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on prior exchanges between the equipment and the network. Note: Unlike virtual call service, when datagrams are sent there are no call establishment or clearing procedures. Thus, the network may not be able to provide protection against loss, duplication, or misdelivery. [ATIS]	41
DCS	A distributed control system (DCS) is part of a manufacturing system. Distributed control systems (DCS) are used in industrial and civil engineering applications to monitor and control distributed equipment with remote human intervention. [WIKI]	41
DDoS	See distributed denial of service	43
Deceptive Trade Practices	Misleading or misrepresenting products or services to consumers and customers. In the United States, these practices are regulated by the Federal Trade Commission at the national level and typically by the Attorney General's Office of Consumer Protection at the state level.	43
Decipherment	The reversal of a corresponding encipherment. [ISO/IEC 9797-1; 1999, ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] Alternative term for decryption. [ISO/IEC WD 18033-1 (12/2001)]	42
Decode	1. To convert data by reversing the effect of previous encoding. [FIPS 140-2]88) 2. To interpret a code. 3. [To] convert encoded text into equivalent plain text by means of a code. [NIS] [FIPS 140-2]88) Note: Decoding does not include deriving plain text by cryptanalysis. [FS-1037C]	41
Decrypt	1. [A] generic term encompassing decode and decipher. [NIS] 2. To convert encrypted text into its equivalent plain text by means of a cryptosystem. (This does not include solution by cryptanalysis.) Note: The term “decrypt” covers the meanings of “decipher” and “decode.” [JP1] [FS-1037C]	41
Decryption	The process of changing ciphertext into plaintext using a	10

Term	Definition	Source
	cryptographic algorithm and key.	
Decryption	1. Reversal of a corresponding encryption. [ISO/IEC 18033-1] 2. The process of changing ciphertext into plaintext using a cryptographic algorithm and key. [RFC2828]	41
Decryption	Reversal of a corresponding encipherment. [ISO/IEC WD 18033-1 (12/2001)]	42
Decryption	The process of converting encrypted content back into its original form, often the process of converting ciphertext to plaintext. Decryption is the opposite of encryption.	43
De-Facto Standard	A standard that is widely accepted and used, but lacks formal approval by a recognized standards organization. [FS-1037C]	41
Defence in Depth	Defence in depth is a military strategy sometimes also called elastic defence. Defence in depth seeks to delay rather than prevent the advance of an attacker, buying time by yielding space. The idea of defence in depth is now widely used to describe non-military strategies. [WIKI] In security, it is a security architecture based on the idea that any one point of protection may, and probably will, be defeated. It implies layers of security and detection, even on single systems and provides the following features: • Attackers are faced with breaking through or bypassing each layer without being detected. • A flaw in one layer can be protected by capabilities in other layers. • System security becomes a set of layers within the overall network security. Security is improved by requiring the attacker to be perfect while ignorant [ISA SP99]	41
Deliverable	The object of an assurance assessment. An object may be a Protection Profile (PP) or Security Target (ST) as defined by ISO 15408 or a product, system, service, process, or environmental factor (i.e. personnel, organisation). NOTE – ISO 9000:2000 holds that a service is a type of product and “product and/or service” when used in the ISO 9000 family of standards. [ISO/IEC WD 15443-1 (11/2001)]	42

Term	Definition	Source
Delivery Authority	An authority trusted by the sender to deliver the data from the sender to the receiver, and to provide the sender with evidence on the submission and transport of data upon request. [ISO?IEC WD 13888-1 (11/2001)]	42
Demand	1. The rate at which electric energy is delivered to or by a system or part of a system, generally expressed in kilowatts or megawatts, at a given instant or averaged over any designated interval of time. 2. The rate at which energy is being used by the customer.	34
Demand-Side Management (DSM)	The term for all activities or programs undertaken by Load-Serving Entity or its customers to influence the amount or timing of electricity they use.	34
Demilitarized Zone	Perimeter network segment that is logically between internal and external networks. It purpose is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.	12
Demilitarized Zone	DMZ is a term used in complex firewall configurations, where a device is placed outside the firewall, but is still available for use by the internal (protected) network.	13
Denial-of-Service (DOS)	The prevention of authorized access to a system resource or the delaying of system operations and functions. (See "interruption.")	10
Denial-of-Service (DOS)	1. The prevention of authorized access to resources or the delaying of time-critical operations. [2382-pt.8] 2. The result of any action or series of actions that prevents any part of an information system (IS) from functioning. [INFOSEC-99] [ATIS] 3. The prevention of authorized access to a system resource or the delaying of system operations and functions. (*See*: *availability, critical (resource of a system), flooding.*) [RFC2828]	41
Denial of Service Attack (DoS)	An attempt by a malicious (or unwitting) user, process, or system to prevent legitimate users from accessing a resource (usually a network service) by exploiting a weakness or design limitation in an information system. Examples of DoS attacks include flooding network connections, filling disk storage, disabling ports, or removing power.	43

Term	Definition	Source
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives. [ISO/IEC 15408-1: 1999]	42
Designated Approving Authority (DAA)	[The] official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. *Synonyms:* accrediting authority, delegated accrediting authority, designated accrediting authority. [INFOSEC-99] [ATIS]	41
Deterministic	Independent of a randomizer, not randomized. [ISO?IEC 14888-1: 1998]	42
Device	A mechanism or piece of equipment designed to serve a purpose or perform a function. (IEEE Std 100-1996, IEEE Dictionary of Electrical and Electronic Terms); e.g., breaker, relay, or distributed energy resource.	41
Device Certificate	In cryptography, a public key certificate or an attribute certificate, issued by a device manufacturer, tying the identity of the device to its attributes. [After X9.45] [ATIS]	41
Diffie-Hellman Key Exchange	Diffie-Hellman key exchange is a cryptographic protocol which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a	41

Term	Definition	Source
	symmetric key cipher. [WIKI]	
Digital Certificate	A digitally signed statement that binds the identifying information of a user, computer, or service to a public/private key pair. A digital certificate is commonly used in the process of authentication and for securing information on networks.	43
Digital Data	**1.** Data represented by discrete values or conditions, as opposed to analogue data. **2.** Discrete representations of quantized values of variables, *e.g.*, the representation of numbers by digits, perhaps with special characters and the "space" character. [ATIS]	41
Digital Rights Management (DRM)	Any technology used to protect the interests of owners of content and services (such as copyright owners). Typically, authorized recipients or users must acquire a license in order to consume the protected material—files, music, movies—according to the rights or business rules set by the content owner.	43
Digital Signature	The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation.	1, 10
Digital Signature	1. Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO/IEC 13888-1: 2004-06-01] 2. A cryptographic modification of data that provides: (a) origin authentication, (b) data integrity, and (c) signer non-repudiation (when associated with a data unit and accompanied by the corresponding public-key certificate). [After X9.49] A cryptographic process used to assure	41

Term	Definition	Source
	message originator authenticity, integrity, and non-repudiation. Synonym electronic signature. [INFOSEC-99] [ATIS] 3. The result of a cryptographic transformation of data which, when properly implemented, provides the services of: • origin authentication• data integrity• signer non-repudiation. [FIPS 140-2]	
Digital Signature	A data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient. [ISO/IEC 11770-3: 1999] Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery, e.g. by the recipient. [ISO/IEC FDIS 15946-3 (02/2001)] A cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient. NOTE - Digital signatures may be used by end entities (see below) for the purposes of authentication, of data integrity, and of non-repudiation of creation of data. The usage for non repudiation of creation of data is the most important one for legally binding digital signatures. [ISO/IEC 15945: 2002]	42
Digital Signature (Signature)	Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery, e.g. by the recipient. [ISO/IEC 9798-1: 1997]	42
Digital Signature	Data that binds a sender's identity to the information being sent. A digital signature may be bundled with any message, file, or other digitally encoded information, or transmitted separately. Digital signatures are used in public key environments and provide nonrepudiation and integrity services.	43

Term	Definition	Source
Digital Signature Standard (DSS)	A standard for digital signing, including the Digital Signing Algorithm, approved by the National Institute of Standards and Technology, defined in NIST FIPS PUB 186, "Digital Signature Standard," published May, 1994 by the U.S. Dept. of Commerce. [NIST]	41
Direct Control Load Management (DCLM)	Demand-Side Management that is under the direct control of the system operator. DCLM may control the electric supply to individual appliances or equipment on customer premises. DCLM as defined here does not include Interruptible Demand.	34
Directly Trusted CA	A directly trusted CA is a CA whose public key has been obtained and is being stored by an end entity in a secure, trusted manner, and whose public key is accepted by that end entity in the context of one or more applications. [ISO/IEC 15945: 2002]	42
Directly Trusted CA Key	A directly trusted CA key is a public key of a directly trusted CA. It has been obtained and is being stored by an end entity in a secure, trusted manner. It is used to verify certificates without being itself verified by means of a certificate created by another CA. NOTE - If for example the CAs of several organizations cross-certify each other (see Annex A) the directly trusted CA for an entity may be the CA of the entity's organization. Directly trusted CAs and directly trusted CA keys may vary from entity to entity. An entity may regard several CAs as directly trusted CAs. [ISO/IEC 15945: 2002]	42
Directory Service	A service to search and retrieve information from a catalogue of well defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses etc. An example is provided by a directory service conforming to the ITU-T Recommendation X.500. [ISO/IEC 15945: 2002]	42
Disclosure	A component of the notice principle, wherein a company should make available its data handling practices, including notices on how it collects, uses, and shares personally identifiable information.	43

Term	Definition	Source
Dispersed Load by Substations	Substation load information configured to represent a system for power flow or system dynamics modeling purposes, or both.	34
Distinguishing Identifier	Information which unambiguously distinguishes an entity. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-2: 1996, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] Information which unambiguously distinguishes an entity in the non-repudiation process. [ISO/IEC WD 13888-1 (11/2001)]	42
Distributed	See Distributed Control Systems (DCS).	33
Distributed Control Systems (DCS)	A DCS is a type of plant automation system similar to a SCADA system, except that a DCS is usually employed in factories and is located within a more confined area. It uses a high-speed communications medium, which is usually a separate wire (network) from the plant LAN. A significant amount of a closed loop control is present in the system	32
Distributed Control Systems (DCS)	In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit.	33
Distributed Denial of Service (DDoS)	A type of denial of service attack in which an attacker uses malicious code installed on various computers to attack a single target. An attacker may use this method to have a greater effect on the target than is possible with a single attacking machine.	43
Distribution Factor (DF)	The portion of an Interchange Transaction, typically expressed in per unit, that flows across a transmission facility (Flowgate).	34
Distribution Provider	Provides and operates the “wires” between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the Transmission Owner also serves as the Distribution Provider. Thus, the Distribution Provider is not defined by a specific voltage, but rather as performing the Distribution function at any voltage.	34
Disturbance	1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.	34
Disturbance Control Standard (DCS)	The reliability standard that sets the time limit following a Disturbance within which a Balancing Authority must return	34

Term	Definition	Source
	its Area Control Error to within a specified range.	
Domain Modulus	A domain parameter, which is a positive integer resulting from the product of two distinct primes which are known only to the trusted third party. [ISO/IEC 14888-2; 1999	42
Domain Parameter	A data item which is common to and known by or accessible to all entities within the domain. [ISO/IEC 14888-1: 1998] A data item which is common to and known by or accessible to all entities within the domain. NOTE - The set of domain parameters may contain data items such as hash-function identifier, length of the hash-token, length of the recoverable part of the message, finite field parameters, elliptic curve parameters, or other parameters specifying the security policy in the domain. [ISO/IEC 9796-3: 2000, ISO/IEC WD 15946-4 (10/2001)] A data item which is common to and known by or accessible to all entities within the domain. NOTE. The set of domain parameters may contain data items such as hash-function identifier, elliptic curve parameters, or other parameters specifying the security policy in the domain. [ISO/IEC FDIS 15946-2 (04/2001)]	42
Domain Verification Exponent	A domain parameter which is a positive integer. [ISO/IEC 14888-2; 1999]	42
DoS	See denial of service attack.	43
Download	To transfer a copy of a file from a remote computer to a requesting computer by means of a modem or network.	43
DRM	See digital rights management.	43
Dual Homed Bridge	A dual-homed computer is a computer that has multiple network interfaces: these are multiple interfaces, some of which are attached to the untrusted network and others of which are attached to the trusted network. The machine acts as a bridge to pass information between the two networks. Not the same as two network interface boards used for redundancy.	13
Dual Homed Gateway	A dual-homed gateway is a computer that runs firewall software and has multiple network interfaces: these are multiple interfaces, some of which are attached to the untrusted network and others of which are attached to the trusted network. A dual-homed gateway relays information	13

Term	Definition	Source
	between the two networks and restricts contact between unauthorized devices. Both circuit-level gateways and application level gateways are dual-homed gateways.	
Dynamic Interchange Schedule or Dynamic Schedule	A telemetered reading or value that is updated in real time and used as a schedule in the AGC/ACE equation and the integrated value of which is treated as a schedule for interchange accounting purposes. Commonly used for scheduling jointly owned generation to or from anotherBalancing [sic] Authority Area.	34
Dynamic Transfer	The provision of the real-time monitoring, telemetering, computer software, hardware, communications, engineering, energy accounting (including inadvertent interchange), and administration required to electronically move all or a portion of the real energy services associated with a generator or load out of one Balancing Authority Area into another.	34
Economic Dispatch	The allocation of demand to individual generating units on line to effect the most economical production of electricity.	34
EFS	See Encrypting File System.	43
Electrical Energy	The generation or use of electric power by a device over a period of time, expressed in kilowatthours (kWh), megawatthours (MWh), or gigawatthours (GWh).	34
Electronic Codebook (ECB)	A block cipher mode in which a plaintext block is used directly as input to the encryption algorithm and the resultant output block is used directly as ciphertext.	10
Electronic Deception	1. The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons. Note: Among the types of electronic deception are: (a) manipulative electronic deception—Actions to eliminate revealing or convey misleading, telltale indicators that may be used by hostile forces; (b) simulative electronic deception—Actions to represent friendly notional or actual capabilities to mislead hostile forces; (c) imitative electronic deception—The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. 2. Deliberate activity designed to mislead an enemy in the interpretation or use of information received by his electronic systems. [FS-	41

Term	Definition	Source
	1037C]	
Electronic Security	Includes the concepts of identification, authentication, accountability, authorization, availability and privacy. The objective is to preclude unauthorized use, modifications to, disclosure, loss of revenue or destruction of critical systems or informational assets in an effort to reduce the risk of personal injury or possibility of endangering public health, loss of public or consumer confidence, disclosure of sensitive assets, and protection of business assets. These concepts are applied to any system in the production process and include both standalone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems.	11
Electronic Security Perimeter	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.	35, 39
Element	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components.	34
Element	An indivisible security requirement. [ISO/IEC 15408-1: 1999]	42
Elevation of Privilege	The process by which a user obtains a higher level of privilege than that for which he has been authorized. A malicious user may use elevation of privilege as a means to compromise or destroy a system, or to access unauthorized information.	43
Eliminated	To be rid of, or having removed a threat.	13
E-mail Bomb	A denial of service attack in which an excessive amount of e-mail data is sent to an e-mail address in an attempt to disrupt the e-mail service, or to prevent the recipient from receiving	43

Term	Definition	Source
	legitimate messages.	
Emergency or BES Emergency	Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System.	34
Emergency Rating	The rating as defined by the equipment owner that specifies the level of electrical loading or output, usually expressed in megawatts (MW) or MVar or other appropriate units, that a system, facility, or element can support, produce, or withstand for a finite period. The rating assumes acceptable loss of equipment life or other physical or safety limitations for the equipment involved.	34
Empty Position	A bit position of an array of bits to which no value is assigned. [ISO/IEC CD 10116 (12/2001)]	42
EM/RF	Electromagnetic and radio frequency	41
Emulate	To represent a system by a model that accepts the same inputs and produces the same outputs as the system represented. For example, to emulate an 8-bit computer with a 32-bit computer.	10
Emulate	To imitate one system with another such that the imitating system accepts the same data, executes the same programs, and achieves the same results as the imitated system.	33
Emulator	1. A device or program that emulates, usually done by microprogramming the imitating system. Contrasted to simulate. 2. A computer that behaves very much like another computer by means of suitable hardware and software.	33
Encipherment	The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the data. [ISO/IEC CD 10116 (12/2001)] The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO/IEC 9797-1: 1999, ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42

Term	Definition	Source
	Alternative term for encryption. [ISO/IEC WD 18033-1 (12/2001)]	
Encipherment Algorithm	Alternative term for encryption algorithm. [ISO/IEC WD 18033-1 (12/2001)]	42
Encrypt	1. [A] generic term encompassing encipher and encode. [INFOSEC-99] 2. To convert plain text into unintelligible forms by means of a cryptosystem. *Note*: The term encrypt covers the meanings of encipher and encode. [JP1-02] [ATIS]	41
Encrypted Data	Data that has been converted from plaintext into ciphertext.	43
Encrypting File System (EFS)	A technology used in Windows 2000 and later versions that enables users to encrypt files and folders on NTFS volumes. EFS protects the confidentiality of data by ensuring that only the original user has access to them.	43
Encryption	Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state. [RFC 2828]	10
Encryption	1. (Reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO/IEC 18033-1] 2. The process of changing plaintext into ciphertext using a	41

Term	Definition	Source
	cryptographic algorithm and key. [RFC2828]	
Encryption	(Reversible) transformation of data by a cryptographic algorithm to produce ciphertext, I.e. to hide the information content of the data. [ISO/IEC WD 18033-1 (12/2001)]	42
Encryption	The process of converting data into a coded form (ciphertext) to prevent it from being read and understood by an unauthorized party.	43
Encryption Algorithm	Cryptographic technique used to protect the confidentiality of data. An encryption algorithm consists of two processes: encryption (or encipherment) which transforms plaintext into ciphertext, and decryption (or decipherment) which transforms ciphertext to plaintext. [ISO/IEC WD 18033-1 (12/2001)]	42
Encryption Appliance	Network-attached devices that offload encryption from a computer's CPU and main memory. Examples of encryption appliances are a communication channel encryptor for serial communications, a VPN gateway, or an SSL accelerator or gateway.	10
Energy Emergency	A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers' expected energy requirements.	34
Enforcement	A privacy principle which provides mechanisms for assuring compliance with the Fair Information Practices, recourse for individuals affected by noncompliance, and consequences for noncompliant organizations. Methods for enforcement include a review by independent third parties, such as BBBOnLine.	43
Entity	An individual, organization, device or process.	10
Entity	An active element within an OSI layer (e.g. Token Bus MAC is an entity in the Layer 2). [Editor's note: ISA definition of OSI: Abbreviation for open system interconnection (a connection between one communication system and another	33

Term	Definition	Source
	using a standard protocol).]	
Entity	The facility or critical asset owner, operator, etc.	36
Entity Authentication	The corroboration that an entity is the one claimed. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-2: 1996, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Entity Authentication of A to B	The assurance of the identity of entity A for entity B. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Entry Label	The naming information that identifies a registered PP or package uniquely. [ISO/IEC 15292: 2001]	42
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.	12, 14
Environment	The ambient natural and artificial conditions that surround a piece of operating equipment.	33
ES-Cyber-GREEN (Low)	ES-Cyber-GREEN condition applies when there is no known threat of cyber attack or only a general concern about hacker activity that warrants only routine security procedures. Any cyber security measures applied should be maintainable indefinitely and without adverse impact to business or expenses. This may be equivalent to normal daily conditions.	37
ES-Cyber-BLUE (Guarded)	ES-Cyber-BLUE condition applies when there is a general threat of increased cyber (hacker intrusions, viruses, etc.) activity with no specific threat directed toward the electric industry. Additional cyber security measures may be necessary, and if initiated they should be maintainable for an indefinite period of time with minimum impact on normal business or expenses.	37
ES-Cyber-YELLOW (Elevated)	ES-Cyber-YELLOW condition applies when a general threat exists of disruptive cyber activity directed against the electric industry. Implementation of additional cyber security measures is expected. Such measures are anticipated to last for an indefinite period of time.	37
ES-Cyber-ORANGE (High)	ES-Cyber-ORANGE condition applies when a credible threat exists of disruptive cyber activity directed against the electric industry. Additional cyber security measures have been implemented. Business entities need to be aware that corporate resources will be required above and beyond those required for normal business or expenses.	37
ES-Cyber-RED (Severe)	ES-Cyber-RED Condition applies when an incident occurs or credible intelligence information is received by the electric industry indicating a disruptive cyber attack against the	37

Term	Definition	Source
	electric industry is imminent or has occurred. This condition may apply as a result of an incident in North America outside of the Electricity Sector. Maximum cyber security measures are necessary. Implementation of such measures could cause hardship on personnel and seriously impact facility business and security activities.	
EU Data Protection Directive	A European Union (EU) law stating that personal data from EU countries can only be transferred to non-EU countries that provide an acceptable level of privacy protection. An organization must inform individuals why information about them is collected, how to contact the organization with inquiries and complaints, the types of third parties to which the organization will disclose, and the options an organization provides to limit the disclosure of certain information. Proper notice and choice must be offered to allow an individual to opt in or opt out of providing specific information the organization plans on tracking. See also Safe Harbor Agreement.	43
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria. [ISO/IEC 15408-1: 1999] Assessment of a deliverable against defined criteria. [ISO/IEC WD 15443-1 (11/2001)]	42
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale. [ISO/IEC 15408-1: 1999]	42
Evaluation Authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community. [ISO/IEC 15408-1: 1999]	42
Evaluation Pass Statement	A statement issued by an organisation that performs evaluations against ISO/IEC 15408 confirming that a PP has successfully passed assessment against the evaluation criteria given in clause 4 of Part 3 of that International Standard. [ISO/IEC 15292: 2001]	42
Evaluation Scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community. [ISO/IEC 15408-1: 1999]	42
Event	An occurrence of some specific data, situation or activity. [ISO/IEC DTR 15947 (10/2001)]	42

