2019

NARUC
Cybersecurity Manual

CYBERSECURITY GLOSSARY

COMPILED BY LYNN COSTANTINI AND MATTHEW ACHO

Introduction

NARUC has developed a comprehensive suite of resources, collectively referred to as the Cybersecurity Manual, to help public utility commissions (PUCs or "commissions") gather and evaluate information from utilities about their cybersecurity risk management practices. These evaluations facilitate well-informed PUC decisions regarding the effectiveness of utilities' cyber security preparedness efforts and the prudence of related expenditures.

The Cybersecurity Manual is comprised of five complementary resources. This *Cybersecurity Glossary* is one of them. A brief description of each resource follows.

1. ***Cybersecurity Strategy Development Guide*** |**2018**
   The Strategy Development Guide defines a roadmap that PUCs can follow to design and implement a structured approach for long-term engagement with utilities on cybersecurity matters. The Guide includes examples from PUCs that demonstrate the process steps and highlights practices that drive successful outcomes.
2. ***Assessing Cybersecurity Preparedness: Questions for Utilities*** |**2019**
   The Questions for Utilities provides a set of comprehensive, context-sensitive questions that PUCs can ask of a utility to gain a detailed understanding of its current cybersecurity risk management program and practices. The questions build upon and add to those included in prior NARUC publications.
3. ***Cybersecurity Preparedness Evaluation Tool (CPET)*** |**2019**
   The CPET provides a structured approach for PUCs to use in assessing the maturity of a utility's cybersecurity risk management program and gauging capability improvements over time. The CPET is designed to be used with the Questions for Utilities on an iterative basis to help PUCs identify cybersecurity gaps, spur utilities' adoption of additional mitigation strategies, and inform cybersecurity investment decisions.
4. ***Cybersecurity Tabletop Exercise (TTX) Guide*** |**2019**
   This guide details the steps that PUCs can take to design and execute an exercise to examine utilities' and other stakeholders' readiness to respond to and recover from a cybersecurity incident. It includes exercise scenarios and examples.
5. ***Cybersecurity Glossary*** |**2019**
   The *Glossary* contains cybersecurity terms used throughout the Cybersecurity Manual, as well as "terms of art" that utilities may use during discussions with PUCs.

Resources within the Cybersecurity Manual can be used individually but are designed to work together. NARUC's intent is to provide a comprehensive set of assessment tools that, when applied, provide a consistent, complete view of utilities' cybersecurity preparedness. **Figure 1**: NARUC Cybersecurity Manual depicts the complementary, process-oriented relationship among these components.

