



CYBERSECURITY GLOSSARY

By: Mary Fitzpatrick, Legislative Analyst II

ISSUE

This report is a table of acronyms and abbreviations related to cybersecurity in the utility sector. The table includes terms used in the Public Utility Regulatory Authority’s (PURA) recent [Cybersecurity Action Plan](#). It also includes links to relevant information. For a summary of the action plan, see [OLR Report 2016-R-0274](#).

Table 1: Cybersecurity Glossary

<i>Term or Acronym</i>	<i>Definition or Explanation</i>	<i>Relevant Links (if applicable)</i>
AWWA Process Control System Security Guidance	The American Water Works Association (AWWA) produced voluntary security guidance to provide water utility companies with a recommended course of action to reduce vulnerabilities to cyber-attacks. It is meant to represent the water sector’s approach to implementing the NIST framework (see below).	AWWA guidance
Bulk electric systems (BES)	BES are generation and transmission facilities and their control systems that are part of the North American interconnected power grid. They generally operate at 100 kilovolts or more.	
Breakers (i.e., circuit breakers)	In electric substations, circuit breakers act as safety switches to protect workers and equipment during an emergency by automatically stopping electric current flowing through a power line.	Explanation of substations
DHS	U.S. Department of Homeland Security	
DOE ES-C2M2	The U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2) is generally a self-evaluation tool that organizations can use to compare their cybersecurity program to industry best practices. The C2M2 for the electricity subsector is ES-C2M2.	ES-C2M2



Table 1 (continued)

Term or Acronym	Definition or Explanation	Relevant Links (if applicable)
Electric reliability organization (ERO)	Currently, NERC (see below) serves as the ERO. The 2005 federal Energy Policy Act (P.L. 109-58) gave FERC the power to certify an organization to act as ERO and to approve mandatory cybersecurity standards the ERO proposes and enforces.	16 U.S.C. 824o
FCC	Federal Communications Commission	
FCC CSRIC IV WG4 Final Report	FCC's Communications Security, Reliability and Interoperability Council (CSRIC IV) published a report known as the Working Group 4 (WG-4) Final Report that assessed and prioritized the NIST framework (see below) for the communications industry.	WG-4 Final Report
FERC	Federal Energy Regulatory Commission	
GridEx	A North American-wide, biennial physical security and cybersecurity exercise sponsored by NERC that tests the electricity sector's response to simulated cybersecurity and physical security incidents	GridEx III Report
Industrial Control System (ICS)	An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic) that act together to achieve an industrial objective (e.g., transport energy). ICS is a general term that encompasses several types of control systems, including SCADA (see entry below).	NIST Guide to ICS Security
Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT)	Unit within DHS' National Cybersecurity and Integration Center that assists control systems vendors and asset owners and operators to identify security vulnerabilities and develop sound mitigation strategies	About ICS-CERT ICS-CERT Alert on Ukraine Cyber Attack
Information technology (IT)	In the ES-C2M2, IT is a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or deposition of information, including interconnected or dependent business systems and their operating environment.	ES-C2M2
Intentional electromagnetic interference device (IEMI)	Devices that intentionally generate electromagnetic energy to introduce noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for malicious purposes	

Table 1 (continued)

Term or Acronym	Definition or Explanation	Relevant Links (if applicable)
Malware	Malware is malicious code or software, including viruses, spyware, and other unwanted software that is installed onto a computer or other equipment without the user's consent. Malware can be used to steal information including users' credentials or cause programs to crash or act erratically.	
MIL	The ES-C2M2 (see entry above) includes Maturity Indicator Levels (MILs) as a measurement that rates a program's completeness and development level of cybersecurity practices as well as the extent to which such practices are ingrained in daily operations. MILs range from M1L0 (an absence of security practices) to M1L3 (extensive implementation of best practices). MILs apply to separate cybersecurity domains (e.g., risk management and situational awareness).	ES-C2M2
National Cyber Incident Response Plan (NCIRP)	Plan developed by DHS and the Federal Emergency Management Authority (FEMA) to describe a nationwide approach to cyber incidents and discuss the role of private sector entities, states, and federal agencies in response to cyber incidents. An Interim NCIRP was released in 2011. DHS and FEMA are currently developing a new NCIRP to replace it.	About NCIRP Draft NCIRP
NIST	National Institute of Standards and Technology	
NIST Cybersecurity Framework	National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity" does not include requirements or standards, but rather a "common language" to address cybersecurity risk and a methodology that organizations can use to apply principles of risk management to improve the security and resilience of critical infrastructure.	NIST: Framework Basics and FAQs
NERC CIP	The cybersecurity standards and requirements created by NERC (see below) that apply to certain BESs (see above) in the United States are known as Critical Infrastructure Protection (CIP). The NERC CIP is the only mandatory federal cybersecurity framework for the utility industry. It includes penalties and sanctions for noncompliance. NERC CIP does not apply to distribution systems.	NERC: CIP Compliance
North American Electric Reliability Corporation (NERC)	NERC is a nonprofit international regulatory authority that, among other things, develops and enforces reliability standards and monitors the bulk power system. NERC is the electric reliability organization (ERO, see above) for North America, subject to oversight by FERC and Canadian authorities.	About NERC

Table 1 (continued)

Term or Acronym	Definition or Explanation	Relevant Links (if applicable)
Operations technology (OT)	In the ES-C2M2, OT is programmable systems or devices that interact with the physical environment (or manage devices that do) (e.g., industrial control systems, building management systems, physical access control mechanisms).	ES-C2M2
PCII	DHS' Protected Critical Infrastructure Information program seeks to protect private sector infrastructure information voluntarily shared with the government for homeland security purposes. The PCII protects such information from public disclosure.	PCII Program
Probe	An attempt to access a system to learn something about that system	
Spear-phishing	Phishing is an attempt to acquire sensitive information (usernames, passwords, or credit card or identity information) by pretending to be a trustworthy entity in an email or other communication. Perpetrators generally send phishing emails to a large number of recipients, asking them to click a link or perform some other action. Spear-phishing refers to a more targeted phishing attack where the fraudulent email appears to be from someone the recipient knows and may include personal information.	
Supervisory Control and Data Acquisition Systems (SCADA)	A generic name for a computerized system capable of gathering and processing data and applying operational controls over long distances. Used for pipeline systems and power transmission and distribution, SCADA was designed for communications challenges posed by the materials that must be used in such systems (e.g., delays due to electric lines).	
Telephone denial-of-service attack (TDOS)	An attack in which a large number of false telephone calls are generated and directed to one or more phone numbers to prevent those numbers from accepting legitimate phone calls.	

RESOURCES

AWWA: [Process Control System Security Guidance for the Water Sector](#), 2014.

FCC, CSRIC IV: [Cybersecurity Risk Management and Best Practices Working Group 4: Final Report](#), March 2015.

NERC: [Grid Security Exercise: GridEx III Report](#), March 2016.

NIST: [Guide to Industrial Control Systems \(ICS\) Security](#), May 2015.

PURA: [Connecticut Public Utilities Cybersecurity Action Plan](#), April 2016.

U.S. DOE and U.S. DHS: [Electricity Subsector Cybersecurity Capability Maturity Model \(ES-C2M2\)](#), February 2014.

U.S. DHS: [Draft National Cyber Incident Response Plan](#), September 2016.

Westar Energy, Community Programs, Kanza Education and Science Park: [The Substation](#)

MF:bs