Term	Definition	Source
Evidence	Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. NOTE - Evidence does not necessarily prove truth or existence of something (see proof) but contributes to establish proof. [ISO/IEC WD 13888-1 (11/2001)]	42
Evidence Requester	An entity requesting an evidence to be generated either by another entity or by a trusted third party. [ISO/IEC WD 13888-1 (11/2001)]	42
Evidence Subject	The entity responsible for the action, or associated with the event, with regard to which evidence is generated. [ISO/IEC WD 13888-1 (11/2001)]	42
Exchange Multiplicity Parameter	Positive integer used to determine how many times the exchange of entity authentication messages shall be performed in one instance of the authentication mechanism. [ISO/IEC 9798-5: 1999]	42
Executive Agency	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.	14, 15, 20
Explicit Key Authentication from A to B	The assurance for entity B that A is the only other entity that is in possession of the correct key. **NOTE - Implicit key authentication from A to B and key confirmation from A to B together imply explicit key authentication from A to B. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]**	42
Exploit	A defined way to breach the security of an IT system through a vulnerability. [ISO/IEC DTR 15947 (10/2001)]	42
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC. [ISO/IEC 15408-1: 1999]	42
External IT Entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE. [ISO/IEC 15408-1: 1999]	42

Term	Definition	Source
Extranet	An extranet can be viewed as a part of a company's intranet that is extended to users outside the company. It has also been described as a "state of mind," in which the Internet is perceived as a way to do business with other companies as well as to sell products to customers.	13
Extranet	An extension of an organization's intranet used to facilitate communication with the organization's trusted partners. An extranet allows such trusted partners to gain limited access to the organization's internal business data.	43
Facility	A plant, building, structure, or complex contiguously located on the same site, defined by a single geographical perimeter (usually determined by a fence or other barrier that surrounds and limits uncontrolled access), and used by the operator or its contractors for the performance of work under the jurisdiction of the operator. The term "facility" includes the land (soil), surface water, and groundwater contained within its geographical perimeter.	13
Facility Rating	The maximum or minimum voltage, current, frequency, or real or reactive power flow through a facility that does not violate the applicable equipment rating of any equipment comprising the facility.	34
Fair Information Practices	The basis for privacy best practices, both online and offline. The Practices originated in the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the U.S. government. In 1980, these principles were adopted by the Organization for Economic Cooperation and Development and incorporated in its Guidelines for the Protection of Personal Data and Transborder Data Flows. They were adopted later in the EU Data Protection Directive of 1995, with modifications. The Fair Information Practices include notice, choice, access, onward transfer, security, data integrity, and remedy.	43
Fault	An event occurring on an electric system such as a short circuit, a broken wire, or an intermittent connection.	34
Family	A grouping of components that share security objectives but may differ in emphasis or rigour. [ISO/IEC 15408-1: 1999]	42
Federal Agency	See Agency.	14
Federal Enterprise Architecture	A business-based framework for government wide improvement developed by the Office of Management and	15, 21

Term	Definition	Source
	Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.	
Federal Information System	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.	14, 15, 22
Feedback Buffer (FB)	Variable used to store input data ffor the encipherment process. At the starting point FBCA has the value of SV. [ISO/IEC CD 10116 (12/2001)]	42
Field Device	A component of a control system that resides level 0, 1 or 2 of the ISA-95, Purdue CIM model. Field devices can collect measurements from sensors or issue control commands that modify a process. Field devices may make logic and control calculations and communicate with an IT application. Examples of field devices include Ply's, RTU's, PAC's and IED's.	40
File Transfer Protocol	FTP is an Internet standard for transferring files over the Internet. FTP programs and utilities are used to upload and download webpages, graphics, and other files from your hard drive to a remote server which allows FTP access.	13
Filter	A pattern or mask through which data is passed to separate specified items. For instance, a filter used in e-mail or in retrieving newsgroup messages can allow users to automatically discard messages from designated users.	43
Financial Modernization Act of 1999	See Gramm-Leach-Bliley Act.	43
Finite Commutative Group	A finite set J with the binary operation "*" such that: For all a, b, c ●J, $(a*b)*c = a*(b*c)$. There exists e ● J with $e*a = a$ for all a ·●J. For all a ·● J there exists b ● J with $b*a = e$. For all a, b·● J, $a*b = b*a$. [ISO/IEC 14888-3: 1998]	42
Firewall	System designed to defend against unauthorized access to or from a private network. [CNSS]	12
Firewall	A set of programs residing on a gateway server that protect the resources of an internal network. Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall is often installed in a specially designated computer that is separate from the rest of the network so that no incoming request can get directly at	13

Term	Definition	Source
	private network resources. There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.	
Firewall	A security solution which segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic filtering rules.	43
Firm Demand	That portion of the Demand that a power supplier is obligated to provide except when system reliability is threatened or during emergency conditions.	34
Firm Transmission Service	The highest quality (priority) service offered to customers under a filed rate schedule that anticipates no planned interruption.	34
Firmware	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.	1, 10
Firmware	Programs or instructions that are permanently stored in hardware memory devices (usually read-only memories) that control hardware at a primitive level.	33
Flowgate	A designated point on the transmission system through which the Interchange Distribution Calculator calculates the power flow from Interchange Transactions.	34
Forced Outage	1. The removal from service availability of a generating unit, transmission line, or other facility for emergency reasons. 2. The condition in which the equipment is unavailable due to unanticipated failure.	34
Formal	Expressed in a restricted syntax language with defined semantics based on wellestablished mathematical concepts. [ISO/IEC 15408-1: 1999]	42
Forward Secrecy with Respect to A	The property that knowledge of A's long-term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys. [ISO/IEC FDIS 15946-3 (02/2001)]	42

Term	Definition	Source
Forward Secrecy with Respect to Both A and B Individually	The property that knowledge of A's long-term private key or knowledge of B's long term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys. NOTE - This differs from mutual forward secrecy in which knowledge of both A's and B's long term private keys does not enable recomputation of previously derived keys. [ISO/IEC FDIS 15946-3 (02/2001)]	42
Frequency Bias	A value, usually expressed in megawatts per 0.1 Hertz (MW/0.1 Hz), associated with a Balancing Authority Area that approximates the Balancing Authority Area's response to Interconnection frequency error.	34
Frequency Bias Setting	A value, usually expressed in MW/0.1 Hz, set into a Balancing Authority ACE algorithm that allows the Balancing Authority to contribute its frequency response to the Interconnection.	34
Frequency Deviation	A change in Interconnection frequency.	34
Frequency Error	The difference between the actual and scheduled frequency. (F_A – F_S)	34
Frequency Regulation	The ability of a Balancing Authority to help the Interconnection maintain Scheduled Frequency. This assistance can include both turbine governor response and Automatic Generation Control.	34
Frequency Response	(Equipment) The ability of a system or elements of the system to react or respond to a change in system frequency. (System) The sum of the change in demand, plus the change in generation, divided by the change in frequency, expressed in megawatts per 0.1 Hertz (MW/0.1 Hz).	34
Full File Replacement	A technology used in hotfixes that replaces the currently installed files with new files. Compare patching.	43
Functions	Tasks which are performed through automation by computer systems with or without direct user interactions. Functions rely on one or more software applications that may exchange	41

Term	Definition	Source
	data with other applications. {Common Usage]	
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.	15, 17
Generator-to-Load Distribution Factor (GLDF)	The algebraic sum of a Generator Shift Factor and a Load Shift Factor to determine the total impact of an Interchange Transaction on an identified transmission facility or Flowgate.	34
Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.	34
Generator Owner	Entity that owns and maintains generating units.	34
Generator Shift Factor (GSF)	A factor to be applied to a generator's expected change in output to determine the amount of flow contribution that change in output will impose on an identified transmission facility or Flowgate.	34
Generic SIO Class	An SIO class in which the data types for one or more of the components are not fully specified. [ISO/IEC 15816: 2001)	42
GLB	See Gramm-Leach-Bliley Act.	43
Globally Unique Identifier (GUID)	A 16-byte value generated from the unique identifier on a device, the current date and time, and a sequence number. A GUID is used to identify a particular device, component, user, or session.	43
Gramm-Leach-Bliley Act (GLB)	A U.S. law containing provisions that require all financial institutions to disclose to consumers and customers their policies and practices for protecting the privacy of nonpublic personal information. Nonpublic personal information includes any personally identifiable information provided by a customer, resulting from transactions with the financial institution or obtained by a financial institution through providing products or services. Also known as the Financial Modernization Act of 1999.	43

Term	Definition	Source
(GUID)	See globally unique identifier.	43
Hacker	1. A person who breaks into, or attempts to break into, or use, a computer network or system without authorization, often at random, for personal amusement or gratification, and not necessarily with malicious intent. 2. [An] unauthorized user who attempts to or gains access to an information system (IS). [INFOSEC-99] 3. A technically sophisticated computer expert who intentionally gains unauthorized access to targeted protected resources. [After ANSDIT] 4. Loosely, a computer enthusiast. [ANSDIT] 5. A person who uses a computer resource in a manner for which it is not intended or which is in conflict with the terms of an acceptable-use policy, but (unlike the work of a cracker) is not necessarily malicious in intent. [ATIS]	41
Half-block	A string of bits of length $L_{\bullet}/2$. [ISO/IEC 10118-4: 1998]	42
Hardware	The physical equipment within the cryptographic boundary used to process programs and data.	1, 10
Hardware	1. Physical equipment directly involved in performing industrial process measuring and controlling functions. 2. In data processing, hardware refers to the physical equipment associated with the computer.	33
Hardware Security Module (HSM)	A special CM used to generate and store key materials and is part. (or in some cases all) of a key escrow system.	10
Hash-code	The string of bits which is the output of a hash-function. NOTE - The literature on this subject contains a variety of terms that have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hashresult, hash-value and imprint are some examples. [ISO/IEC 10118-1: 2000] The string of bits which is the output of a hash-function. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)]	42

Term	Definition	Source
	String of bits which is the output of a hash-function. [ISO/IEC FDIS 9796-2 (12/2001), ISO/IEC FDIS 9797-2 (09/2000)]	
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: It is computationally infeasible to find any input that map to any pre-specified output, and It is computationally infeasible to find any two distinct inputs that map to the same output.	10
Hash Function	1. A function which maps strings of bits to fixed-length strings of bits, satisfying two properties. - it is computationally infeasible to find for a given output, an input which maps to this output; - it is computationally infeasible to find for a given input, a second input which maps to the same output. NOTES a – The literature on this subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples. b – Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC PreFDIS 9796-3: 2006-01-26] 2. A computational function performed on a message with results similar to a cyclic redundancy check. A good cryptographic hash function has the following characteristics: a) Any change to the message is likely to affect the hashed value; b) It is computationally infeasible to derive the original message from the hashed value; c) It is computationally infeasible to find another message that produces the same hashed value. [WIKI]	41
Hash-function	A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. It is computationally infeasible to find for a given output, an input which maps to this output. It is computationally infeasible to find for a given input, a second input which maps to the same output. NOTE - Computational feasibility depends on the	42

Term	Definition	Source
	specific security requirements and environment. [ISO/IEC 10118-1: 2000] A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. For a given output, it is computationally infeasible to find an input which maps to this output; For a given input, it is computationally infeasible to find a second input which maps to the same output. NOTE - Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC 14888-1: 1998] Function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. It is computationally infeasible to find for a given output an input which maps to this output. It is computationally infeasible to find for a given input a second input which maps to the same output. [ISO/IEC 9798-5: 1999] A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: For a given output, it is computationally infeasible to find an input which maps to this output; and For a given input, it is computationally infeasible to find a second input which maps to the same output. NOTE - Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 9796-3: 2000, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)] Function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. For a given output, it is computationally infeasible to find an input which maps to this output. For a given input, it is computationally infeasible to find a second input which maps to the same output. [ISO/IEC FDIS 9796-2 (12/2001); ISO/IEC FDIS 9797-2 (09/2000)] A function which maps strings of bits to fixed-length strings of bits, satisfying two properties. It is computationally infeasible to find for a given output, an input which maps to this output. It is computationally infeasible to find for a given input, a second input which maps to the same output.	

Term	Definition	Source
	The literature on this subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples. Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC FDIS 15946-3 (02/2001)]	
Hash-function Identifier	A byte identifying a specific hash-function. [ISO/IEC 10118-1: 2000, ISO/IEC ISO/IEC 10118-4: 1998]	42
Hash-token	A concatenation of a hash-code and an optional control field, which can be used to identify the hash-function and the padding method. NOTE - The control field with hash-function identifier is mandatory unless the hash-function is uniquely determined by the signature mechanism or by the domain parameters. [ISO/IEC 9796-3: 2000, ISO/IEC WD 15946-4 (10/2001)] A concatenation of a hash-code and an optional control field, called hash-function identifier, which can be used to identify the hash-function and the padding method. [ISO/IEC 14888-1: 1998]	42
Health Insurance Portability and Accountability Act (HIPAA)	A U.S. regulation that gives patients greater access to their own medical records and more control over how their personally identifiable health information is used. The regulation also addresses the obligations of healthcare providers and health plans to protect health information. In general, covered entities such as health plans, healthcare clearinghouses, and healthcare providers which conduct certain financial and administrative transactions electronically had until April 14, 2003, to comply.	43
HFNETCHK	A command-line tool that enables an administrator to check the update status of all Windows NT 4.0, Windows 2000, and Windows XP computers on a network from a central location.	43
High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.	14, 15
High Priority Update	A classification used on the Windows Update Web site and by the Windows Update Service to recommend Microsoft software updates and drivers that help protect against the latest publicly known security threats and reliability issues. All software updates and drivers that can be installed by turning on Automatic Updates on your computer are classified as high priority. These can also be installed by	43

Term	Definition	Source
	visiting the Windows Update Web site.	
HIPAA	See Health Insurance Portability and Accountability Act.	43
Honeypot	Generic term for a decoy system used to deceive, distract, divert and to encourage the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user. [ISO/IEC FDIS 18043: 2006-03-14]	41
Host Balancing Authority	1. A Balancing Authority that confirms and implements Interchange Transactions for a Purchasing Selling Entity that operates generation or serves customers directly within the Balancing Authority's metered boundaries. 2. The Balancing Authority within whose metered boundaries a jointly owned unit is physically located.	34
Hotfix	A single cumulative package composed of one or more files used to address a problem in a product. Hotfixes address a specific customer situation and may not be distributed outside the customer organization. The terms QFE, patch, and update have been used in the past as synonyms for hotfix.	43
Hourly Value	Data measured on a Clock Hour basis.	34
Human Machine Interface	A computer terminal normally associated with a graphics terminal that allows interaction between people and end devices.	13
Human User	Any person who interacts with the TOE. [ISO/IEC 15408-1: 1999]	42

Term	Definition	Source
ICCP	Intercontrol centre communications protocol, also known as IEC 60870-6, TASE.2. [IEC 60870-6]	41
ICRA	See Internet Content Rating Association.	43
Identification	Process of uniquely determining the unique identity of an entity [ISO/IEC TR 13335-4; 1999]	42
Identification Data	Sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it. NOTE - Examples of data items which may be included in the identification data include: an account number, expiry date, serial number, etc. [ISO/IEC 9798-5: 1999] A sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it. NOTE - The identification data may additionally contain data items such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters. [ISO/IEC 14888-1: 1998]	42
Identity	A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym. [ISO/IEC 15408-1: 1999]	42

Term	Definition	Source
IDS	Intrusion Detection System	41
IEEE 802.11i	IEEE 802.11i is an amendment to the 802.11 standard specifying security mechanisms for wireless networks (see WiFi). The draft standard was ratified on 24 June 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. WiFi Protected Access (WPA) had previously been introduced by the WiFi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i. The WiFi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2 . 802.11i makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher. The 802.11i architecture contains the following components: 802.1X for authentication (entailing the use of EAP and an authentication server), RSN for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication. [WIKI]	41
IETF	Internet Engineering Task Force. The IETF is charged with developing and promoting Internet standards, in particular, those of the TCP/IP protocol suite. It is an open, all-volunteer organization, with no formal membership or membership requirements. [WIKI]	41
Impact	The result of an unwanted incident. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Impersonation	The ability of an operating system process or thread to run temporarily in the security context of a specific caller and gain authorized access to resources using that identity.	43

Term	Definition	Source
Implicit Key Authentication from A to B	The assurance for entity B that A is the only another entity can possibly be in possession of the correct. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] [sic]	42
Implicit Profiling	An information collection process in which the actions and behaviors of a user visiting a Web site are recorded as the user moves around in and interacts with the Web site.	43
Implicit Targeting	An information delivery process in which existing user data is used to deliver tailored content to users who browse a Web site.	43
Imprint	A string of bits, either the hash-code of a data string or the data string itself.	42
Inadvertent Interchange	The difference between the Balancing Authority's Net Actual Interchange and Net Scheduled Interchange. ($I_A – I_S$)	34
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	14
Independent Power Producer (IPP)	Any entity that owns or operates an electricity generating facility that is not included in an electric utility's rate base. This term includes, but is not limited to, cogenerators and small power producers and all other nonutility electricity producers, such as exempt wholesale generators, who sell electricity.	34
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.	15
Informal	Expressed in natural language. [ISO/IEC 15408-1; 1999]	42
Information	An instance of an information type.	14, 25
Information Disclosure	The exposure of information to individuals who normally would not have access to it.	43
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.	12, 14, 15
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.	14, 15, 23

Term	Definition	Source
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	14, 15, 18
Information Security	The protection of written, verbal and electronic information against unauthorized disclosure, transfer, modification, or destruction. Traditionally, information technology security has focused on the confidentiality, integrity and availability of data.	32
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [NIST]	41
Information Security	The preservation of confidentiality, integrity and availability of information. NOTE - Confidentiality is defined as ensuring that information is accessible only to those authorized to have access. Integrity is defined as safeguarding the accuracy and completeness of information and processing methods. Availability is defined as ensuring that authorised users have access to information and associated assets when required. [ISO/IEC 17799: 2000]	42
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.	12, 15
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.	14, 15, 17, 23
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.	12*, 14, 15
Information System Security Officer	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.	12, 15

Term	Definition	Source
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.	14, 15, 24
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, executive order, directive, policy, or regulation.	14, 15, 25
Informative	Information included making the content of a standard easier to understand.	10
Initial Transformation	A function that is applied at the beginning of a MAC algorithm. [ISO/IEC 9797-1: 1999]	42
Initialization Vector (IV)	A vector used in defining the starting point of an encryption process within a cryptographic algorithm.	1, 10
Initializing Value	A value used in defining the starting point of a hash-function. [ISO/IEC 10118-1: 2000] Value used in defining the starting point of a hash-function. [ISO/IEC FDIS 9797-2 (09/2000)] Value used in defining the starting point of an encipherment process. [ISO 8372: 1987, ISO/IEC CD 10116 (12/2001)]	42
Input data	Information that is entered into a cryptographic module for the purposes of transformation or computation using an approved security function.	1, 10
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.	1, 10
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	14, 15, 18

Term	Definition	Source
Integrity	Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.	12
Integrity	1. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [NIST] 2. The property that sensitive data have not been modified or deleted in an unauthorized and undetected manner. [FIPS 140-2] 3. Property that sensitive data has not been modified or deleted in an unauthorised and undetected manner. [ISO/IEC 19790: 2006-03-01]	41
Integrity	The property of safeguarding the accuracy and completeness of assets. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Intelligent Electronic Device (IED)	Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers). [Common Usage]	10, 41
Interactive Logon	The process of logging on to a local computer using a keyboard. Compare network logon.	43
Interception	Capture and disclosure of message contents—often referred to as sniffing—or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes. [??]	41
Interchange Distribution Calculator (IDC)	The mechanism used by Reliability Coordinators in the Eastern Interconnection to calculate the distribution of Interchange Transactions over specific Flowgates. It includes a database of all Interchange Transactions and a matrix of the Distribution Factors for the Eastern Interconnection.	34
Interchange Transaction	An agreement to transfer energy from a seller to a buyer that crosses one or more Balancing Authority Area boundaries.	34

