NIST Augmented CIP Glossary

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

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.

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets.

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.

~~Electronic~~ Cyber Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected ~~and~~, for which access is controlled. Critical and non-critical Cyber Asset within a defined Cyber Security Perimeter shall protected pursuant to the requirements of the CIPs.

==========

[Discussion is not part of the recommendation. It is provided to assist the drafting committee.]

Information may be stored, transmitted, and processed using multiple ditital and analog media including electro-magnetic fields in space on on media in frequencies commonly described as electrical and optical. For example, fibre optic, infrared, and radio wireless communications are all common, but are not "electronic." NIST believes that "Electronic" is too limited a term and has replaced it with "Cyber" as being more inclusive.

The last sentence is added to incorporate CIP-005 requirement R1.4.

==========

Dial-up: Use of public or private switched telephone network to establish data communication between modems. Call establishment in the switched telephone network occurs prior to the data communication.

Industrial Control System (ICS): An information system (e.g., a discrete set of information resources) used to control industrial processes such as the bulk electric grid. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. All cyber assets within the Cyber Security Perimeter are part of the ICS.

=========Based on SP 800-53 glossary and 44 U.S.C., Sec. 3502==========

Multifactor Authentication: Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. Multifactor authentication is a system wherein more than one different factors are used to authenticate, thereby delivering a higher level of authentication assurance. Using more than one factor is sometimes called strong authentication. Human authentication factors are generally classified into three cases: (1) Something the user has (e.g., ID card, security token, software token, phone, or cell phone); (2) Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN)); and (3) Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier).

===Based on PC Magazine Encyclopedia http://www.pcmag.com/category2/0,2806,1846380,00.asp===

Physical Security Perimeter: The physical 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.

Remote Access: Any access to an Cyber Security Perimeter by a user (or a cyber asset) communicating through an external network not under the control of the Responsible Entity (e.g., the Internet, public switched telephone network).

==========Based on SP 800-53 glossary ==========

Routing of Data Communications Protocols:

Data communication protocols consist of a header, which contains addressing and other information, followed by user data. Data communication protocols can be Routable or Non-routable.

In Routable protocols, the header contains a network address as well as a device address. The network address allows message units (packets or frames) to be

forwarded from a device in one network to a device in another. Examples of routable protocols are TCP/IP, IPX, and DECnet.

In Non-routable protocols, the header contains only a device address and not a network address. They do not incorporate an addressing scheme for sending data from one network to another (i.e., the communicating devices must reside in the same network). Examples of non-routable protocols are NetBIOS and DEC's LAT protocols.

Security Plan: Formal document that provides an overview of the security requirements for the Cyber Security Perimeter and all cyber assets within the Cyber Security Perimeter, and describes the security controls in place or planned for meeting those requirements.

==========Based on SP 800-53 glossary ==========