Term	Definition	Source
Interchange Schedule	An agreed-upon Interchange Transaction size (megawatts), start and end time, beginning and ending ramp times and rate, and type required for delivery and receipt of power and energy between the Source and Sink Balancing Authorities involved in the transaction.	34
Interchange Transaction Tag or Tag	The details of an Interchange Transaction required for its physical implementation.	34
Interchangeability	The ability to replace a device supplied by one manufacturer with a device supplied by another manufacturer, without making changes to the other elements in the system. [Common Usage]	41
Interconnected Operations Service	A service (exclusive of basic energy and transmission services) that is required to support the reliable operation of interconnected Bulk Electric Systems.	34
Interconnection	When capitalized, any one of the three major electric system networks in North America: Eastern, Western, and ERCOT.	34
Interconnection Reliability Operating Limit	The value (such as MW, MVar, Amperes, Frequency or Volts) derived from, or a subset of the System Operating Limits, which if exceeded, could expose a widespread are of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages.	34
Interface	A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals. [FIPS 140-2]	1, 10, 41
Interface	A specific electronic circuit that is a boundary between other circuits or devices.	33
Interleaving Attack	A masquerade which involves use of information derived from one or more ongoing or previous authentication exchanges. [ISO/IEC 9798-1: 1997]	42
Intermediate Balancing Authority	A Balancing Authority Area that has connecting facilities in the Scheduling Path between the Sending Balancing Authority Area and Receiving Balancing Authority Area and operating agreements that establish the conditions for the use of such facilities	34
Internal	Information that is accessible to all Employees and Contractors while providing services to the operator. For Operators use only (See Information Distribution for more details.)	13

Term	Definition	Source
Internal	In PC ladder programs, a coil or contact whose reference is a logical element in the program and not directly concerned with I/O. May also refer to the storage location used for the logical status of such an element. [Editor's note: ISA defines I/O as Acronym for Input/Output.]	33
Internal Communication Channel	A communication channel between separated parts of TOE. [ISO/IEC 15408-1: 1999]	42
Internal TOE Transfer	Communicating data between separated parts of the TOE. [ISO/IEC 15408-1: 1999]	42
Internet Content Rating Association (ICRA)	An international nonprofit group that has developed a content advisory service for the Internet. ICRA's aim is to protect children from potentially harmful material on the Internet.	43
Internet Control Message Protocol	An extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.	13
Interoperability	The ability of two or more IEDs, computer systems, and/or software applications from the same vendor or different vendors, to exchange information and use that information for correct execution of the specified functions. [Common Usage]	41
Interrupt (INT)	In data processing, a signal that, when activated, causes a transfer of control to a specific location in memory, thereby breaking the normal flow of control of the routine being executed. An interrupt is normally caused by an external event such as a "done" condition in a peripheral. It is distinguished from a trap, which is caused by the execution of a processor instruction.	33
Interruptible Load or Interruptible Demand	Demand that the end-use customer makes available to its Load-Serving Entity via contract or agreement for curtailment.	34
Interruption	Degrading or destroying the communication links or device using message flooding, generation of invalid messages, or physical attacks on the communication system. Most commonly known as Denial of Service (DoS) or Distributed Denial of Service (DDoS) if multiple attackers are involved.	10

Term	Definition	Source
Interrupt Service Routine	In data processing, a unique address that points to two consecutive memory locations containing the start address of the interrupt service routine and priority at which the interrupt is to be serviced.	33
Interrupt Vector	In data processing, and address generated by an interrupt. It points to the start of the interrupt service routine.	33
Interrupt Vector Register	In data processing, a register for storing the interrupt vector.	33
Inter-TSF Transfers	Communicating data between the TOE and the security functions of other trusted IT products. [ISO/IEC 15408-1: 1999]	42
Intranet	An intranet is the generic term for a collection of private computer networks within an organization's established policies. Intranets generally use standard network technologies like Ethernet, TCP/IP, Web browsers and Web servers. An organization's intranet often enjoys Internet access, but is firewalled so that its computers cannot be reached directly from the public net.	13
Intruder	Any unauthorized individual or any individual performing unauthorized activity within the substation.	36
Intrusion	Unauthorized act of bypassing the security mechanisms of a system.	12
Intrusion	A deliberate or accidental set of events that potentially causes unauthorized access to, activity against, and/or activity in, an information technology (IT) system. [ISO/IEC DTR 15947 (10/2001)]	42
Intrusion Detection	Intrusion Detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a device or a network to identify possible security breaches, including intrusions (attacks from outside the organization) and misuse (attacks from within the organization).	13
Intrusion Detection System (IDS)	Information system used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in Information Systems and networks. [ISO/IEC FDIS 18043: 2006-03-14]	41

Term	Definition	Source
Intrusion Detection System (IDS)	A technical system that is used to identify and respond to intrusions in IT systems. [ISO/IEC DTR 15947 (10/2001)]	42
Intrusion Protection Systems	IPS supports the ability to receive IDS Sensor or Scanner data and then apply analytical processes and information to derive conclusions about intrusions. IPS-conformant products also provide the ability to protect themselves and their associated data from unauthorized access or modification and to ensure accountability for authorized actions	13
Ipsec	Short for "IP Security," a set of protocols developed by the IEFT to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.	13
ISA	The Instrumentation, Systems, and Automation Society (ISA) is a non-profit professional organization for instrument engineers that was originally known as the Instrument Society of America. The society is more commonly known by its acronym, ISA. ISA is one of the foremost professional organizations in the world for setting standards and educating industry professionals in the instrumentation and automation industry. Instrumentation and automation are some of the key technologies involved in nearly all industrialized manufacturing. Modern industrial manufacturing is a complex interaction of numerous systems. Instrumentation provides regulation for these complex systems using many different measurement and control devices. Automation provides the programmable devices that permit greater flexibility in the operation of these complex manufacturing systems. [WIKI]	41

Term	Definition	Source
ISO	International Standards Organization	41
IT Security	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability. [ISO/IEC PDTR 13335-1 (11/2001)]	42
IT Security Policy	Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its IT systems. [ISO/IEC PDTR 13335-1 (11/2001)]	42
IT Security Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. [ISO/IEC WD 15443-1 (11/2001)]	42
Iteration	The use of a component more than once with varying operations. [ISO/IEC 15408-1: 1999]	42
JTC1 Registration Authority	An organisation appointed by the ISO and IEC councils to register objects in accordance with a JTC 1 procedural Standard. [ISO/IEC 15292: 2001]	42
Joint Control	Automatic Generation Control of jointly owned units by two or more Balancing Authorities.	34
KB Article	A technical document in the Microsoft Knowledge Base accessible through Microsoft.com.	43
Key [alpha order: put all words beginning with “key” together, alphabetized according to second word]	See cryptographic key	10

Term	Definition	Source
Key	1. Sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption). [ISO/IEC 18033-1] 2. Unique digital information used to perform a cryptographic operation such as hashing, encryption or decryption. Called a key because it serves a similar purpose as a physical key in that the key is required to “lock” or “unlock” encrypted or hashed information. [WIKI]	41
Key	A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification). [ISO/IEC 9797-1: 1999, ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996] A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature calculation, or signature verification). [ISO/IEC 11770-3: 1999] A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment). [ISO/IEC CD 10116 (12/2001)] A sequence of symbols that controls the operation of a cryptographic transformation (e.g.encipherment, decipherment, cryptographic check function computation, signature generation, signature verification, or key agreement). [ISO/IEC FDIS 15946-3 (02/2001)] Sequence of symbols that controls the operation of a cryptographic transformation (e.g.encipherment, decipherment). [ISO/IEC WD 18033-1 (12/2001)]	42
Key	In encryption and digital signatures, a value used in combination with an algorithm to encrypt or decrypt data.	43
Key Agreement	The process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. [ISO/IEC 11770-1: 1996, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)	42
Key Component	See “cryptographic key component.”	10

Term	Definition	Source
Key Confirmation	A process used to validate the accuracy and authenticity of a parameter used in the encryption or decryption function.	10
Key Confirmation	The assurance for one entity that another identified entity is in possession of the correct key. [ISO/IEC 11770-1: 1996, ISO/IEC 11770-2: 1996]	42
Key Confirmation from A to B	The assurance for entity B that entity A is in possession of the correct key. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Key Control	The ability to choose the key, or the parameters used in the key computation. [ISO/IEC 11770-1: 1996, ISO/IEC 11770-2: 1996, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Key Derivation Function	A key derivation function outputs one or more shared secrets, used as keys, given shared secrets and other mutually known parameters as input. [ISO/IEC FDIS 15946-3 (02/2001)]	42
Key Distribution	The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key. [RFC2828]	41
Key Distribution Centre	An entity trusted to generate or acquire, and distribute keys to entities that each share a key with the KDC. [ISO/IEC 11770-1: 1996]	42
Key Distribution Service	The service of distributing keys securely to authorized entities performed by a Key Distribution Center and described in ISO/IEC 11770-1. [ISO/IEC FDIS 15945 (10/2000)]	42
Key Escrow System	Software, devices, and procedures used to generate, store, and retrieve securely cryptographic keys and key materials securely for the purposes of installation, maintenance, and backup.	10
Key Establishment	The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).	1
Key establishment	The process by which cryptographic keys are distributed securely among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of	10

Term	Definition	Source
	key transport plus key agreement). [1]	
Key Establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Key Generating Function	A function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application. The function shall have the property that it shall be computationally infeasible to deduce the output without prior knowledge of the secret input. [ISO/IEC 11770-2: 1996]	42
Key Generation Exponent	A positive integer known only to the trusted third party. [ISO/IEC 14888-2: 1999]	42
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.	1, 10
Key Management	The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy. [ISO/IEC 11770-1: 1996]	42
Key Pair	A public key and its corresponding private key. A key pair is used with a public key algorithm.	10
Key Pair	A public key and its corresponding private key used with a public key algorithm. [RFC2828]	41

Term	Definition	Source
Key Token	Key management message sent from one entity to another entity during the execution of a key management mechanism. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Key Translation Centre (KTC)	An entity trusted to translate keys between entities that each share a key with the KTC. [ISO/IEC 11770-1: 1996]	42
Key Transport	The process of transferring a key from one entity to another entity, suitably protected. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Keyed-Hash Message Authentication Code (HMAC)	A mechanism for message authentication using cryptographic hash functions, in combination with a shared secret key.	4, 10
Keying Material	A string of numbers and/or characters, identically having a high degree of randomness or unpredictability, used to carry out an agreed upon logical function.	10
Keying Material	The data (e.g. keys, initialisation values) necessary to establish and maintain cryptographic keying relationships. [ISO/IEC 11770-1: 1996]	42
Kids Passport	A .NET Passport service that helps participating sites and services obtain parental consent to collect, use, and disclose a child's personal information. This service is used to support legal requirements such as the Children's Online Privacy Protection Act or Korean Kids.	43
Knowledgeable Escort	A person who is familiar with the work to be performed by a non-cleared person. This individual must have a solid understanding of the risk involved in the work to be performed. This individual will monitor the work being performed.	13

Term	Definition	Source
Label	See Security Label.	15
Label	In data processing, a set of symbols used to identify or describe an item, record, message, or file. Occasionally it may be the same as the address in storage.	33
Labeled Common	Named data areas that are accessible to all computer programs declaring the named area.	33
Latency	The time it takes for a packet to cross a network connection, from sender to receiver.	10
Latency	In data processing, the time between the completion of the interpretation of an address and the start of the actual transfer from the addressed location. Latency includes the delay associated with access to storage devices such as drums and delay lines.	33
Latency	Time delay between the moment something is initiated, and the moment one of its effects begins. [WIKI]	41
Layer Two (2) Tunneling Protocol	An extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs), L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. Like PPTP, L2TP requires that the ISP's routers support the protocol.	13
Least Privilege Administration	A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.	43
Life Cycle Stage	An instance within the deliverable life cycle that relates to the state of the deliverable. [ISO/IEC WD 15443-1 (11/2001)]	42
Limiting Element	The element that is 1.)Either operating at its appropriate rating, or 2,) Would be following the limiting contingency. Thus, the Limiting Element establishes a system limit.	34
Load	An end-use device or customer that receives power from the electric system.	34
Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.	34
Load Shift Factor (LSF)	A factor to be applied to a load's expected change in demand to determine the amount of flow contribution that change in demand will impose on an identified transmission facility or monitored flowgate.	34

Term	Definition	Source
Local	Inside the substation.	10
Local Area Network (LAN	A communications network designed to connect computers and other intelligent devices in a limited geographic area (typically under 10 km. [ATIS]	41
Local Area Networks	Acronym for local area network, a group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.	13
Local Attack	An attack that targets the computer to which the attacker is interactively logged on.	43
Logical Networks	The SCADA network and the business network share the same infrastructure and freely route data between the two.	13
Low-Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.	14, 15, 25
MAC	See Message Authentication Code.	43
MAC Algorithm Key	A key that controls the operation of a MAC algorithm. [ISO/IEC 9797-1: 1999] mask generation function Function which maps strings of bits to strings of bits of arbitrary specified length, satisfying the following property it is computationally infeasible to predict, give one part of the output but not the input, another part of the output. [ISO/IEC FDIS 9796-2 (12/2001)] [sic]	42
Mail Bomb	See e-mail bomb.	43

Term	Definition	Source
Mail Relaying	A practice in which an attacker sends e-mail messages from another system's e-mail server in order to use its resources and/or make it appear that the messages originated from the other system.	43
Maintenance port	The physical access mechanism (interface) on an IED or RTU through which a maintenance engineer can access data, and access or change settings and programs with the IED or RTU. The port is typically RS-232 (a standard for asynchronous serial data communications). The access may be controlled by several levels of passwords. Remote access via dial-up phone lines requires an external or internal automatic answering modem.	10
Major Application	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.	15, 17
Major Information System	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.	15, 17
Malicious Code	Software that fulfills the deliberately harmful intent of an attacker when run. For example, viruses, worms, and Trojan horses are malicious code.	43
Malicious User	A user who intentionally accesses a system with the intent to cause harm to the system or to use it in an unauthorized manner.	43
Malware	1. Malicious software, such as a virus or a Trojan horse, designed specifically to damage or disrupt a system. [ISO/IEC FDIS 18028-1: 2006-03-31] 2. Malware (a portmanteau of "malicious software") is software designed to infiltrate or damage a computer system, without the owner's consent. Once installed, it is often very difficult to remove, and depending on the severity of the program installed, its handiwork can range in degree from the slightly annoying (such as unwanted pop up ads while a user is performing regular computing tasks on or offline), to irreparable damage requiring the reformatting of one's hard drive, since	41

Term	Definition	Source
	much of malware is poorly written. Examples of malware include viruses and Trojan horses. [WIKI]	
Man-in-the-Middle	A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association. [RFC2828]	41
Man Machine Interface	A computer terminal, normally associated with a graphics terminal that allows interaction between people and end devices.	13
Management of Change (MOC)	The review of proposed facility changes to determine if there are any adverse impacts on cybersecurity or other important facility attributes such as safety and the control of these impacts.	32
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.	14, 15, 26
Management Port	The physical or virtual access mechanism (interface) on a cryptographic module through which configuration and cryptographic parameters may be set.	10
Manufacturing & Control Systems	Manufacturing and Control Systems include all systems (personnel, hardware, and software) that can affect or influence the safe, secure and reliable operation of an industrial process. They include, but are not limited to: – process control systems, including Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Intelligent Electronic Devices (IED), Supervisory Control and Data Acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems (In this context, process control systems include Basic Process Control System (BPCS) and Safety Instrumented System (SIS) functions, whether they are physically separate or integrated.) – associated information systems such as advanced or multi-variable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems and plant information management systems – associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.	11

Term	Definition	Source
Manufacturing Operations	Manufacturing operations encompass the collection of production, maintenance, and quality assurance operations with other activities of a production facility. Operations include: – manufacturing or processing facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials and/or parts into products – functions that may be performed by physical equipment, human effort, and information systems – managing information about the schedules, use, capability, definition, history, and status of all resources (personnel, equipment, and material) within the manufacturing facility	11
Masquerade	The pretence by an entity to be a different entity in order to gain unauthorized access. [ATIS]	41
Masquerade	The pretence by an entity to be a different entity. [ISO/IEC 9798-1: 1997]	42
Master	A device that initiates communications requests to gather data or perform controls.	2, 10
Master	1. A device which controls other devices in a system. 2. A precise pattern for making replicate workpieces, as in certain types of casting processes.	33
Master key	See “cryptographic key component.”	10
Matrix	An 8 by 8 matrix in which each entry is a string of 8 bits in dedicated hash-function 7. [ISO/IEC CD 10118-3 (11/2001)]	42

Term	Definition	Source
May	The word “may,” equivalent to “is permitted,” is used to indicate a course of action permissible.	10
Mechanism	1. Generally, an arrangement of two or more mechanical parts in which motion of one part compels the motion of the others. 2. Specifically the arrangement of parts in an indicating instrument which control motion of the pointer or other indicating means, excluding those parts which form the enclosure, scale, or support structure, or which adapt the instrument to the quantity being measured. 3. In a recording instrument, the arrangement of parts which control motion of the marking device, the marking device itself, the device for driving the chart, and the parts which carry the chart.	33
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, firmware, or physical devices) employed within or at the boundary of an information system.	15
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.	14
Media	1. The physical interconnection between devices attached to the LAN. Typical LAN media are twisted pair, baseband coax, broadband coax, and fiber optics. 2. The plural of medium.	33
Medium	In data processing, the material on which data is recorded and stored.	33
Media Access Control Address	A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.	15
Message	An ordered series of characters used to convey information.	10
Message	An arbitrary amount of information whose beginning and end are defined or implied.	33
Message	String of bits of any length. [ISO/IEC FDIS 9796-2 (12/2001)] A string of bits of any length. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)	42
Message Authentication Code	Data that is associated with authenticated information that allows an entity to verify the integrity of the information.	10

Term	Definition	Source
(MAC)		
Message Authentication Code (MAC)	The string of bits which is the output of a MAC algorithm. NOTE – A MAC is sometimes called a cryptographic check value. [ISO/IEC 9797-1: 1999, ISO/IEC WD 13888-1 (11/2001)]	42
Message Authentication Code (MAC)	An algorithm that allows a receiver to ensure that a block of data has retained its integrity from the time it was sent until the time it was received.	43
Message Authentication Code (MAC) Algorithm	An algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: for any key and any input string the function can be computed efficiently; for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i-1 function values. NOTE 1 - A MAC algorithm is sometimes called a cryptographic check function. NOTE 2 - Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC 9797-1: 1999]	42
Message Exchange	A device placed between a communication line and a computer to take care of certain communication functions and thereby free the computer for other work.	33
Message Representative	Bit string derived as a function of the message and which is combined with the private signature key to yield the signature. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Message Routing	The function performed at a central message processor of selecting the route, or alternate route if required, by which a message will proceed to the next point in reaching its destination.	33
Message Switching	The technique of receiving a message, storing it until the proper outgoing circuit is available, and then retransmitting it.	33

Term	Definition	Source
MIB	Management Information Base. A MIB is a type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network. Objects in the MIB are defined using Abstract Syntax Notation One (ASN.1), the software that performs the parsing is a MIB compiler. The database is hierarchical (tree structured) and entries are addressed through object identifiers. Internet documentation RFCs discuss MIBs, notably RFC 1155, "Structure and Identification of Management Information for TCP/IP based internets", and its two companions, RFC 1213, "Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, "A Simple Network Management Protocol" (SNMP). SNMP, a communication protocol between management stations (consoles, for example) and managed objects, (such as routers, gateways, and switches) makes use of MIBs. Components controlled by the management console need a so-called SNMP agent -- a software module that can communicate with the SNMP manager. [WIKI]	41
Microsoft Download Center	A Microsoft Web site that provides security and technology updates for Microsoft software.	43
Microsoft Passport Network	A service for businesses that lets customers use the same sign-in information to sign in anywhere on the network.	43
Microsoft Security Bulletin	A document that describes a specific security issue in Microsoft software and directs the reader to a downloadable file that resolves the issue.	43

Term	Definition	Source
Microsoft Virus Alert	An announcement that describes a specific virus, the impact of potential attacks on Microsoft software, and suggestions for preventing or recovering from such attacks.	43
MMS	Manufacturing Message Specification. MMS is an ISO 9506 standard. Control Networks uses the MMS protocol and a reduced OSI stack with the TCP/IP protocol in the transport/network layer, and Ethernet and/or RS-232C as physical media. This means that all communication handling will be the same, regardless of network type and connected devices. The protocol defines communication messages transferred between controllers as well as between the engineering station and the controller (e.g. downloading an application or reading/writing variables). It has been developed especially for industrial applications. [WIKI] MMS is one of the communication protocols that IEC 61850 is mapped to. [IEC 61850]	41
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.	15
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).	15
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.	14, 15
Modification	The alteration of data or information; in the adverse situation, the alteration results in a condition other than intended by the originator.	10
Modulus	A parameter which is a positive integer and a product of two distinct prime numbers. [ISO/IEC 10118-4: 1998] Integer used as a divisor of an integer dividend in order to obtain an integer remainder. [ISO/IEC FCD 7064 (09/2000)]	42
Monitor	1. To measure a quantity continuously or at regular intervals so that corrections to a process or condition may be made without delay if the quantity varies outside of prescribed limits. 2. Software or hardware that observes, supervises, controls, or verifies the operations of a system. 3. In data	33

Term	Definition	Source
	processing, a high-resolution viewing screen.	
Monitor (Monitoring Authority)	A trusted third party monitorin the actions and events and is trusted to provide evidence about what was monitored. [ISO/IEC WD 13888-1 (11/2001)]	42
Monitoring	The act of observing, carrying out surveillance on, and/or recording the presence of individuals for the purpose of maintaining and improving procedural standards and security. The act of detecting the presence of unauthorized personnel, sounds, or visual signals, and the measurement thereof with appropriate measuring instruments.	13
Multicast	A message addressed to a group of stations connected to a LAN.	33
Multicast	1. In a network, a technique that allows data, including packet form, to be simultaneously transmitted to a selected set of destinations. Note: Some networks, such as Ethernet, support multicast by allowing a network interface to belong to one or more multicast groups. 2. To transmit identical data simultaneously to a selected set of destinations in a network, usually without obtaining acknowledgement of receipt of the transmission. [ATIS]	41
Multicast mode	Concurrent transfer mode of information to a predefined subset of all connected receivers with one message from the information source. Contrast: unicast and broadcast modes.	10
Multi-factor authentication	A mechanism that employs more than one means to validate the identity of an entity.	10
Must	The use of the word “must” is deprecated and shall not be used when stating mandatory requirements. The word “must” is used to describe unavoidable situations only.	10
Mutual Authentication	Entity authentication which provides both entities with assurance of each other’s eidentity. [ISO/IEC 9798-1: 1997]	42
Mutual Entity Authentication	Entity authentication which provides bothe entities with assurance of each other’s identity. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Mutual Forward Secrecy	The property that knowledge of both A's and B's long-term private keys subsequent to a key agreement operation does not enable the opponent to recompute previously derived keys. [ISO/IEC FDIS 15946-3 (02/2001)]	42

Term	Definition	Source
n	-bit block cipher A block cipher with the property that plaintext blocks and ciphertext blocks are n bits in length. [ISO/IEC 9797-1: 1999, ISO/IEC CD 10116 (12/2001), ISO/IEC 10118-2: 2000), ISO/IEC WD 18033-1 (12/2001)]	42
n-bit	Quantity of length “n” bits	10
National Security Emergency Preparedness Telecommunications Services	Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.	15, 27
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.	14, 15
National Security System	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.	14, 15, 18
Native Load	The end-use customers that the Load-Serving Entity is obligated to serve.	34
NERC	North American Electric Reliability Council	41

Term	Definition	Source
Net Actual Interchange	The algebraic sum of all metered interchange over all interconnections between two physically Adjacent Balancing Authority Areas.	34
Net Energy for Load	Net Balancing Authority Area generation, plus energy received from other Balancing Authority Areas, less energy delivered to Balancing Authority Areas through interchange. It includes Balancing Authority Area losses but excludes energy required for storage at energy storage facilities.	34
Net Interchange Schedule	The algebraic sum of all Interchange Schedules with each Adjacent Balancing Authority.	34
Net Scheduled Interchange	The algebraic sum of all Interchange Schedules across a given path or between Balancing Authorities for a given period or instant in time.	34
Network Integration Transmission Service	Service that allows an electric transmission customer to integrate, plan, economically dispatch and regulate its network reserves in a manner comparable to that in which the Transmission Owner serves Native Load customers.	34
Network Layer Protocol	Protocols for routing of messages through a complex network. Layer 3 of the OSI reference model. [ATIS]	41
Network Logon	The process of logging on to a computer by means of a network. Typically, a user first interactively logs on to a local computer, then provides logon credentials to another computer on the network, such as a server, that he or she is authorized to use. Compare interactive logon.	43
Network Management	Process of planning, designing, implementing, operating, monitoring and maintaining a network. [ISO/IEC FDIS 18028-1: 2006-03-31]	41
Nibble	Block of four consecutive bits (half an octet). [ISO/IEC FDIS 9796-2 (12/2001)]	42

Term	Definition	Source
Non-Firm Transmission Service	Transmission service that is reserved on an as-available basis and is subject to curtailment or interruption.	34
Non-recoverable Part	Part of the message stored and transmitted along with the signature; empty when message recovery is total. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Non-Repudiation	A service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the originator.	10
Non-Repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.	12, 15
Non-Repudiation	1. The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later [ISO/IEC 13888-1; ISO IS 7498-2] 2. A security service that provides protection against false denial of involvement in a communication. [RFC2828]	41
Non-repudiation	The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Nonrepudiation	A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Nonrepudiation provides undeniable proof that a user took a specific action such as transferring money, authorizing a purchase, or sending a message.	43
Non-repudiation Exchange	A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of nonrepudiation. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation Information	A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation of Creation	This service is intended to protect against an entity's false denial of having created the content of a message (i.e. being responsible for the content of a message). [ISO/IEC WD 13888-1 (11/2001)] Protection against an entity's false denial of having created the content of a message (i.e., being responsible for the content of a message). [ISO/IEC 15945: 2002]	42

Term	Definition	Source
Non-repudiation of Delivery	This service is intended to protect against a recipient's false denial of having received the message and recognised the content of a message. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation of Knowledge	This service is intended to protect against a recipient's false denial of having taken notice of the content of a received message. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation of Origin	This service is intended to protect against the originator's false denial of having approved the content of a message and of having sent a message. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation of Receipt	This service is intended to protect against a recipient's false denial of having received a message. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation of Sending	This service is intended to protect against the sender's false denial of having sent a message. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation of Submission	This service is intended to provide evidence that a delivery authority has accepted the message for transmission. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation of Transport	This service is intended to provide evidence for the message originator that a delivery authority has delivered the message to the intended recipient. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation Policy	A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-repudiation Token	A special type of security token as defined in ISO/IEC 10181-1 consisting of a set of evidence, and, optionally, of additional data. [ISO/IEC WD 13888-1 (11/2001)]	42
Non-Spinning Reserve	1. That generating reserve not connected to the system but capable of serving demand within a specified time. 2. interruptible load that can be removed from the system in a specified time.	34
Normal Rating	The rating as defined by the equipment owner that specifies the level of electrical loading, usually expressed in megawatts (MW) or other appropriate units that a system, facility, or element can support or withstand through the daily demand cycles without loss of equipment life.	34
Normative	A specification of requirements that is mandatory for the product or system to claim compliance.	10
Notarization	The provision of evidence by a notary about the properties of the entities involved in an action or event, and of the data stored or communicated. [ISO/IEC WD 13888-1 (11/2001)]	42

Term	Definition	Source
Notarization Token	A non-repudiation token generated by a notary. [ISO/IEC WD 13888-1 (11/2001)]	42
Notary (Notary Authority)	A trusted third party trusted to provide evidence about the properties of the entities involved and of the data stored or communicated, or to extend the lifetime of an existing token beyond its expiry or beyond subsequent revocation. [ISO/IEC WD 13888-1 (11/2001)]	42
Notice	A privacy principle that requires reasonable disclosure to a consumer of an entity's personally identifiable information collection and use practices. This disclosure information is typically conveyed in a privacy notice or privacy policy. Notice is addressed in Fair Information Practices.	43
NRD Token	Non-repudiation of delivery token. A data item which allows the originator to establish non-repudiation of delivery for a message. [ISO/IEC WD 13888-1 (11/2001)]	42
NRO Token	Non-repudiation of origin token. A data item which allows recipients to establish non-repudiation of origin for a message. [ISO/IEC WD 13888-1 (11/2001)]	42
NRS Token	Non-repudiation of submission token. A data item which allows either the originator (sender) or the delivery authority to establish non-repudiation of submission for a message having been submitted for transmission. [ISO/IEC WD 13888-1 (11/2001)]	42
NRT Token	Non-repudiation of transport token. A data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message. [ISO/IEC WD 13888-1 (11/2001)]	42
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations. [ISO/IEC 15408-1: 1999]	42
Octet	String of eight bits. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Office Update	A Microsoft Web site maintained by the Microsoft Office product group for the purpose of providing critical updates, add-ins, converters, and viewers that increase the performance and stability of currently released Office programs.	43
Off-Peak	Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of lower electrical demand.	34
On-Peak	Those hours or other periods defined by NAESB business	34

Term	Definition	Source
	practices, contract, agreements, or guides as periods of higher electrical demand.	
Onward Transfer	The transfer of personally identifiable information by the recipient of the original data to a second recipient. For example, the transfer of personally identifiable information from an entity in Germany to an entity in the United States constitutes onward transfer of that data. Onward transfer is addressed in Fair Information Practices.	43
One-way Function	A function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input which maps to this output. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Open Access Same Time Information Service (OASIS)	An electronic posting system that the Transmission Service Provider maintains for transmission access data and that allows all transmission customers to view the data simultaneously.	34
Open Access Transmission Tariff (OATT)	Electronic transmission tariff accepted by the U.S. Federal Energy Regulatory Commission requiring the Transmission Service Provider to furnish all shippers with non-discriminating service comparable to that provided by Transmission Owners to themselves.	34
Open Protocol	Protocol whose stack is either standardized or public available. [ATIS]	41
Open System	A system with characteristics that comply with specified, publicly maintained, readily available standards, and that therefore can be connected to other systems that comply with these same standards. [ATIS]	41
Open Systems Architecture	1. The layered hierarchical structure, configuration, or model of a communications or distributed data processing system that • (a) enables system description, design, development, installation, operation, improvement, and maintenance to be performed at a given layer or layers in the hierarchical structure,	41

Term	Definition	Source
	• (b) allows each layer to provide a set of accessible functions that can be controlled and used by the functions in the layer above it, • (c) enables each layer to be implemented without affecting the implementation of other layers, and • (d) allows the alteration of system performance by the modification of one or more layers without altering the existing equipment, procedures, and protocols at the remaining layers. Note 1: Examples of independent alterations include (a) converting from wire to optical fibres at a physical layer without affecting the data-link layer or the network layer except to provide more traffic capacity, and (b) altering the operational protocols at the network level without altering the physical layer. Note 2: Open systems architecture may be implemented using the Open Systems Interconnection--Reference Model (OSI--RM) as a guide while designing the system to meet performance requirements. 2. Non-proprietary systems architecture. [ATIS]	
Operating Reserve	That capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages and local area protection. It consists of spinning and non-spinning reserve.	34
Operating Reserve – Spinning	The portion of Operating Reserve consisting of: • Generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.	34
Operating Reserve – Supplemental	The portion of Operating Reserve consisting of: • Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event; or • Load fully removable from the system within the	34

Term	Definition	Source
	Disturbance Recovery Period following the contingency event.	
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).	14, 15, 26
Operational use	A stage in the lifecycle of keying material; a stage whereby keying material is used for standard cryptographic purposes.	10
Operative limits	The range of operating conditions to which a device may be subjected without permanent impairment of operating characteristics.	33
Operator	1. The person who initiates and monitors the operation of a computer. 2. The person who initiates and monitors the operation of a process. 3. Any person who is working at a piece of equipment. 4. A mathematical symbol which represents a mathematical process to be performed on an associated operand. 5. The portion of an instruction which tells the machine what to do.	33
Operator, cryptographic	An individual accessing a cryptographic module or a process operating on behalf of the individual, regardless of the assumed role.	1, 10
Operator (SCADA)	An individual in the utility control center that is responsible for on-line SCADA system control.	10
Operator Work Station	A computer terminal, normally associated with a graphics terminal that allows interaction between people and end devices.	13
Operator's Console	A device which enables the operator to communicate with the computer. It can be used to enter information into the computer, to request and display stored data, to actuate various preprogrammed command routines, etc. See also process engineer's console and programmer's console.	33
Opt In	To explicitly consent to participate. Typically used in marketing programs and offerings, whereby an action (such as the use of personal information beyond the original, primary purpose for which it was collected) is not undertaken unless an individual explicitly consents. An element of choice.	43
Opt Out	To explicitly decline to participate. Typically used in marketing programs and offerings, whereby an action (such as the use of personal information beyond the original, primary purpose for which it was collected) is undertaken unless an individual explicitly declines. An element of choice.	43

Term	Definition	Source
Order of an Element in a Finite Commutative Group	If $a^0 = e$, and $a^n+1 = a*a^n$ (for n ●●●●●● 0), is defined recursively, the order of a ● J is the least positive integer n such that $a^n = e$. [ISO/IEC 14888-3: 1998]	42
Organization	A federal agency or, as appropriate, any of its operational elements.	14
Organisational Security Policies	One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations. [ISO/IEC 15408-1: 1999]	42
Originator	The entity that sends a message to the recipient or makes available a message for which non-repudiation services are to be provided. [ISO/IEC WD 13888-1 (11/2001)]	42
OSI-RM	OSI-RM (Open Standards Interconnection – Reference Model) is a layered abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnect initiative. It is also called the OSI seven layers model. [WIKI]	41
OSI-RM Layer 1: Physical Layer	The physical layer defines all the electrical and physical specifications for devices. This includes the layout of pins, voltages, and cable specifications. Hubs and repeaters are physical-layer devices. The major functions and services performed by the physical layer are: • Establishment and termination of a connection to a communications medium. • Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control. Modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling -- copper and fibre optic, for example. SCSI operates at this level. [WIKI]	41

Term	Definition	Source
OSI-RM Layer 2: Data Link Layer	The data link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical layer. The addressing scheme is physical which means that the addresses (MAC address) are hard-coded into the network cards at the time of manufacture. The addressing scheme is flat. Note: The best known example of this is Ethernet. Other examples of data link protocols are HDLC and ADCCP for point-to-point or packet-switched networks and LLC and Aloha for local area networks. This is the layer at which bridges and switches operate. Connectivity is provided only among locally attached network nodes. [WIKI]	41
OSI-RM Layer 3: Network Layer	The network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the Transport layer. The Network layer performs network routing, flow control, segmentation/desegmentation, and error control functions. Routers operate at this layer -- sending data throughout the extended network and making the Internet possible (there also exist layer 3 (or IP) switches). This is a logical addressing scheme - values are chosen by the network engineer. The addressing scheme is hierarchical. This layer can be of least significance in case of Broadcasting Networking. [WIKI]	41
OSI-RM Layer 4: Transport Layer	The transport layer provides transparent transfer of data between end users, thus relieving the upper layers from any concern with providing reliable and cost-effective data transfer. The transport layer controls the reliability of a given link. Some protocols are stateful and connection oriented. This means that the transport layer can keep track of the packets and retransmit those that fail. The best known example of a layer 4 protocol is TCP. [WIKI]	41
OSI-RM Layer 5: Session Layer	The session layer provides the mechanism for managing the dialogue between end-user application processes (By dialog we mean that whose turn it is to transmit). It provides for either duplex or half-duplex operation and establishes checkpointing, adjournment, termination, and restart procedures (keeping a track so as to restart from the very same point where they had left in case of a crash). This layer is responsible for setting up and tearing down TCP/IP sessions. [WIKI]	41
OSI-RM Layer 6:	The presentation layer relieves the Application layer of concern regarding syntactical differences in data representation within the end-user systems. MIME encoding, data compression, encryption, and similar manipulation of the presentation of data is done at this layer. An example of a presentation service would be the conversion of an EBCDIC-coded text file to an ASCII-coded file or serializing	41

Term	Definition	Source
Presentation Layer	objects and other data structures into and out of XML. [WIKI]	
OSI-RM Layer 7: Application Layer	The application layer interfaces directly to and performs common application services for the application processes. The common application services provide semantic conversion between associated application processes. Examples of common application services include the virtual file, virtual terminal (for example, Telnet), transfer and Manipulation protocol" (JTM, standard ISO/IEC 8832). [WIKI]	41
Output Transformation	A function that is applied at the end of the MAC algorithm, before the truncation operation. [ISO/IEC 9797-1: 1999] A transformation or mapping of the output of the iteration stage to obtain the hash-code. [ISO/IEC 10118-1: 2000]	42
Overlap Regulation Service	A method of providing regulation service in which the Balancing Authority providing the regulation service incorporates another Balancing Authority's actual interchange, frequency response, and schedules into providing Balancing Authority's AGC/ACE equation.	34
P3P	See Platform for Privacy Preferences Project.	43
Package	A reusable set of either functional or assurance components combined together to satisfy a set of identified security objectives. [ISO/IEC 15292: 2001] A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives. [ISO/IEC 15408-1: 1999]	42
Padding	Appending extra bits to a data string. [ISO/IEC FDIS 9797-2 (09/2000), ISO/IEC 10118-1: 2000]	42
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.	1, 10
Password	1. Secret word, phrase, number or character sequence used for entity authentication, which is a memorized weak secret. [ISO/IEC FDIS 11770-4: 2006-01-09] 2. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [FIPS 140-2]	41
Password	A string of characters entered by a user to verify his or her identity to a network or to a local computer. See also strong password and weak password.	43

Term	Definition	Source
Password Propagation	A process that coordinates each user's password changes across multiple computers, devices, folders, or networks in password synchronization.	43
Password Synchronization	A service that replicates users' passwords between multiple computers, devices, folders, or networks, resulting in users having the same password in each environment.	43
Patch	See security update.	43
Patching	A method of updating a file that replaces only the parts being changed, rather than the entire file. Compare full file replacement.	43
Peak Demand	1. The highest hourly integrated Net Energy For Load within a Balancing Authority Area occurring within a given period (e.g., day, month, season, or year). 2. The highest instantaneous demand within the Balancing Authority Area.	34
Peopleware	The people who use computers.	32
Permission for Kids	The level of permission that determines whether a specific Microsoft Passport Network account can be used to access any site on the Passport Network, or can only access sites that adhere to specific government guidelines for child-friendly content. The permission level for each account is set by parents.	43
Permissions	Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.	43
Personal Data	See personally identifiable information.	43
Personal Identification Number (PIN)	An alphanumeric code or password used to authenticate an identity. [FIPS 140-2]	41
Personal Identification Number (PIN)	A secret identification code similar to a password that is assigned to an authorized user. A PIN is used in combination with an ATM card or smart card, for example, to unlock an authorized functionality such as access to a bank account.	43
Personally Identifiable Information (PII)	Any information relating to an identified or identifiable individual. Such information may include name, country, street address, e-mail address, credit card number, Social Security number, government ID number, IP address, or any unique identifier that is associated with PII in another system. Also known as personal information or personal data.	43

Term	Definition	Source
Personal Information	See personally identifiable information.	43
Personal Security Environment (PSE)	Secure local storage for an entity's private key, the directly trusted CA key and possibly other data. Depending on the security policy of the entity or the system requirements this may be e. g. a cryptographically protected file or a tamper resistant hardware token. [ISO/IEC 15945: 2002]	42
Personalization Service	The service of storing cryptographic information (especially private keys) to a PSE. NOTE - The organizational and physical security measures for a service like this are not in the scope of this document. For organizational measures refer to ITU-T Rec. X.842 | ISO/IEC TR 14516 Guidelines for the use and management of Trusted Third Parties. [ISO/IEC 15945: 2002]	42
Phisher	A malicious user or Web site that deceives people into revealing personal information, such as account passwords and credit card numbers. A phisher typically uses deceptive e-mail messages or online advertisements as bait to lure unsuspecting users to fraudulent Web sites, where the users are then tricked into providing personal information.	43
Physical Layer Protocol	Protocols for transmitting raw electrical signals over the communications channel. Deals with transmission physics such as cabling, modulation, and transmission rates. Layer 1 of the OSI reference model. [ATIS]	41
Physical security	Measures intended to improve protection by means such as fencing, locks, vehicle barriers, area lighting, surveillance systems, guards and dogs, intrusion detection systems and alarms, access controls, vehicle control and housekeeping.	32
Physical Security Perimeter	The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.	35
Physical Security Perimeter	A type of gate, door, wall, or fence system that is intended to restrict and control the physical access or egress of personnel.	36
Physical Security Perimeter	The physical border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled.	39

Term	Definition	Source
Physical Vulnerability	Failure to provide physical security for a computer, such as leaving an unlocked workstation running in a workspace that is accessible to unauthorized users.	43
PICS	Protocol Implementation Conformance Statements	41
PII	See personally identifiable information.	43
PIN	See personal identification number.	43
PIXIT	Protocol Implementation eXtra Information for Testing	41
PKI [See public Key Infrastructure]	Public Key Infrastructure	41
PKI	See public key infrastructure.	43
Plaintext	Unencrypted data with format additions or changes, such as framing or padding.	10
Plaintext	Unencrypted information. [ISO/IEC 10116: 2006-02-01]	41
Plaintext	Unenciphered information. [ISO 8372: 1987, ISO/IEC 9797-1: 1999, ISO/IEC 9798-1: 1997, ISO/IEC CD 10116 (12/2001), ISO/IEC WD 18033-1 (12/2001)]	42
Plaintext	Data in its unencrypted or decrypted form.	43
Plaintext Key	An unencrypted cryptographic key.	1, 10
Plaintext Port	The cryptographic module communications port connected to a protected device. All communications on this port are in cleartext.	10
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.	15, 28
Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.	34
Platform for Privacy Preferences Project (P3P)	An open privacy specification developed and administered by the World Wide Web Consortium (W3C) that, when implemented, enables people to make informed decisions about how they want to share personal information with Web sites.	43

Term	Definition	Source
PLC	See Programmable Logic Controller.	33
Point of Delivery (POD)	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction leaves or a Load-Serving Entity receives its energy.	34
Point of Receipt (POR)	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a Generator delivers its output.	34
Point-to-Point Key Establishment	The direct establishment of keys between entities, without involving a third party. [ISO/IEC 11770-2; 1996]	42
Point-to-Point Protocol (PPP)	The protocol defined in RFC 1661, the Internet standard for transmitting network layer datagrams (e.g. IP packets) over serial point-to-point links.	41
Point to Point Transmission Service (PTP)	The reservation and transmission of capacity and energy on either a firm or non-firm basis from the Point(s) of Receipt to the Point(s) of Delivery.	34
Point-to-Point Tunneling Protocol	A new technology for creating Virtual Private Networks (VPNs), developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum. A VPN is a private network of computers that uses the public Internet to connect some nodes. Because the Internet is essentially an open network, the Point-to-Point Tunneling Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.	13
Pooling	See throttling.	43
Port	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).	1, 10
Port	1. The entry or exit point from a computer for connecting communications or peripheral devices. 2. An aperture for passage of steam or other fluids.	33
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or	14, 15, 25

Term	Definition	Source
	individuals.	
Prefix Free Representation	A representation of a data element for which concatenation with any other data does not produce a valid representation. [ISO/IEC FDIS 15946-3 (02/2001)]	42
Pre-signature	A value computed in the signature process which is a function of the randomizer but is independent of the message. [ISO/IEC 9796-3: 2000] A value computed in the signature process which is a function of the randomizer but which is independent of the message. [ISO/IEC 14888-1: 1998, ISO/IEC WD 15946-4 (10/2001)]	42
Pretty Good Privacy (PGP)	A publicly available encryption software program based on public key cryptography. The message formats are specified in RFC 1991 and RFC 2440. [ISO/IEC 18028-4: 2005-04-01]	41
Principal	An entity whose identity can be authenticated. [ISO/IEC 9798-1: 1997]	42
Principal	See security principal.	43
Privacy	The control customers have over the collection, use, and distribution of their personal information.	43
Privacy Compromise	A scenario in which an unauthorized individual is able to gain access to personal or confidential information about another user.	43
Privacy Impact Assessment	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.	15, 29
Privacy Policy	An organization's requirements for complying with privacy regulations and directives. The policy is expressed in a privacy statement.	43
Privacy Statement	A document describing a company's position on privacy, detailing what information its Web site collects, with whom the data is shared, and how users can control the use of their personal data.	43
Privacy Wizard	A software tool developed by Microsoft that helps businesses craft privacy policies based on widely accepted	43

Term	Definition	Source
	privacy principles. Currently, the Privacy Wizard is being updated to include support for the Platform for Privacy Preferences Project..	
Private Accreditation Exponent	Value known only to the accreditation authority, and which is used in the production of claimants' private accreditation information. This value shall be kept secret. This value is related to the public accreditation verification exponent. [ISO/IEC 9798-5: 1999]	42
Private Accreditation Exponent	Private information provided to a claimant by an accreditation authority, and of which a claimant proves knowledge, thereby establishing the claimant's identity. [ISO/IEC 9798-5: 1999]	42
Private Decipherment Key	Private key which defines the private decipherment transformation. [ISO/IEC 9798-1: 1997]	42
Private Decipherment Transformation	Decipherment transformation determined by an asymmetric encipherment system and the private key of an asymmetric key pair. [ISO/IEC 9798-5: 1999]	42
Private Fix	An unofficial hotfix which may not be fully tested or packaged. It is released to the customer to verify that it solves the problem before final testing and packaging.	43
Private Key	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.	1, 10
Private Key	1. That key of an entity's asymmetric key pair which should only be used by that entity. [ISO/IEC 11770-1: 1996] 2. One of a pair of keys used to perform asymmetric encryption in public key cryptography. The private key is kept secret, while the public key may be widely distributed. In a sense, one key "locks" a lock; while the other is required to unlock it. It should not be feasible to deduce the private key of a pair given the public key, and in high quality algorithms no such technique is known. [WIKI]	41
Private Key	That key of an entity's asymmetric key pair which should only be used by that entity. NOTE - A private key shall not normally be disclosed. [ISO/IEC 11770-1: 1996, ISO/IEC WD 18033-1 (12/2001)] That key of an entity's asymmetric key pair which should only be used by that entity. NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. [ISO/IEC 9798-1:	42

Term	Definition	Source
	1997, ISO/IEC FDIS 15946-3 (02/2001)] That key of an entity's asymmetric key pair which can only be used by that entity. NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. [ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1 (11/2001)] That key of an entity's asymmetric key pair which should only be used by that entity. [ISO/IEC FDIS 9796-2 (12/2001)]	
Private Key	One of two keys in public key encryption. The user keeps the private key secret and typically uses it to digitally sign data, or to decrypt data that has been encrypted with the corresponding public key.	43
Private Signature Key	Private key which defines the private signature transformation. NOTE – This is sometimes referred to as a secret signature key. [ISO/IEC 9798-1; 1997] Private key which defines the private signature transformationl [ISO/IEC FDIS 9796-2 (12/2001)]	42
Privileges	See user rights.	43
Pro Forma Tariff	Usually refers to the standard OATT and/or associated transmission rights mandated by the U.S. Federal Energy Regulatory Commission Order No. 888.	34
Process	An organised set of activities which uses resources to transform inputs to outputs. [ISO/IEC WD 15443-1 (11/2001)]	42
Process Assurance	Assurance derived from an assessment of activities of a process. [ISO/IEC WD 15443-1 (11/2001)]	42
Process Control	1. Descriptive of systems in which computers or controllers are used for automatic regulation of operations or processes. Typical are operations wherein the operation control is applied continuously and adjustments to regulate the operation are directed by the computer to keep the value of a controlled variable constant. Contrasted with numerical control. 2. The regulation or manipulation of variables influencing the conduct of a process in such a way as to obtain a product of desired quality and quantity in an efficient manner.	33
Process Control Engineering	A branch of engineering that deals with ways and means of keeping process variables as close as possible to desired	33

Term	Definition	Source
	values, or keeping them within specified ranges.	
Process Control Loop	A system of control devices linked together to control one phase of a process.	33
Process Engineer's Console	A man-machine interface, consisting of various information entry/retrieval devices arranged as a packaged unit, it is used by the person responsible for the performance of a manufacturing process to adjust the external behavior of the process controller. See also operator's console and programmer's console.	33
Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. [ISO/IEC 15408-1: 1999]	42
Programmable Logic Controller (PLC)	A PLC is a hardened, special-purpose computer that was developed to replace relay-based control systems. PLCS are often integrated with DCSs to obtain the benefit of a superior user interface by the DCS consoles. PCs are being used to replace PLCs in some applications since the offer standard hardware, software, and graphical user interfaces.	32
Programmable Logic Controller (PLC)	Abbreviation for programmable logic controller, microcomputer-based control device used to replace relay logic.	33
Programmer's Console	A man-machine interface, consisting of various information entry/retrieval devices, arranged as a packaged unit. It is used by the programmer of a computer control system for a manufacturing process, to monitor, modify, and control the internal behavior of the digital controller. See also operator's console, process engineer's console.	33
Proof	The corroboration that evidence is valid in accordance with the non-repudiation policy in force. NOTE – Proof is evidence that serves to prove truth or existence of something. [ISO/IEC WD 13888-1 (11/2001)]	42
Proof-of-Possession (PoP)	A verification process to prove that the owner of a key pair actually has the private key associated with the public key.	10
Protection Profile	An implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs. [FIPS 140-2]	41
Protection Profile	An implementation-independent set of security requirements for a category of IT products or systems that meet specific consumer needs. [ISO/IEC 15292: 2001] An implementation-independent set of security requirements	42

Term	Definition	Source
	for a category of TOEs that meet specific consumer needs. [ISO/IEC 15408-1: 1999]	
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.	15
Proxy Server	A firewall component that manages Internet traffic to and from a local area network (LAN) and can provide other functions, such as document caching and access control.	43
Pseudorandom Number Generator (PRNG)	An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the PRNG “appears” to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. [RFC2828]	41
Pseudo-Tie	A telemetered reading or value that is updated in real time and used as a “virtual” tie line flow in the AGC/ACE equation but for which no physical tie or energy metering actually exists. The integrated value is used as a metered MWh value for interchange accounting purposes.	34
Public	Information that can be shared with the general public.	13
Public Accreditation Verification Exponent	Value agreed by all members of a group of entities, and which, in conjunction with the modulus, determines the value of the private accreditation exponent. [ISO/IEC 9798-5; 1999]	42
Public Encipherment Key	Public key which defines the public encipherment transformation. [ISO/IEC 9798-1: 1997]	42
Public Encipherment Transformation	Encipherment transformation determined by an asymmetric encipherment system and the public key of an asymmetric key pair. [ISO/IEC 9798-5: 1999]	42
Public Key	A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered CSPs.)	1, 10
Public Key	1. That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1: 1997] 2. A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. [FIPS 140-2]	41

Term	Definition	Source
Public Key	That key of an entity's asymmetric key pair which can be made public. [ISO/IEC FDIS 9796-2 (12/2001), ISO/IEC 11770-1: 1996, ISO/IEC WD 18033-1 (12/2001)] That key of an entity's asymmetric key pair which can be made public. NOTE - In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1 (11/2001), ISO/IEC FDIS 15946-3 (02/2001)]	42
Public Key	One of two keys in public key encryption. The user releases this key to the public, who can use it to encrypt messages to be sent to the user and to verify the user's digital signature. Compare with private key.	43
Public key (asymmetric) cryptographic algorithm	A cryptographic algorithm that uses two related keys — a public key and a private key. The two keys have the property that deriving the private key from the public key is not computationally feasible. [1]	1, 10
Public Key Asymmetric Cryptographic Algorithm	A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. [FIPS 140-2]	41
Public Key Certificate	A set of data that uniquely identifies an entity, contains the entity’s public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [FIPS 140-2]	1, 10, 41
Public Key Certificate	The public key information of an entity signed by the certification authority and thereby rendered unforgeable. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996, ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1 (11/2001)] The public key information of an entity signed by the certification authority and thereby rendered unforgeable. NOTE - In the context of this part of ISO/IEC 9796 the public key information contains the information about the verification key and the domain parameters. [ISO/IEC 9796-3: 2000]	42
Public Key Cryptography	1. The type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with	41

Term	Definition	Source
	knowledge of both parts of the decryption process can decrypt the cipher text. Note: Commonly called non-secret encryption in professional cryptologic circles. FIREFLY is an application of public key cryptography. [NIS] 2. [An] Encryption system using a linked pair of keys. What one pair of keys encrypts, the other pair decrypts. [INFOSEC-99] [ATIS]	
Public Key Derivation Function	A domain parameter, whose function is to map strings of bits into positive integers. NOTE 1 - This function is used to transform an entity's identification data into the entity's verification key, and satisfies the following two properties. • l It is computationally infeasible to find any two distinct inputs which map to the same output. • l Either the probability that a randomly chosen value Y is in the range of the function is negligibly small, or for a given output it is computationally infeasible to find for a given output an input which maps to this output. NOTE 2 - Negligibility and computational infeasibility depend on the specific security requirements and environment. [ISO/IEC 14888-2: 1999]	42
Public Key Encryption	A method of encryption that uses a pair of mathematically related keys: a public key and a corresponding private key. Either key can be used to encrypt data, but the corresponding key must be used to decrypt it. Also called asymmetric encryption.	43
Public Key Information	Information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, and the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms. [ISO/IEC 9798-1: 1997] Information specific to a single entity which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, and the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms. [ISO/IEC 11770-1: 1996]	42

Term	Definition	Source
	Information containing at least the entity's distinguishing identifier and public key. The public key information is limited to data regarding one entity, and one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, restrictions on key usage, the validity period, or the involved algorithms, included in the public key information. [ISO/IEC 11770-3: 1999]	
Public Key Infrastructure (PKI)	A framework that is established to issue, maintain and revoke public key certificates. [RFC2828]	10, 41
Public Key Infrastructure (PKI)	The system consisting of TTPs, together with the services they make available to support the application (including generation and validation) of digital signatures, and of the persons or technical components, who use these services. NOTE - Sometimes the persons and the technical components participating in a PKI by using the services of TTPs, but not being TTPs themselves, are referred as end entities. An example of a technical equipment used by an end entity is a smart card which may be used as a storage and or processing device. [ISO/IEC 15945: 2002]	42
Public Key Infrastructure (PKI)	A framework encompassing the laws, policies, standards, hardware, and software to provide and manage the use of public key cryptography on public networks such as the Internet.	43
Public Key System (for Digital Signature)	Cryptographic scheme consisting of three functions: • Key production, a method for generating a key pair made up of a private signature key and a public verification key, • Signature production, a method for generating a signature • from a message representative F and a private signature key, and • Signature opening, a method for obtaining the recovered message representative F* from a signature • and a public verification key. The output of this function also contains an indication as to whether the signature opening procedure succeeded or failed.	42
Public Verification Key	Public key which defines the public verification transformation. [ISO/IEC 9798-1: 1997, ISO/IEC FDIS 9796-2 (12/2001)]	42
Purchasing-Selling	The entity that purchases or sells, and takes title to, energy,	34

Term	Definition	Source
Entity	capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.	
QFE	See Quick Fix Engineering.	43
QoS	See Quality of Service.	43
Quality of Service (QoS)	A set of quality assurance standards and mechanisms for data transmission.	43
Quick Fix Engineering (QFE)	A team within Microsoft that produces hotfixes. Most of these teams now refer to themselves as Sustained Engineering teams.	43
Race Condition	A condition caused by the timing of events within or among software components. Race conditions typically are associated with synchronization errors that provide a window of opportunity during which one process can interfere with another, possibly introducing a security vulnerability.	43
Radix	Base of a geometric progression. [ISO/IEC FCD 7064 (09/2000)]	42
Ramp Rate or Ramp	(Schedule) The rate, expressed in megawatts per minute, at which the interchange schedule is attained during the ramp period. (Generator) The rate, expressed in megawatts per minute, that a generator changes its output.	34
Random Number	A time variant parameter whose value is unpredictable. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996, ISO/IEC 11770-2: 1996]	42
Randomized	Dependent on a randomizer. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1; 1998, ISO/IEC WD 15946-4 (10/2001)]	42
Randomizer	A secret data item produced by the signing entity in the pre-signature production process, and not predictable by other entities. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)]	42
Rating	The operational limits of a transmission system element under a set of specified conditions.	34
Reactive Power	The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive	34

Term	Definition	Source
	power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar).	
Real Power	The portion of electricity that supplies energy to the load.	34
Reallocation	The total or partial curtailment of Transactions during TLR Level 3a or 5a to allow Transactions using higher priority to be implemented.	34
Receiving Balancing Authority	The Balancing Authority importing the Interchange.	34
Recipient	The entity that gets (receives or fetches) a message for which non-repudiation services are to be provided. [ISO/IEC WD 13888-1 (11/2001)]	42
Recommended	The word “recommended” is used to indicate flexibility of choice with a strong preference alternative.	10
Record	1. A group of related facts or fields of information treated as a unit, thus a listing of information, usually in printed or printable form. 2. To put data into a storage device. 3. A segment of a file consisting of an arbitrary number of words or characters. 4. In data processing, a group of data that contains all the information about a single item.	33
Record (noun)	On a computer tape, the smallest group of words which can be located and input by the computer. In telemetry systems, this is usually 1,000 to 4,000 data words.	33
Record (verb)	To store on some permanent (generally magnetic) medium, as on a magnetic tape or disk.	33
Records	The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).	14, 15
Recoverable Part	Part of the message conveyed in the signature. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Reduction-function	A function RED that is applied to the block H_q of length $L_\bullet$ to generate the hash-code H of length L_p. [ISO/IEC 10118-4: 1998]	42
Redundancy	Any information that is known and can be checked. [ISO/IEC	42

Term	Definition	Source
	11770-2: 1996, ISO/IEC WD 13888-1 (11/2001)]	
Redundant Identity	Sequence of data items obtained from an entity's identification data by adding redundancy using techniques specified in ISO/IEC 9796. [ISO/IEC 9798-5: 1999]	42
Reference Monitor	The concept of an abstract machine that enforces TOE access control policies. [ISO/IEC 15408-1: 1999]	42
Reference Validation Mechanism	An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing. [ISO/IEC 15408-1; 1999]	42
Refinement	The addition of details to a component. [ISO/IEC 15408-1: 1999]	42
Reflection Attack	A masquerade which involves sending a previously transmitted message back to its originator. [ISO/IEC 9798-1: 1997]	42
Regional Reliability Organization	1. An entity that ensures that a defined area of the Bulk Electric System is reliable, adequate and secure. 2. A member of the North American Electric Reliability Council. The Regional Reliability Organization can serve as the Compliance Monitor.	34
Regional Reliability Plan	The plan that specifies the Reliability Coordinators and Balancing Authorities within the Regional Reliability Organization, and explains how reliability coordination will be accomplished.	34
Register	A set of files (electronic, or a combination of electronic and paper) containing entry labels and their associated definitions and related information. [ISO/IEC 15292: 2001]	42
Register Entry	The information within a register relating to a specific PP or package. [ISO/IEC 15292: 2001]	42
Registration	The process of assigning a register entry. [ISO/IEC 15292: 2001]	42
Registration Authority (RA)	An entity who is responsible for identification and authentication of subjects of certificates, but is not a CA or an AA, and hence does not sign or issue certificates. An RA may assist in the certificate application process, revocation process, or both. [ISO/IEC TR 14516: 2000] Authority entitled and trusted to perform the registration service as described below. [ISO/IEC 15945: 2002]	42
Registration Service	The service of identifying entities and registering them in a	42

Term	Definition	Source
	way that allows the secure assignment of certificates to these entities. [ISO/IEC 15945: 2002]	
Regulating Reserve	An amount of reserve responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin.	34
Regulating Service	The process whereby one Balancing Authority contracts to provide corrective response to all or a portion of the ACE of another Balancing Authority. The Balancing Authority providing the response assumes the obligation of meeting all applicable control criteria as specified by NERC for itself and the Balancing Authority for which it is providing the Regulation Service.	34
Reliability	The property of consistent intended behaviour and results. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Reliability Coordinator Area	The collection of generation, transmission, and loads within the boundaries of the Reliability Coordinator. Its boundary coincides with one or more Balancing Authority Areas.	34
Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.	34
Reliability Coordinator Information System (RCIS)	The system that Reliability Coordinators use to post messages and share operating information in real time.	34
Remedial Action Scheme (RAS)	See "Special Protection System"	34
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.	15
Remote Access	Pertaining to communication with a data processing facility by one or more stations that are distant from that facility.	33
Remote Attack	An attack that targets a computer other than the one that the attacker is interactively logged on to. For example, an attacker can log on to a workstation and attack a server on	43

Term	Definition	Source
	the same network or on an entirely different one.	
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.	15
Remote Procedure Call (RPC)	A communication mechanism that allows computers to communicate with one another over a network. An RPC consists of a procedure identifier, parameters passed to the procedure, and a value returned to the caller (client computer) after the procedure has executed on the remote system (server computer).	43
Removable Cover	A cover designed to permit physical access to the contents of a cryptographic module.	1, 10
Replay	Recording message traffic and “playing it back” to a device later in order to make it do what you want.	3, 10
Replay Attack	1. A masquerade which involves use of previously transmitted messages. [ISO/IEC 9798-1: 1997-08-01] 2. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack. [WIKI]	41
Replay Attack	A masquerade which involves use of previously transmitted messages. [ISO/IEC 9798-1: 1997]	42
Reportable Disturbance	Any event that causes an ACE change greater than or equal to 80% of a Balancing Authority’s or reserve sharing group’s most severe contingency. The definition of a reportable disturbance is specified by each Regional Reliability Organization. This definition may not be retroactively adjusted in response to observed performance.	34
Repudiation	The ability to deny that a transaction took place (for example an individual could claim “I never performed that action”).	3, 10
Repudiation	The ability to deny that a transaction took place (e.g., “I never performed that control.” [RFC2828]	41
Repudiation	The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.	43
Request for Collaboration (RFC)	A request for development engagement where Product Support Services (PSS) is technically blocked; also used to formalize and track support statement requests and to	43

Term	Definition	Source
	review proposed action plans. The request process was introduced to help reduce the time it takes to provide a solution to a customer. An RFC may become a DCR, CDCR, or hotfix request.	
Requests for Comments (RFC)	The RFC document series is a set of technical and organizational notes about the Internet, which discuss many aspects of computer networking, including protocols, procedures, programs, and concepts. The official specification documents of the Internet Protocol suite are recorded and published as standards track RFCs. The RFC publication process plays an important role in the Internet standards process.	10
Reserve Sharing Group	A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply operating reserves required for each Balancing Authority's use in recovering from contingencies within the group. Scheduling energy from an Adjacent Balancing Authority to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., ten minutes). If the transaction is ramped in quicker (e.g., between zero and ten minutes) then, for the purposes of Disturbance Control Performance, the Areas become a Reserve Sharing Group.	34
Residual Risk	The remaining risk after the security controls have been applied.	12
Residual Risk	The risk that remains after implementation of the IT security plan. [ISO/IEC PDTR 13335-1 (11/2001)] Any combination of the risk that have been accepted by the organization, the risks that remain after all identified controls have been implemented because further action could not be identified. [ISO/IEC 17799; 2000]	42
Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.	34
Response	Data item sent by the claimant to the verifier, and which the verifier can process to help check the identity of the claimant. [ISO/IEC 9798-5: 1999]	42
Response Rate	The Ramp Rate that a generating unit can achieve under normal operating conditions expressed in megawatts per minute (MW/Min).	34
Restricted	Information with limited or confined distribution, which is not accessible to the general public or other Company	13

Term	Definition	Source
	employees.	
RFC	See Request for Collaboration.	43
Rights	See user rights.	43
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [FIPS PUB 200 (2005)]	10
Risk	Possibility that a particular threat will adversely impact a system by exploiting a particular vulnerability.	12
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals results from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.	14, 15, 30
Risk	A measure combining the severity and likelihood of harm from an event. Alternatively, the likelihood of an adverse outcome. Risk = L (attack) x P (success) x C.L (attack), i.e. the likelihood of attack depends on the motivation, capabilities and intent of adversaries. P (success) is the probability of success and depends on vulnerabilities present. C is the consequence(s). Risk is also the potential for damage to or loss of an asset. Risk in a chemical security perspective includes: 1) the potential for a catastrophic outcome such as intentional release of hazardous materials to the atmosphere, 2) theft of chemicals that could be used as weapons, 3) contamination of chemicals that may later harm the public, or 4) economic costs of the damage or disruption of a chemical process.	32
Risk	1. The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence. [ISO/IEC 13335-1: 2004-11-15] 2. An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. [RFC2828]	41
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Risk Analysis	The process of estimating risks.	32

Term	Definition	Source
Risk Analysis	The systematic process of estimating the magnitude of risks. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.	15, 30
Risk Assessment	The process of using risk analysis results to make decisions on risk reduction.	32
Risk Assessment	1. A risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The target of the risk assessment process is the identification and evaluation of risks, which have negative impacts to identified assets and the definition of appropriate safeguards and actions, which minimize the effects of the identified risks. [ISO/IEC 5th WD 15443-3:2005-06-03] 2. Risk assessment is a step in the risk management process. Risk assessment is measuring two quantities of the risk, the magnitude of the potential loss, and the probability that the loss will occur. Risk assessment may be the most important step in the risk management process, and may also be the most difficult and prone to error. Once risks have been identified and assessed, the steps to properly deal with them are much more programmatical. [WIKI]	41
Risk Assessment	The process of combining risk identification, risk analysis and risk evaluation. [ISO/IEC PDTR 13335-1 (11/2001)] The assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence. [ISO/IEC 17799: 2000]	42
Risk Evaluation	The process of comparing analysed levels of risk against pre-established criteria and identifying areas needing risk treatment. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Risk Identification	The process of identifying risks considering business objectives, threats and vulnerabilities as the basis for further analysis. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Risk Management	Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.	12, 30
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit	15

Term	Definition	Source
	analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.	
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.	14
Risk Management	The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost	32
Risk Management	The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources. [ISO/IEC PDTR 13335-1 (11/2001)] The process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost. [ISO/IEC 17799: 2000]	42
Risk Treatment	The process of defining an IT security management plan based on risk evaluation. [ISO/IEC PDTR 13335-1 (11/2001)]	42
Role	A set of transactions that a user or set of users can perform within the context of an organization.	10
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE. [ISO/IEC 15408-1: 1999]	42
Role-based Authorization	A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.	43
Rollup	See update rollup.	43
Round-function	A function ●(.,.) that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L_2. It is used iteratively as part of a hash-function, where it combines a data string of length L_1 with the previous output of length L_2. [ISO/IEC 10118-1: 2000, ISO/IEC] Function ●(.,.) that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L2.	42

Term	Definition	Source
	NOTE - It is used iteratively as part of a hash-function, where it combines a data string of length L_1 with the previous output of length L_2. [ISO/IEC FDIS 9797-2 (09/2000)] A function ●(.,.) that transforms two binary strings of lengths *L*●· to a binary string of length *L*●·. NOTE - It is used iteratively as part of a hash-function, where it combines an 'expanded' data block of length L• with the previous output of length L•. [ISO/IEC 10118-4: 1998]	
RPC	See remote procedure call.	43
RSA	The public key algorithm invented by Rivest, Shamir, and Adleman.	10
RSA	RSA (Rivest, Shamir and Adleman) is an algorithm for public-key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys. [WIKI]	41
Safe Harbor Agreement	An agreement between the United States and the European Union (EU) regarding the transfer of personally identifiable information from the EU to the United States, which is consistent with Fair Information Practices. Companies that register for Safe Harbor with the U.S. Department of Commerce and abide by the agreement are deemed by the EU to provide adequate data protection for personally identifiable information transferred from the EU to the United States.	43
Safe Harbor Principles	Seven principles agreed to by the United States and the European Union (EU) for the transfer of personally identifiable information from the EU to the United States to which a company must adhere if it registers for Safe Harbor. The seven principles are categorized into the following subjects: notice; choice; access; onward transfer; security; data integrity; and enforcement. See also Safe Harbor Agreement.	43
Safeguard	A practice, procedure or mechanism that reduces risk. Note that the term ‘safeguard’ is normally considered to be synonymous with the term ‘control’. [ISO/IEC PDTR 13335-1 (11/2001)]	42

Term	Definition	Source
Safeguard	A technology, policy, or procedure that counters a threat or protects assets.	43
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.	12*, 14, 15
Salt	Random data produced by the signing entity during the generation of the message representative in Signature scheme 2. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Sandbox	A security mechanism used to constrain the actions a program can take. A sandbox restricts a program to a defined set of privileges and actions that reduce the likelihood that the program may damage the system hosting the program.	43
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.	12*, 14, 15
SCADA [See also Supervisory Control and Data Acquisition below.]	See “supervisory control and data acquisition system.”	10
SCADA [See also Supervisory Control and Data Acquisition below.]	Abbreviation for supervisory control and data acquisition technique (in industrial control/monitor work).	33
SCADA [See also Supervisory Control and Data Acquisition below.]	Supervisory Control and Data Acquisition. The term refers to a large-scale, distributed measurement and control system. The three components of a SCADA system are: • Multiple Remote Terminal Units (also known as RTUs). • Central Control Room with Host Computer(s). Communication infrastructure. [WIKI]	41

Term	Definition	Source
SCADA System	Supervisory Control and Data Acquisition systems are a combination of computer hardware and software used to send commands and acquire data for the purpose of monitoring and controlling.	13
Schedule	(Verb) To set up a plan or arrangement for an Interchange Transaction. (Noun) An Interchange Schedule.	34
Scheduled Frequency	60.0 Hertz, except during a time correction.	34
Scheduling Entity	An entity responsible for approving and implementing Interchange Schedules.	34
Scheduling Path	The Transmission Service arrangements reserved by the Purchasing-Selling Entity for a Transaction.	34
Scheme	Set of rules defining the environment, including criteria and methodology required to conduct an assessment. [ISO/IEC WD 15443-1 (11/2001)]	42
Scoping Guidance	Provides organizations with specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security controls in the control baseline.	15
Scoping Guidance	Specific factors related to technology, infrastructure, public access, scalability, common security controls, and risk that can be considered by organizations in the applicability and implementation of individual security controls in the security control baseline.	14
Script Kiddies	A kind of hacker who only uses code created by others.	43
Secondary Data Uses	Uses of personal information for purposes other than those for which the information was collected. The Fair Information Practices state that a person can provide personal information for a specific purpose without the fear that it may later be used for an unrelated purpose without that person's knowledge or consent.	43
Secret	Information that must be known only to authroised users and/or the TSF in order to enforce a specific SFP. [ISO/IEC 15408-1: 1999]	42
Secret Key	A cryptographic parameter that is held private by one or more entities to limit the ability to communicate or access that group or entity.	10

Term	Definition	Source
Secret Key	1. A key used with symmetric cryptographic techniques and usable only by a set of specified entities. [ISO/IEC 13888-1: 2004-06-01] 2. A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. [FIPS 140-2]	41
Secret Key	A key used with symmetric cryptographic techniques and usable only by a set of specified entities. [ISO/IEC 11770-1: 1996, ISO/IEC WD 13888-1 (11/2001)] A key used with symmetric cryptographic techniques by a set of specified entities. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)] Key used with symmetric cryptographic techniques by a set of specified entities. [ISO/IEC WD 18033-1 (12/2001)]	42
Secret Key Symmetric Cryptographic Algorithm	A cryptographic algorithm that uses a single secret key for both encryption and decryption. [FIPS 140-2]	41
Secure Envelope (SENV)	A set of data items which is constructed by an entity in such a way that any entity holding the secret key can verify their integrity and origin. For the purpose of generating evidence, the SENV is constructed and verified by a TTP with a secret key known only to the TTP. [ISO/IEC WD 13888-1 (11/2001)]	42
Secure Hash Standard (SHS)	The U.S. government standard (FIPS PUB 180-2) that specifies four secure hash algorithms (SHA-1, SHA-256, SHA-384, and SHA-512) that produce a fixed-length hash result for input data of any length less than 2**64 bits (for SHA-1 and SHA-256), or 2**128 bits (for SHA-384 and SHA-512).	10
Secure Shell	A set of commands and protocols that uses digital certificates for authenticating host and client as well as for encrypting communications to ensure security.	13
Secure Shell (SSH)	A protocol that provides secure remote login utilising an insecure network. SSH is proprietary but will become an IETF standard in the near future. SSH was originally developed by SSH Communications Security. [ISO/IEC 18028-4: 2005-04-01]	41
Secure Sockets Layer (SSL)	A protocol that provides secure data communication through data encryption. This protocol enables authentication, integrity, and data privacy over networks through a combination of digital certificates, public-key cryptography, and bulk data encryption. This protocol does not provide authorization or nonrepudiation.	43

Term	Definition	Source
Security	Protection against threats and attacks.	32
Security	1. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. [JP1] 2. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. [After JP1] 3. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. [JP1] [ATIS] 4. All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability. [ISO/IEC 13335-1]	41
Security	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability. NOTE - A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. This is usually considered in the context of an assessment of actual or perceived threats. [ISO/IEC WD 15443-1 (11/2001)]	42
Security	See computer security.	43
Security Alert	Documentation for developers that describes specific security risks and how to avoid them when implementing Microsoft software.	43
Security Assets	Fences, gates, alarm systems, guards, and other security elements that can individually or as a system be applied to critical electrical assets to maintain reliability or reduce risk.	36
Security Attribute	Information associated with subjects, users and/or objects that is used for the enforcement of the TSP. [ISO/IEC 15408-1: 1999]	42
Security Authority	The entity accountable for the administration of a security policy within a security domain. [ISO/IEC 15816; 2002]	42
Security Boundary	An explicitly defined continuous perimeter that establishes the physical or logical bounds of a security domain.	10

Term	Definition	Source
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.	14, 15, 25
Security Components (countermeasures)	Techniques such as firewalls, authentication modules, or encryption software used to improve the security performance of the Manufacturing and Control System.	11
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.	14, 15, 25
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.	14, 15
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.	15
Security Domain	A system or subsystem that is under the authority of a single trusted authority. Security domains may be organized (e.g., hierarchically) to form larger domains. [RFC2828]	10, 41
Security Domain	A collections of users and systems subject to a common security policy. [ISO/IEC 15816: 2002]	42
Security Element	An indivisible security requirement. [ISO/IEC WD 15443-1 (11/2001)]	42
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP. [ISO/IEC 15408-1: 1999]	42
Security Function Policy (SFP)	The security policy enforced by an SF. [ISO/IEC 15408-1: 1999]	42
Security Guidelines	Security guidelines define the objectives and constraints for the security program. Guidelines are created at several levels, ranging from company or corporate policy to specific operational constraints (e.g., remote access). In general, guidelines provide answers to the questions “what” and “why” without dealing with “how.” Guidelines are normally stated in terms that are technology-independent. [ISA SP99]	41
Security Identifier (SID)	In Windows-based systems, a unique value that identifies a user, group, or computer account within an enterprise. Every account is issued a SID when it is created.	43

Term	Definition	Source
Security Impact Analysis	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.	15
Security Information Object	An instance of an SIO class. [ISO/IEC 15816: 2002]	42
Security Information Object Class	An Information Object Class that has been tailored for security use. [ISO/IEC 15816: 2002]	42
Security Key	A four-character code used for additional security by Web sites on the Microsoft Passport Network.	43
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.	15
Security Management	In network management, the set of functions (a) that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences and (b) that includes many subfunctions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges. [ATIS]	41
Security Objective	Confidentiality, integrity, or availability.	14, 15, 25
Security Objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions. [ISO/IEC 15408-1; 1999]	42
Security Performance	Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, post compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.	11

Term	Definition	Source
Security Performance	Security Performance—Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, post compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance. [ISA SP99]	41
Security Perimeter	See Accreditation Boundary.	15
Security Plan	A document that describes an operator's plan to address security issues and related events, such as security assessments and mitigation options, and includes security levels and response measures to security threats.	13
Security Plan	See System Security Plan.	14, 15
Security Policies	Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from company or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.	11
Security Policy	See "Cryptographic module security policy."	10
Security Policy	1. Set rules internal to an organizational unit that regulate how this unit protects the management of its assets conform to specified organizational objectives within its legal and cultural context. [ISO/IEC 15408] 2. A security policy is a plan of action for tackling security issues, or a set of regulations for maintaining a certain level of security. It can span anything from the practices for securing a single computer, to building/premises security, to securing the existence of an entire nation-state. [WIKI]	41
Security Policy Information File	A construct that conveys domain-specific security policy information. [ISO/IEC 15816: 2002]	42
Security Practices	Security practices provide a means of capturing experiences and activities that help ensure system protection and reduce potential Manufacturing and Control Systems compromise. Subject areas include physical security, procedures, organization, design, and programming. Security practices include the actual steps to be taken to ensure system protection.	11

Term	Definition	Source
Security Principal	In Windows-based systems, a user, group, or computer that is automatically assigned a security identifier to control access to resources.	43
Security Procedures	Security procedures define exactly how practices are implemented and executed. They are implemented through personnel training and actions using currently available and installed technology (such as disconnecting modems). Procedures and contained criteria also include more technology-dependent system requirements that need careful analysis, design, planning, and coordinated installation and implementation.	11
Security Program	A security program brings together all aspects of managing security, ranging from the definition and communication of guidelines through implementation of best industry practices and ongoing operation and auditing.	11
Security Requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.	14, 15
Security Risk Assessment	The process of analyzing threats to and vulnerabilities of an information system (IS) and the potential impact the loss of information or capabilities of a system would have on national [or any system] security. The resulting analysis is used as a basis for identifying appropriate and cost-effective countermeasures. [INFOSEC-99]	41
Security Services	Mechanisms used to provide confidentiality, data integrity, authentication or non-repudiation of information. [RFC2828]	41
Security Target	A set of security requirements and specifications to be used as the basis for evaluation of an identified IT product or system. [ISO/IEC 15292: 2001] A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE. [ISO/IEC 15408-1: 1999]	42
Security Update	A broadly released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated based on their severity, which is indicated in the Microsoft security bulletin as critical, important, moderate, or low.	43
Security Vulnerability	A vulnerability in software that is addressed by a Microsoft security update and security bulletin or a service pack.	43
Security Vulnerability	A SVA is the process of determining the likelihood of an adversary successfully exploiting a vulnerability (a threat	32

Term	Definition	Source
Analysis (SVA)	scenario), and the resulting degree of damage or impact on an asset. It can include qualitative risk analysis.	
Selection	The specification of one or more items from a list in a component. [ISO/IEC 15408-1: 1999]	42
Semiformal	Expressed in a restricted syntax language with defined semantics. [ISO/IEC 15408-1: 1999]	42
Sending Balancing Authority	The Balancing Authority exporting the Interchange.	34
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.	14, 15, 31
Sensitive Data	From the European Union perspective, personally identifiable information regarding race or ethnic origin, political opinions, religious or philosophical beliefs, sexual preference, or trade union membership. Within the United States, sensitive information also includes information about health, finances, and children.	43
Sensor or Monitor	A compnent/agent of an IDS, which collects event data from an IT system under observation. [ISO/IEC DTR 15947 (10/2001)]	42
Sequence Number	A time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996, ISO/IEC 11770-2: 1996, ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Server	A device or computer system that is dedicated to providing specific facilities to other devices attached to the network.	10
Server	A device or application that provides information or services to client applications and devices. [ATIS]	41
Service Pack	A tested, cumulative set of all hotfixes, security updates, critical updates, and updates created and fixes for defects found internally since the release of the software. Service packs may also contain a limited number of customer-requested design changes or features.	43
Service Release	See service pack.	43

Term	Definition	Source
Session	A period defined either by an amount of time, a number of messages, or a user-initiated change during which two CMs operate using specific parameters.	10
Session	Layer 5 of OSI. [ISA definition of OSI: Abbreviation for open system interconnection (a connection between one communication system and another using a standard protocol). OSI reference model, Layer 5 – Session: provides user-to-user connections.]	33
Session Establishment Key	Cryptographic value(s) used to set up the parameters that secure the communications between two devices or persons.	10
Session Key	A session key is a key used for encrypting one message or a group of messages in a communication session. Session keys introduce complication in a crypto system, normally an undesirable end. However, they also help with some real problems, which is why they are used. There are two primary reasons for session keys: • First, several cryptanalytic attacks are made easier as more material encrypted with a specific key is available. By limiting the material processed using a particular key, those attacks are made more difficult. Second, many otherwise good encryption algorithms require that keys be distributed securely before encryption can be used. All secret key algorithms have this undesirable property. There are other algorithms which don't require secure distribution of secret keys, but they are too slow to be practical for encrypting long messages (see public key cryptography). By using one of these "asymmetric" algorithms to distribute an encrypted secret key for another, faster, algorithm, it's possible to improve overall performance considerably. [WIKI]	41
SHA-1 Hash Function	The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard. The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512 — sometimes collectively referred to as SHA-2. Attacks have been found for both SHA-0 and SHA-1, while	41

Term	Definition	Source
	no attacks have been reported on the SHA-2 variants. [WIKI]	
Shall	Equivalent to "is required to", and is used to indicate mandatory requirements, strictly to be followed in order to conform to the standard and from which no deviation is permitted.	10
Shall	The term “shall” is used in this standard to indicate those practices that are mandatory	13
SHA-1, SHA-256, SHA-384, and SHA-512	See “Secure Hash Standard.”	10
Shared Secret	A value that is generated during a key agreement process. The shared secret is typically used to derive keying material for a symmetric key algorithm.	10
Should	Equivalent to “is recommended that,” is used to indicate several possibilities recommended as particularly suitable, without mentioning or excluding other, that a certain course of action is preferred but not required, that (in the negative form) a certain course of action is deprecated but not prohibited.	10
Should	The term “should” is used in this standard to indicate: ● Those practices for which engineering judgment is required. ● Those practices which are preferred, but for which operators may determine that alternative practices are equally or more effective.	13
SID	See security identifier.	43
Signature	String of bits resulting from the signature process. [ISO/IEC FDIS 9796-2 (12/2001)] The string of bits resulting from the signature process. NOTE - This string of bits may have internal structure specific to the signature mechanism. The signatures produced by the mechanisms specified in this part of ISO/IEC 9796 have two parts, of which only the second one depends on the signature key. [ISO/IEC 9796-3: 2000] The string of bits resulting from the signature process. [ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)] The string of bits resulting from the signature process. NOTE - This string of bits may have internal structure	42

Term	Definition	Source
	specific to the signature mechanism. [ISO/IEC 14888-1: 1998]	
Signature Equation	An equation defining the signature function. [ISO/IEC 14888-1: 1998]	42
Signature Function	A function in the signature process which is determined by the signature key and the domain parameters. A signature function takes the assignment and possibly the randomizer as inputs and gives the second part of the signature as output. [ISO/IEC 14888-1: 1998] A function in the signature process which is determined by the signature key and the domain parameters. A signature function takes the assignment and possibly the randomizer as inputs and gives the second part of the signature as output. NOTE - In the context of this part of ISO/IEC 9796, the assignment is the data input. [ISO/IEC 9796-3: 2000]	42
Signature Key	A secret data item specific to an entity and usable only by this entity in the signature process. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)]	42
Signature Process	A process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)]	42
Signature System	A system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification. [ISO/IEC 11770-3: 1999, ISO/IEC FDIS 15946-3 (02/2001)]	42
Signed Message	A set of data items consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998] A set of data items formed by the signature, the part of the message which cannot be recovered from the signature, and an optional text field. [ISO/IEC WD 15946-4 (10/2001)]	42
Signer	The entity generating a digital signature. [ISO/IEC WD 13888-1 (11/2001)]	42
Simple Network Management Protocol	A standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP compliant devices contain a MIB which supplies the pertitent	13

Term	Definition	Source
	attributes of a device. Some attributes are fixed or “hard coded” in the MIB while others are dynamic values calculated by agent software running on the device.	
Sink Balancing Authority	The Balancing Authority in which the load (sink) is located for an Interchange Transaction. (This will also be a Receiving Balancing Authority for the resulting Interchange Schedule.)	34
Slave	A device that gathers data or performs control operations in response to requests from the master, and sends response messages in return. A slave device may also generate unsolicited responses.	10
Slave	A mechanical or electronic device that is under the control of a another [sic] device.	33
Smart Card	A credit card–sized device with an embedded microprocessor and a small amount of storage that is used, with an access code, to enable certificate-based authentication. Smart cards securely store certificates, public and private keys, passwords, and other types of personal information.	43
Sniffing	See interception.	10, 41
SOF-basic [Ed. note: See also Strength of Function below.]	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential. [ISO/IEC 15408-1: 1999]	42
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential. [ISO/IEC 15408-1: 1999]	42
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential. [ISO/IEC 15408-1: 1999]	42
Software	The programs and data components within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution.	1, 10
Software	1. A set of programs, procedures, rules, and possibly associated documentation concerned with the operation of a computer system, for example, compilers, library routines, manuals, circuit diagrams. 2. Contrast with hardware. [ISA definition of hardware: 1. Physical equipment directly involved in performing industrial process measuring and	33

Term	Definition	Source
	controlling functions. 2. In data processing, hardware refers to the physical equipment associated with the computer.]	
Software Update	Any update, update rollup, service pack, feature pack, critical update, security update, or hotfix used to improve or fix software released by Microsoft.	43
Software Upgrade	See upgrade.	43
Source Balancing Authority	The Balancing Authority in which the generation (source) is located for an Interchange Transaction. (This will also be a Sending Balancing Authority for the resulting Interchange Schedule.)	34
SP	See service pack.	43
Spam	Unsolicited commercial e-mail. Also known as junk e-mail.	43
Special Protection System (Remedial Action Scheme)	An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) underfrequency or undervoltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS). Also called Remedial Action Scheme.	34
Specific SIO Class	An SIO class in which the data types for all components are fully specified. [ISO/IEC 15816; 2002]	42
Specifications	An assessment object that includes document-related artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.	15
Spinning Reserve	Unloaded generation that is synchronized and ready to serve additional demand.	34

Term	Definition	Source
Split Knowledge	A process by which a cryptographic key is divided into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.	10
Sponsor	An entity (organisation, individual, etc.) responsible for the content of a register entry. [ISO/IEC 15292: 2001]	42
Spoof	Pretending to be an authorized user.	3, 10
Spoof	Pretending to be an authorized user and performing an unauthorized action. [RFC2828]	41
Spoof	To make a transmission appear to come from a user other than the user who performed the action.	43
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.	15
Spyware	Spyware covers a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party. Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, however, spyware - by design - exploits infected computers for commercial gain. Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites. [WIKI]	41
Spyware	Software that can display advertisements (such as pop-up ads), collect information about you, or change settings on your computer, generally without appropriately obtaining your consent.	43
SSL	Secure Sockets Layer. SSL provides endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated; mutual authentication requires public key infrastructure (or PKI) deployment to clients. The protocols	41

Term	Definition	Source
	allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. [WIKI]	
SSL	See Secure Sockets Layer (SSL).	43
Stability	The ability of an electric system to maintain a state of equilibrium during normal and abnormal conditions or disturbances.	34
Stability Limit	The maximum power flow possible through some particular point in the system while maintaining stability in the entire system or the part of the system to which the stability limit refers.	34
Standard	A reference established by authority, custom, or general consent as a model or example. For the purposes of the U.S. Chemicals Sector Cybersecurity Strategy, a standard is considered a voluntary practice or guideline that is established by consensus of the industry.	32
Starting Variable (SV)	Variable derived from the initializing value and used in defining the starting point of the modes of operation. NOTE - The method of deriving the starting variable from the initializing value is not defined in this International Standard. It needs to be described in any application of the modes of operation. [ISO 8372: 1987] Variable defining the starting point of the mode of operation. NOTE - The method of deriving the starting variable from the initializing value is not defined in this International Standard. It needs to be described in any application of the modes of operation. [ISO/IEC CD 10116 (12/2001)]	42
Status Information	Information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module.	10
Stream Cipher	Symmetric encryption algorithm with the property that the encryption process involves combining the plaintext with a pseudorandom enciphering sequence one bit at a time. Each ciphertext bit is thus a function of both the corresponding plaintext bit and its position within the sequence of plaintext bits. [ISO/IEC WD 18033-1 (12/2001)]	42
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms. [ISO/IEC 15408-1: 1999]	42

Term	Definition	Source
Strong Password	A password that provides an effective defense against unauthorized access to a resource. A strong password is at least six characters long, does not contain all or part of the user's account name, and contains at least three of the four following categories of characters: uppercase letters, lowercase letters, base 10 digits, and symbols found on the keyboard, such as !, @, and #.	43
Strong Secret	Secret with a sufficient degree of entropy that conducting an exhaustive search for the secret is infeasible, even given knowledge that would enable a correct guess for the secret to be distinguished from an incorrect guess NOTE -- This might, for example, be achieved by randomly choosing the secret from a sufficiently large set of possible values with an even probability distribution. [ISO/IEC FDIS 11770-4: 2006-01-09]	41
Subject	An entity within the TSC that causes operations to be performed. [ISO/IEC 15408-1: 1999]	42
Substation or Station	The term, including its qualifier, is used to generically address all remote sites housing devices that control transmission and distribution of gas, electricity, water, wastewater, etc. Examples are electric power substations, pumping stations, compressor stations, and gate stations.	10
Substation Secure Area	The area contained within the first or outer substation physical security perimeter.	36
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.	15
Subsystem	A portion of a larger system consisting of several components or process units which, together, have the characteristics of a system by themselves.	33
Superuser Do	A utility for Unix based systems that provides an efficient way to give specific users permission to use specific system commands at the root (most powerful) level of the system. SUDO also logs all commands and arguments.	13
Supervisory Control	A term used to imply that a controller output or computer program output is used as an input to other controllers, e.g., generation of setpoints in cascaded control systems. Used to distinguish from direct digital control.	33
Supervisory Control and Data Acquisition	A computer control system used in real time to monitor and control one or more remote facilities. The system collects	32

Term	Definition	Source
(SCADA)	data and/or sends control instructions, either automatically or by operators at other locations. SCADA is used to control facilities in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation.	
Supervisory Control and Data Acquisition (SCADA)	A system of remote control and telemetry used to monitor and control the transmission system.	34
Supervisory Control and Data Acquisition (SCADA) system	A system operating with coded signals over communication channels so as to provide control of remote equipment (using typically one communication channel per remote station). The supervisory system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions.	10
Supplemental Regulation Service	A method of providing regulation service in which the Balancing Authority providing the regulation service receives a signal representing all or a portion of the other Balancing Authority's ACE.	34
Supplementary Character; Supplementary Check Character	Check character which does not belong to the character set of the strings which are to be protected. [ISO/IEC FCD 7064 (09/2000)]	42
Supply Chain	Companies directly involved in the production of goods, from raw materials through intermediate products and final use. The supply chain extends beyond the chemicals sector and includes raw material producers and manufacturers of products including chemicals. The supply chain typically includes transportation, distribution, and utility companies, but does not include producers of chemical equipment or providers of administrative services.	32
Surge	A transient variation of current, voltage, or power flow in an electric circuit or across an electric system.	34
Symmetric Communications	In telecommunications, the term symmetric (also symmetrical) refers to any system in which data speed or quantity is the same in both directions, averaged over time. [WhatIs]	41
Symmetric Cryptographic Technique	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-1: 1996]	42

Term	Definition	Source
	Cryptographic technique that uses the same secret key for both the encryption and the decryption transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation. [ISO/IEC WD 18033-1 (12/2001)]	
Symmetric Cryptography	Cryptographic technique that uses the same secret key for both the encryption and the decryption transformations. [ISO/IEC 19790: 2006-03-01]	41
Symmetric Encipherment Algorith	An encipherment algorithm that uses the same secret key for both the originator's and the recipient's transformation. [ISO/IEC 9798-1: 1997]	42
Symmetric Encryption Algorithm	Encryption algorithm that uses the same secret key for both the encryption and decryption processes. NOTE – A symmetric encryption algorithm is a symmetric cryptographic technique that is also an encryption algorithm. [ISO/IEC WD 18033-1 (12/2001)]	42
Symmetric Key	A single parameter is used to both encrypt and decrypt a message or object. [RFC2828]	10, 41
Symmetric Key Algorithm	See Secret Key Cryptographic Algorithm [RFC2828]	41
Synchronized sequence numbers (SYN)	Synchronized control flag in TCP header used to indicate the start of the process to establish a TCP connection; also refers to the message containing the set control flag. [5]	10
System	1. An assembly of procedures, processes, methods, routines, or techniques united by some form of regulated interaction to form an organized whole. 2. The complex or hardware and software utilized to affect the control of a process. 3. An assemblage of equipment, machines, control devices, or a combination thereof, interconnected mechanically, hydraulically, pneumatically or electrically, and intended to act together to perform a predetermined function. 4. In data processing, any group of software and hardware that is connected to operate as a unit.	33
System	See Information System.	14, 15
System	A combination of generation, transmission, and distribution components.	34
System	A specific IT installation, with a particular purpose and operational environment. [ISO/IEC 15408-1: 1999, ISO/IEC WD 15443-1 (11/2001)]	42
System Life Cycle	The evolution with time of the system from conception	42

Term	Definition	Source
	through to disposal. [ISO/IEC WD 15443-1 (11/2001)]	
System Operating Limit	The value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to: • Facility Ratings (Applicable pre- and post-Contingency equipment or facility ratings) • Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits) • Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) • System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits)	34
System Operator	An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.	34
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.	14, 15, 26
System Software	The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data. [FIPS 140-2]	1, 10, 41
System-Specific Security Control	A security control for an information system that has not been designated as a common security control.	15
Tamper	To maliciously modify data.	43
Tamper Detection	Automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module. [ISO/IEC 19790: 2006-03-01]	41
Tampering	1. In INFOSEC, penetration or modification of internal operations, or the insertion of active or passive tapping mechanisms, to determine the nature of, or monitor or record, e.g., secret data. [After X9.24] 2. Unauthorized modification altering the proper functioning of INFOSEC equipment. [INFOSEC-99] 3. Unauthorized modification of	41

Term	Definition	Source
	sensitive systems or sensitive information. [ATIS]	
Target of Evaluation	An IT product ro system and its associated administrator and user guidance documentation that is the subject of an evaluation. [ISO/IEC 15408-1: 1999]	42
TASE.2	Telecontrol Application Service Element, number 2, formally IEC 60870-6 and informally ICCP. [IEC 60870-6]	41
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.	14, 15
Technical Evaluation	An investigation to determine the suitability of materials, equipment or systems to perform a specific function.	33
Technical Specifications	A detailed description of the technical characteristics of an item or system in sufficient detail to form the basis for design, development, production and, in some cases, operation.	33
Telemetering	The process by which measurable electrical quantities from substations and generating stations are instantaneously transmitted to the control center, and by which operating commands from the control center are transmitted to the substations and generating stations.	34
Thermal Rating	The maximum amount of electrical current that a transmission line or electrical facility can conduct over a specified time period before it sustains permanent damage by overheating or before it sags to the point that it violates public safety requirements.	34
Third Party	Refers to vendors, support personnel, other companies.	13
Third-party Seal	An online seal of approval certifying that a Web site's privacy statement has been examined and tested by an organization such as BBBOnLine or TRUSTe, in accordance with the Fair Information Practices.	43
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.	10, 11
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-	12*, 14

Term	Definition	Source
	source to successfully exploit a particular information system vulnerability.	
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	15
Threat	The possibility of injury, damage, destruction, or diversion of an asset or other hostile action towards an asset.	32
Threat	1. Capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others. [ISO/IEC 1st WD 21827: 2006-02-07] 2. Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability. [NIST]	41
Threat	A potential cause of an unwanted incident that may result in harm to a system or organization. [ISO/IEC PDTR 13335-1 (11/2001)] A potential cause of an unwanted incident that may result in harm to an IT system. [ISO/IEC DTR 15947 (10/2001)] A potential cause of an unwanted incident which may result in harm to a system or organization. [ISO/IEC 17799: 2000]	42
Threat Agent/Source	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.	15
Threat Assessment	Formal description and evaluation of threat to an information system.	15
Threat Scenario	A specific event or sequence of events that has an undesirable consequence resulting from the realization of a threat. It is the security equivalent of a hazard scenario.	32
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.	14
Throttling	A method of preventing a denial of service attack by limiting the number of requests that can be made to a system. Also called *pooling*.	43

Term	Definition	Source
Throughput	The total capability of equipment to process or transmit data during a specified time period.	10
Throughput	The net rate at which data can be received by a device, manipulated as specified, and output to some other specified device.	33
Throughput	The maximum continuous traffic rate that a device can handle without dropping a single packet. [ATIS]	41
Throughput Rate	See Throughput.	33
Tie Line	A circuit connecting two Balancing Authority Areas.	34
Tie Line Bias	A mode of Automatic Generation Control that allows the Balancing Authority to 1.) maintain its Interchange Schedule and 2.) respond to Interconnection frequency error.	34
Time Error	The difference between the Interconnection time measured at the Balancing Authority(ies) and the time specified by the National Institute of Standards and Technology. Time error is caused by the accumulation of Frequency Error over a given period.	34
Time Error Correction	An offset to the Interconnection's scheduled frequency to return the Interconnection's Time Error to a predetermined value.	34
Time Stamp	A time variant parameter which denotes a point in time with respect to a common time reference. [ISO/IEC 11770-1; 1996] A time variant parameter which denotes a point in time with respect to a common reference. [ISO/IEC 9798-1: 1997] A data item which denotes a point in time with respect to a common time reference. [ISO/IEC 11770-3: 1999] A data item which denotes a point in time with respect to a common reference. [ISO/IEC FDIS 15946-3 (02/2001)]	42
Time-stamp Requester	An entity which possesses data it wants to be time-stamped. NOTE – A requester may also be a Trusted Third Party including a time-stamping authority. [ISO/IEC FDIS 18014-1 (02/2002)]	42
Time-stamp Token	A data structure containing a verifiable cryptographic binding between a data items' representation and a time-value. A time-stamp token may also include additional data items in the binding. [ISO/IEC FDIS 18014-1 (02/2002)]	42

Term	Definition	Source
Time-stamp Verifier	An entity which possesses data and wants to erify that it has a valid time-stamp bound to it. The verification process may be performed by the verified itself or by a Trusted Third Party. [ISO/IEC FDIS 18014-1 (02/2002)]	42
Time-stamping Authority	A trusted third party trusted to provide evidence which includes the time when the secure time stamp is generated. [ISO/IEC 11770-3: 1999]	42
Time-stamping Authority (TSA)	A trusted third party trusted to provide a time stamping service. [ISO/IEC FDIS 18014-1 (02/2002)]	42
Time-stamping Service	A service providing evidence that a data item existed before a certain point in time. NOTE – An example is given by adding a time stamp to a data items representation and signing the result. [ISO/IEC FDIS 18014-1 (02/2002)] A service which attests the existence of electronic data at a precise instant of time. NOTE – Time stamping services are useful and probably indispensable to support long term validation of signatures. They will be defined in a separate document. [ISO/IEC 15945: 2002]	42
Time Variant Parameter	A data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp. [ISO/IEC 9798-1: 1997, ISO/IEC 11770-2: 1996, ISO/IEC 11770-3: 1999] A data item used by an entity to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp. [ISO/IEC 11770-1: 1996]	42
TLR Log	Report required to be filed after every TLR Level 2 or higher in a specified format. The NERC IDC prepares the report for review by the issuing Reliability Coordinator. After approval by the issuing Reliability Coordinator, the report is electronically filed in a public area of the NERC web site.	34
TLS	Transport Level Security. TLS is equivalent to SSL v3. TLS provides endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated; mutual authentication requires public key infrastructure (or PKI) deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. [WIKI]	41
TLS	See Transport Layer Security.	43

Term	Definition	Source
TOE Resource	Anything useable or consumable in the TOE. [ISO/IEC 15408-1: 1999]	42
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP. [ISO/IEC 15408-1: 1999]	42
TOE Security Functions Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF. [ISO/IEC 15408-1: 1999]	42
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.[ISO/IEC 15408-1: 1999]	42
TOE Security Policy Model	A structured representation of the security policy to be enforced by the TOE. [ISO/IEC 15408-1: 1999]	42
Token	A message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique. [ISO/IEC 9798-1; 1997]	42
Token	See access token.	43
Total Transfer Capability (TTC)	The amount of electric power that can be moved or transferred reliably from one area to another area of the interconnected transmission systems by way of all transmission lines (or paths) between those areas under specified system conditions.	34
Traffic Analysis	Listening to messages, and without understanding their content, inferring information from the fact that certain messages are always sent when certain real-life events happen (e.g., closing a breaker).	3, 10
Traffic Analysis	1. In a communications system, the analysis of traffic rates, volumes, densities, capacities, and patterns specifically for system performance improvement. [From Weik '89] 2. [The] study of communications characteristics external to the text. [NIS] 3. The analysis of the communications-electronic environment for use in the design, development, and operation of new communications systems. [From Weik '89] 4. In cryptology, the inference of information from observation and analysis of the presence, absence, amount, direction, and frequency of the traffic flow. [After 2382-pt. 8] 5. [The] Study of communications patterns. [INFOSEC-99] [ATIS]	41

Term	Definition	Source
Trailer	String of bits of length one or two octets, concatenated to the end of the recoverable part of the message during message representative production. [ISO/IEC FDIS 9796-2 (12/2001)]	42
Transaction	See Interchange Transaction.	34
Transcription Gateway	A virtual, software-based translation mechanism on the PC that converts one content protection scheme or format to another, while retaining the license and rights in the license from the original content protection format.	43
Transfer Capability	The measure of the ability of interconnected electric systems to move or transfer power *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is *not* generally equal to the transfer capability from "Area B" to "Area A."	34
Transfer Distribution Factor	See Distribution Factor.	34
Transfers Outside TSF Control	Communicating data to entities not under control of the TSF. [ISO/IEC 15408-1: 1999]	42
Transmission	An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.	34
Transmission Constraint	A limitation on one or more transmission elements that may be reached during normal or contingency system operations.	34
Transmission Control Protocol	TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two host to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.	13
Transmission Customer	1. Any eligible customer (or its designated agent) that can or does execute a transmission service agreement or can or does receive transmission service. 2. Any of the following responsible entities: Generator Owner, Load-Serving Entity, or Purchase-Selling Entity.	34
Transmission	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the	34

Term	Definition	Source
Operator	operations of the transmission facilities.	
Transmission Owner	The entity that owns and maintains transmission facilities.	34
Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.	34
Transmission Service	Services provided to the Transmission Customer by the Transmission Service Provider to move energy from a Point of Receipt to a Point of Delivery.	34
Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.	34
Transmission Reliability Margin (TRM)	The amount of transmission transfer capability necessary to provide reasonable assurance that the interconnected transmission network will be secure. TRM accounts for the inherent uncertainty in system conditions and the need for operating flexibility to ensure reliable system operation as system conditions change.	34
Transparency	A standard that requires that the structure for processing personal information be in a fashion that is open and understandable to the individual whose data is being processed. It is a goal of the Fair Information Practices, which requires a company to inform users what personal information the company collects and how the data is used.	43
Transport Layer Security (TLS)	A protocol that provides communications privacy and security between two applications communicating over a network. TLS provides a secure channel by encrypting communications and enables clients to authenticate servers or, optionally, servers to authenticate clients.	43
Trapdoor	A hidden software or hardware mechanism, usually created for testing and troubleshooting, that may be used to circumvent computer security. [2382-pt.8] [ATIS]	41
Trivial File Transfer Protocol	A simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.	13
Trojan Horse	1. An apparently harmless program containing malicious logic that allows the unauthorized collection, falsification, or destruction of data. [2382-pt.8] 2. [A] program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. [INFOSEC-99]	41

Term	Definition	Source
Trojan Horse	A program that appears to be useful or harmless but that contains hidden code designed to exploit or damage the system on which it is run. Trojan horse programs are most commonly delivered to users through e-mail messages that misrepresent the program's purpose and function. Also called Trojan code.	43
Trust	In cryptology and cryptosystems, that characteristic allowing one entity to assume that a second entity will behave exactly as the first entity expects. Note: Trust may apply only for some specific function. The critical role of trust in the authentication framework is to describe the relationship between an authenticating entity and a certification authority; an authenticating entity must be certain that it can trust the certification authority to create only valid and reliable certificates. [After X.509].	41
TRUSTe	An organization offering an online privacy seal program that certifies eligible Web sites and holds Web sites to a baseline privacy standard. This key privacy watchdog organization plays an important enforcement role in the dispute and resolution of privacy issues.	43
Trusted Channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP. [ISO/IEC 15408-1: 1999]	42
Trusted Path	A communication link that has been certified to a specific level of security or risk avoidance.	10
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by software that is not trusted.	15
Trusted Path	A means by which a user and a TSF can communicate with necessary confidence to suppot the TSP. [ISO/IEC 15408-1: 1999]	42
Trusted Third Party	A security authority, or its agent, trusted by other entities with respect to security related activities. [ISO/IEC 11770-3: 1999, ISO/IEC WD 13888-1 (11/2001), ISO/IEC 14888-2: 1999] A security authority or its agent, trusted by other entities with respect to security-related activities. In the context of ISO/IEC 9798, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication. [ISO/IEC 9798-1: 1997]	42

Term	Definition	Source
Trusted Time Stamp	A data item with time and date information assured by a trusted time stamping authority. [ISO/IEC WD 13888-1 (11/2001)]	42
Trusted Time Stamping Authority	A trusted third party trusted to provide evidence which includes the time when the trusted time stamp is generated. [ISO/IEC WD 13888-1 (11/2001)]	42
TSF Data	Data created by and for the TOE, that might affect the operation of the TOE. [ISO/IEC 15408-1: 1999]	42
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP. [ISO/IEC 15408-1: 1999]	42
Unauthorized Disclosure	An event involving the exposure of information to entities not authorized access to the information.	10
Unilateral Authentication	Entity authentication which provides one entity with assurance of the other's identity but not vice versa. [ISO/IEC 9798-1: 1997]	42
Update	A broadly released fix for a specific problem addressing a noncritical, non-security-related bug.	43
Update	To make a system or data file more current.	43
Update Key	Every key pair needs to be updated regularly (i.e., replaced with a new key pair), and a new certificate needs to be issued. … When a key pair is due to expire the relevant end entity MAY request a key update - that is, it MAY request that the CA issue a new certificate for a new key pair. The request is made using a key update request (kur) message. [IETF RFC2510]	41
Update Rollup	A tested, cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or component of a product, such as Microsoft Internet Information Services (IIS).	43
Upgrade	A software package that replaces an installed version with a newer version of the same software. The upgrade process typically leaves existing customer data and preferences intact while replacing the existing software with the newer version.	43
Upgrade	To change to a newer, usually more powerful or sophisticated version.	43
User	An individual or process acting on behalf of the individual	1, 10

Term	Definition	Source
	that accesses a cryptographic module in order to obtain cryptographic services.	
User	Individual or (system) process authorized to access an information system.	14, 15, 12
User	In data processing, the person or client who makes use of a computer system.	33
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. [ISO/IEC 15408-1: 1999]	42
User Data	Data created by and for the user, that does not affect the operation of the TSF. [ISO/IEC 15408-1: 1999]	42
User Profile	Settings that define customization preferences for a particular user, such as desktop settings, persistent network connections, personally identifiable information, Web site use, or other behaviors and demographics data.	43
User Rights	Tasks that a user is permitted to perform on a Windows-based computer or domain. There are two types of user rights: privileges and logon rights. An example of a privilege is the right to shut down the system. An example of a logon right is the right to log on to a computer interacitively. Both types are assigned by administrators to individual users or groups as part of the security settings for the computer.	43
User Token	A hardware or software object consisting of an identity and, optionally, a set of associated privileges.	10
Utilities:	The supply of Electric Power, Water, Natural Gas, and telecommunications to a control facility	13
Utility	A generic term that, when qualified, identifies the business entity including all its operating and business functions; e.g., electric utility, gas utility, water utility, wastewater utility, pipeline utility.	10
Utility	1. Any general-purpose computer program included in an operating system to perform common functions. 2. Any of the systems in a process plant, manufacturing facility not directly involved in production; may include any or all of the following – steam, water, refrigeration, heating, compressed air, electric power, instrumentation, waste treatment and effluent systems.	33
Value Chain	All those involved in the production and distribution of chemical products, including the supply chain, chemical equipment producers and administrative services (such as banks and insurance companies) through end-use	32

Term	Definition	Source
	consumers.	
Verification Function	A function in the verification process which is determined by the verification key and which gives a recomputed value of the witness as output. [ISO/IEC 9796-3; 2000, ISO/IEC 14888-1: 1998]	42
Verification Key	A value required to verify a cryptographic check value. [ISO/IEC WD 13888-1 (11/2001)] A data item which is mathematically related to an entity's signature key and which is used by the verifier in the verification process. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001), ISO/IEC WD 15946-4 (10/2001)]	42
Verification Process	A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid. [ISO/IEC 9796-3: 2000, ISO/IEC 14888-1: 1998, ISO/IEC FDIS 15946-2 (04/2001)] A process, which takes as input the signed message, the verification key and the domain parameters, and which gives as its output the recovered message if valid. [ISO/IEC CD 15946-4 (12/2000)]	42
Verifier	An entity that verifies evidence. [ISO/IEC WD 13888-1 (11/2001)] An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges. [ISO/IEC 9798-1: 1997]	42
Virtual Private Network	A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.	13
Virtual Private Network (VPN)	1. Restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunneling links of the virtual network across the real network. [ISO/IEC FDIS 18028-1: 2006-03-31] 2. A protected information-system (IS) link utilizing tunnelling, security controls (*see* information assurance), and end-point address translation giving the user the impression	41

Term	Definition	Source
	a dedicated line exists between nodes. [INFOSEC-99]	
Virtual Private Network (VPN)	The extension of a private network that encompasses encapsulted, encrypted, and authenticated links across shared or public networks. VPN connections typically provide remote access and router-to-router connections to private networks over the Internet.	43
Virus	1. An unwanted program which places itself into other programs, which are shared among computer systems, and replicates itself. Note: A virus is usually manifested by a destructive or disruptive effect on the executable program that it affects. 2. Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. [INFOSEC-99] [ATIS}	41
Virus	Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. Compare worm. See also the definition provided by the Virus Info Alliance (f-secure.com).	43
VPN	See virtual private network.	43
Vulnerability	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.	10
Vulnerability	Weakness in and information system. System security procedures, internal controls or implementation that could be exploited.	12
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	14, 15
Vulnerability	1. A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy. [RFC2828] 2. A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely effect an organization's operations or assets through a loss of confidentiality, integrity, or availability. [NIST] 3. A weakness of an asset or group of assets that can be exploited by one or more threats [ISO/IEC 13335-1:2004]	41
Vulnerability	A weakness of an asset or group of assets which can be exploited by one or more threats. [ISO/IEC PDTR 13335-1 (11/2001)]	42

Term	Definition	Source
	A weakness that can be exploited by one or more threats. [ISO/IEC DTR 15947 (10/2001)] A weakness of an asset or group of assets which can be exploited by a threat. [ISO/IEC 17799: 2000]	
Vulnerability	Any weakness, administrative process or act, or physical exposure that makes a computer susceptible to exploit by a threat.	43
Vulnerability Analysis	The identification of the ways in which assailants may attack a facility to cause harm. It can include qualitative risk analysis.	32
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.	12, 15
Vulnerability Assessment	Vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. The system being studied could be a physical facility like a nuclear power plant, a computer system, or a larger system (for example the communications infrastructure or water infrastructure of a region). Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed according to the following steps: • Cataloguing assets and capabilities (resources) in a system • Assigning quantifiable value and importance to the resources • Identifying the vulnerabilities or potential threats to each resource • Mitigating or eliminating the most serious vulnerabilities for the most valuable resources When dealing with computers, vulnerability assessment is also known as "white hat hacking". [WIKI]	41
Weak Password	A password that does not provide an effective defense against unauthorized access to a resource. A weak password might be less than six characters long, contain all or part of a user's account name, or contain less than three of the four following categories of characters: uppercase letters, lowercase letters, base 10 digits, and symbols found on the keyboard, such as !, @, and #.	43
WEP	1. A cryptographic protocol offering stream cipher encryption with a key length of 128 bits; it is defined within the IEEE 802.11 Wireless LAN specifications. [ISO/IEC 18028-4: 2005-04-01] 2. Wired Equivalent Privacy (WEP) is a scheme to secure wireless networks (WiFi). Because a wireless network	41

Term	Definition	Source
	broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network, hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by WiFi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping. [WIKI]	
Wide Area	The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits.	34
Wide Area Network (WAN)	A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide. [ATIS]	41
Wide Area Networks	A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.	13
WiFi	A trademark provided by the WiFi Alliance promoting the use of wireless LAN equipment, based on IEEE 802.11 standards. [ISO/IEC 18028-4: 2005-04-01]	41
Windows Update	1. A Microsoft Web site maintained by the Windows product group for the purpose of providing updates for core Windows components. 2. An application in Windows that enables a user to download files from the Internet that are necessary to keep a computer up to date.	43
Wireless LAN - WLAN	A network using radio frequencies. The most common standards in use are IEEE 802.11b and 802.11g with up to 11 Mbps respectively 54 Mbps transfer rate utilising the 2,4 GHz frequency band. [ISO/IEC 18028-4: 2005-04-01]	41
Witness	Data item which provides evidence of the claimant's identity to the verifier. [ISO/IEC 9798-5: 1999] A data item which provides evidence to the verifier.	42

Term	Definition	Source
	NOTE - In the context of this part of ISO/IEC 9796 the witness is based on a hash-token. [ISO/IEC 9796-3: 2000] A data item which provides evidence to the verifier. [ISO/IEC 14888-1: 1998]	
Word	A string of 32 bits in dedicated hash-funcitons 1, 2, 3 and 4, or a string of 64 bits in dedicated hash-functions 5 and 6. [ISO/IEC CD 10118-3 (11/2001)] String of 32 bits. [ISO/IEC FDIS 9797-2 (09/2000)]	42
Work Product	All items (i.e. documents, reports, files, data, etc.) generated in the course of performing any process for developing and supplying the deliverable. [ISO/IEC WD 15443-1 (11/2001)]	42
Worm	1. A computer virus capable of disrupting a computer program. [After Weik '96] 2. A self-contained program that can propagate itself through systems or networks. Note: Worms are often designed to use up available resources such as storage or processing time. [ANSDIT] 3. [An] independent program that replicates from machine to machine across network connections, often clogging networks and computer systems as it spreads. [INFOSEC-99]	41
Worm	Self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial of service attack. Compare virus.	43
WPA, WPA2	WiFi Protected Access (WPA and WPA2) are systems to secure wireless (WiFi) networks. They were created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues: • Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions. In the "Personal" mode, the most likely choice for homes and small offices, a passphrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ. [WIKI]	41

Term	Definition	Source
X.400	The International Telecommunication Union standard that defines message access tokens.	43
X.509	X.509 is an ITU-T standard for public key infrastructure (PKI). X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm. [WIKI]	41
Zero a Device	See Zeroization.	33
Zeroization	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of data.	1, 10
Zeroization	To erase all the data stored on a volume and reinitialize the format of the volume.	33

Definition of Acronyms

Acronym	Definition	Source
3DES	Triple Data Encryption Standard	1, 10
AA	Attribute Authority	42
A/D	Analog/Digital (used in the context of analog to digital conversion)	10
ACC	American Chemistry Council	32
ACE	Area Control Error	34
ACE	Access Control Entry	43
ACL	Access Control List	41, 43
ACSI	Abstract Communication Service Interface	41
AEP	Awareness Education Plan	10
AES	Advanced Encryption Standard specified in FIPS PUB 197	10, 41
AGA	American Gas Association	10, 41
AGC	Automatic Generation Control	34
AIS	Automated Information System	11
ANSI	American National Standards Institute	11
API	American Petroleum Institute	32
API	Application Program Interface	1, 10
ATC	Available Transfer Capability	34
AV	Antivirus Software	43
BA	Balancing Authority	34
BBBOnLine	A privacy seal program established by the Better Business Bureau which certifies that certain Web sites conform to baseline privacy standards. Microsoft is a sponsor of BBBOnLine.	43
BCP	Business Continuity Plan	10
BSP	Business Continuity Plan	10

Acronym	Definition	Source
CA	Certification Authority	41, 42
CAPI	Common Application Programming Interface	10
CBC	Cipher Block Chaining	4, 6, 10
CBM	Capacity Benefit Margin	34
CCPS	Center for Chemical Process Safety	32
CFR	Code of Federal Regulations	15
CIDX	Chemical Industry Data Exchange	32
CIO	Chief Information Officer	14, 15
CM	Cryptographic Module	1, 10
CMVP	Cryptographic Module Validation Program	1, 10
CNSS	Committee for National Security Systems	14, 15
COPPA	Children's Online Privacy Protection Act	43
COTS	Commercial-off-the Shelf	11, 15
CPS	Control Performance Standard	34
CPU	Computer Processing Unit	10
CRC	Cyclic Redundancy Check	10, 41
CRL	Certificate Revocation List	10
CRM	Cryptographic Reference Model	10
CSP	Critical Security Parameter	1, 10
CSTP	Cryptographic System Test Plan	10
CTR	Counter (as used in the block cipher function)	4, 10
DAA	Designated Approving Authority	41
DCID	Director of Central Intelligence Directive	15
DCLM	Direct Control Load Management	34
DCS	Digital Control System	32

Acronym	Definition	Source
DCS	Distributed Control System	10, 11, 41
DCS	Disturbance Control Standard	34
DDoS	Distributed Denial of Service	10, 43
DES	Data Encryption Standard	1, 10, 41
DF	Distribution Factor	34
DiD	Defense-in-Depth	10
DMZ	Demilitarized Zone	11
DNP	Distributed Network Protocol	10
DO	Data Object	41
DoC/NIST	U.S. Department of Commerce/National Institute of Standards and Technology	10
DOE	U.S. Department of Energy	10
DoS	Denial of Service	10, 41
DoS	Denial of Service Attack	43
DRM	Digital Rights Management	43
DSM	Demand-Side Management	34
DSS	Digital Signature Standard	41
DUT	Device Under Test	10
EAL	Evaluation Assurance Level	42
ECB	Electronic Codebook	4, 6, 10
ECDSA	Elliptic Curve Digital Signature Algorithm	10
EEPROM	Electronically-Erasable Programmable Read-Only Memory	1, 10
EFS	Encrypting File System	43
EH&S	Environment, Health, & Safety	32
EM/RF	Electromagnetic and radio frequency	41
EMC	Electromagnetic Compatibility	10

Acronym	Definition	Source
EMI	Electromagnetic Interference	10
EMS	Energy Management System	10
EPROM	Erasable Programmable Read-Only Memory	1, 10
ERP	Enterprise Resource Planning	11
FB	Feedback Buffer	42
FCC	Federal Communications Commission	1, 10
FEA	Federal Enterprise Architecture	15
FEP	Front End Processor	10
FIPS	Federal Information Processing Standard	1,10,14,15
FIPS PUB	FIPS Publication	1, 10
FISMA	Federal Information Security Management Act	14, 15
FLASH	Flash memory	10
FTP	File Transfer Protocol	13
GLB	Gramm-Leach-Bliley Act	43
GLDF	Generator-to-Load Distribution Factor	34
GOTS	Government Off-The-Shelf	15
GSF	Generator Shift Factor	34
GUI	Graphical User Interface	10
(GUID)	Globally Unique Identifier	43
HAZOP	Hazardous Operations	10
HAZOP	Hazard and Operability	32
HFNETCHK	A command-line tool that enables and administrator to check the update status of all Windows NT 4.0, Windows 2000, and Windows XP computers on a network from a central location.	43
HIPAA	Health Insurance Portability and Accountability Act	43
HMAC	Keyed-Hashed Message Authentication Code	9, 10

Acronym	Definition	Source
HMI	Human Machine Interface	13
HSM	Hardware Security Module	10
HTTP	HyperText Transfer Protocol	10
I&A	Identification and Authentication	10
IAM	INFOSEC Assessment Methodology	32
IBM	International Business Machines	32
IC	Integrated Circuit	10
ICCP	Intercontrol centre communications protocol	41
ICMP	Internet Control Message Protocol	13
ICRA	Internet Content Rating Association	43
IDC	Interchange Distribution Calculator	34
IDS	Intrusion Detection System	10, 13, 41, 42
IEC	International Electro-technical Committee	10
IED	Intelligent Electronic Device	2, 10, 41
IEEE	Institute of Electrical and Electronics Engineers	15
IEEE	Institute of Electrical and Electronics Engineers, Inc.	10
IETF	Internet Engineering Task Force	41
IPP	Independent Power Producer	34
IROL	Interconnection Reliability Operating Limit	34
IRT	Incident Response Team	10
InfoSec	Information Security (as used in the context of a InfoSec team)	10
IP	Internet Protocol	10, 15
IPS	Intrusion Protection System	13
IPv6	Internet Protocol Version 6	15
ISA	The Instrumentation, Systems, and Automation Society	41

Acronym	Definition	Source
ISA-TR	Instrumentation, Systems, and Automation Society Technical Report	10
ISO	International Standards Organization	10, 41
IT	Information Technology	10, 32
IV	Initialization Vector	1, 10
KAT	Known Answer Test	10
KB Article	A technical document in the Microsoft Knowledge Base accessible through Microsoft.com.	43
key	Cryptographic key	10
key component	Cryptographic key component	10
KTC	Key Translation Centre	42
L2TP	Layer Two (2) Tunneling Protocol	13
LAN	Local Area Network	10, 13, 32, 41
LSF	Load Shift Factor	34
MAC	Message Authentication Code	10, 42, 43
MAC	Media Access Control	15
MAS	Multiple Address System	10
MCM	Maintenance Cryptographic Module	10
MCT	Monte Carlo Tests	10
MES	Manufacturing Execution System	11
MIB	Management Information Base	41
MMI	Man Machine Interface	13
MMS	Manufacturing Message Specification	41
MOA	Memorandum of Agreement	15
MOU	Memorandum of Understanding	15
MPH	Messages Per Hour	10

Acronym	Definition	Source
NERC	North American Electric Reliability Council	10, 41
NIST	National Institute of Standards and Technology	1,10,14,15,32
NIST SP	National Institute of Standards and Technology Special Publication	10
NRD Token	Non-repudiation of delivery token	42
NRO Token	Non-repudiation of origin	42
NRS Token	Non-repudiation of submission	42
NRT Token	Non-repudiation of transport token	42
NSA	National Security Agency	10, 15, 32
OASIS	Open Access Same Time Information Service	34
OATT	Open Access Transmission Tariff	34
OCSP	Online Certificate Status Provider	10
OFB	Output Feedback (as used in the block cipher function)	10
OMB	Office of Management and Budget	14, 15
OSI-RM	Open Standards Interconnection – Reference Model	41
OWS	Operator Work Station	
P3P	Platform for Privacy Preferences Project	43
PAA	Preliminary Action Audit	10
PCI	Peripheral Component Interconnect	10
PCMCIA	Personal Computer Memory Card International Association	10
PCN	Process Control Network	32
PGP	Pretty Good Privacy	41
PHA	Process Hazard Analysis	32
PICS	Protocol Implementation Conformance Statements	41
PII	Personally Identifiable Information	43
PIMS	Process Information Management System	11

Acronym	Definition	Source
PIN	Personal Identification Number	10, 41, 43
PIXIT	Protocol Implementation eXtra Information for Testing	41
PKCS	Public-Key Cryptography Standards	10
PKI	Public Key Infrastructure	10, 41, 42, 43
PLC	Programmable Logic Controller	32, 33
POD	Point of Delivery	34
PoP	Proof-of-Possession	10
POR	Point of Receipt	34
PPP	Point to Point Protocol	10, 41
PPTP	Point-to-Point Tunneling Protocol	13
PRNG	Pseudorandom Number Generator	41
PROM	Programmable Read-Only Memory	1, 10
PSE	Personal Security Environment	42
PSTN	Public Switched Telephone Network	10
PT	Pre-transmission (as used in communication channels)	10
PTA	Penetration Test Assessment	10
PTP	Point to Point Transmission Service	34
PUB	Publication	10
QFE	Quick Fix Engineering	43
QoS	Quality of Service	43
RA	Registration Authority	42
RAS	Remedial Action Scheme	34
RBAC	Role-Based Access Control	10
RCIS	Reliability Coordinator Information System	34
RF	radiofrequency	10

Acronym	Definition	Source
RFC	Requests for Comments	10
RFC	Request for Collaboration	43
ROM	Read-Only Memory	1, 10
ROSI	Return on Security Investment	32
RPC	Remote Procedure Call	43
RSA	Rivest, Shamir, and Adleman (a public key algorithm)	10, 41
RST	Reset flag, TCP header	10
RTU	Remote Terminal Unit	2, 10
SAA	Security Architecture Analysis	10
SCA	Successive Compromise Analysis	10
SCADA	Supervisory Control and Data Acquisition	32, 34, 41, 42
SCADA	Supervisory Control And Data Acquisition System	2, 10, 13
SCM	SCADA Cryptographic Module	10
SCSI	Small Computer System Interface	10
SENV	Secure Envelope	42
SF	Security Function	42
SFP	Security Function Policy	42
SHA	Secure Hash Algorithm	10, 41
SHS	Secure Hash Standard	10
SID	Security Identifier	43
SNMP	Simple Network Management Protocol	13
SOF	Strength of Function	42
SP	Service Pack	43
SSH	Secure Shell	13, 41
SSL	Secure Socket Layer	10, 41

Acronym	Definition	Source
SSL	Secure Sockets Layer	43
SUDO	Superuser do	13
SUT	System Under Test	10
SV	Starting Variable	42
SVA	Security Vulnerability Assessment	32
SYN	Synchronized sequence numbers. Synchronized control flag in TCP header used to indicate the start of the process to establish a TCP connection; also refers to the message containing the set control flag.	5
SYN	Synchronized sequence numbers	10
TASE.2	Telecontrol Application Service Element, number 2	41
TCP	Transmission Control Protocol	13, 15
TFTP	Trivial File Transfer Protocol	13
TLA	Three Layer Analysis	10
TLS	Transport Level Security	41
TLS	Transport Layer Security	43
TTC	Total Transfer Capability	34
TRM	Transmission Reliability Margin	34
TRUSTe	An organization offering an online privacy seal program that certifies eligible Web sites and holds Web sites to a baseline privacy standard. This key privacy watchdog organization plays an important enforcement role in the dispute and resolution of privacy issues.	43
TSA	Time-stamping Authority	42
TSC	TSF Scope of Control	42
TSF	TOE Security Functions Interface	42
TSP	TOE Security Policy	42
URL	Uniform Resource Locator	1, 10
USB	Universal Serial Bus	10
USC	United States Code	14, 15

Acronym	Definition	Source
VAM	Vulnerability Assessment Methodology	32
VOIP	Voice Over Internet Protocol	15
VPN	Virtual Private Network	10, 13, 15, 41, 43
WAN	Wide Area Network	32, 10, 41
WAN	Wide Area Networks	13
WEP	Wired Equivalent Privacy	10, 41
WLAN	Wireless LAN	41
WPA, WPA2	WiFi Protected Access	41
XOR	Exclusive OR Operation	10