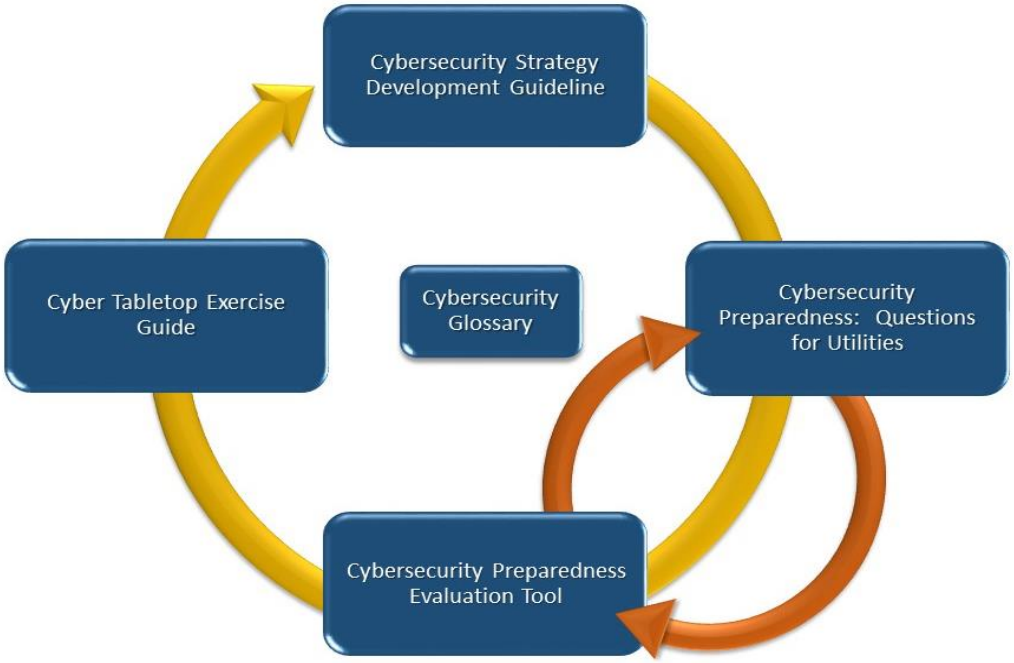

Figure 1: NARUC Cybersecurity Manual Components

The content of each component in the Cybersecurity Manual is customizable to meet specific goals, objectives, and requirements that PUCs have established around cybersecurity, complementing resources developed by and for utilities and other practitioners. Geared toward non-technical, policy-oriented users, each component captures information in sufficient detail to support PUC decision making.

Cybersecurity Glossary

This *Cybersecurity Glossary* contains definitions of cybersecurity terms and concepts found throughout the resources that comprise NARUC's Cybersecurity Manual. It also contains terms that public utility commissions may encounter during engagements with utilities on the topic of cybersecurity. A list of notable cybersecurity events is included at the end of the glossary.

Definitions contained in this glossary are from authoritative sources. They are gathered here for ease of use. Many definitions are cited verbatim; however, some have been paraphrased or adapted for clarity and conciseness. Links to original sources are included.

The *Cybersecurity Glossary* is a "living document." This means that new cybersecurity terms and concepts will be added to reflect the advancement of cybersecurity risk management and technology as time goes on.

Term	Definition	Source
Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).	NIST
Access Control List (ACL)	A list of permissions associated with an object (e.g., computer hardware or software or a gate that provides ingress and egress to a physical facility). The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.	CNSS
Advanced Persistent Threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources used to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the	NIST

Term	Definition	Source
	future. The advanced persistent threat: (1) pursues its objectives repeatedly over an extended period of time; (2) adapts to defenders' efforts to resist it; and (3) is determined to maintain the level of interaction needed to execute its objectives.	
After-Action Report (AAR)	Summary of key post-exercise evaluation information, including the exercise overview and analysis of objectives and core capabilities. It is developed in conjunction with an improvement plan, which identifies specific corrective actions, assigns them to responsible parties, and establishes target dates for their completion. The lead evaluator and exercise planning team draft the AAR.	FEMA
All-Hazards	A threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.	Presidential Policy Directive / PPD-21
Attestation	The validation of all aspects of a computer or system that relate to its safe, secure, and correct operation.	NRECA / Cooperative Research Network
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources.	NIST
Authorization	Verifying a user's permissions (after a user has been authenticated) for accessing certain resources or functionality.	NRECA / Cooperative Research Network

Term	Definition	Source
Availability	Ensuring timely and reliable access to and use of information. Resiliency objectives extend the concept to refer to point-in-time availability (i.e., the system, component, or device is usable when needed) and the continuity of availability (i.e., the system, component, or device remains usable for the duration of the time it is needed). With confidentiality and integrity, availability is considered part of the CIA Triad, which represents the three most crucial components of information security.	NIST
Bandwidth	The amount of information that can be passed through a communication channel in a given amount of time, usually expressed in bits per second.	ATIS
Bitcoin	An electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.	Bitcoin.org
Blacklist	A list of entities that are blocked or denied privileges or access.	US-CERT
Black Sky Hazard/Event	A catastrophic event that severely disrupts the normal functioning of critical infrastructures in multiple regions for long durations.	EIS Council
Black Start	The restoration of a power station without reliance on the external power transmission system. Black start capabilities are often provided by small co-located diesel generators used to start larger generators, which in turn start the main power station generators.	Idaho National Laboratory
Blockchain	Tamper-resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and	NIST

Term	Definition	Source
	usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation, no transaction can be changed once published.	
Botnet	A collection of computers compromised by malicious code and controlled across a network. (See Command and Control.) The word botnet is a combination of the words robot and network.	US-CERT
Boundary Protection	Monitoring and control of digital communications at the external perimeter of an information system to prevent and detect malicious and other unauthorized communications, using devices such as proxies, gateways, routers, firewalls, guards, and encrypted tunnels. Also referred to as perimeter protection.	NRECA / Cooperative Research Network
Bulk Electric System (BES) Cyber Asset	A Cyber Asset that, if rendered unavailable, degraded, or misused, would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	NERC
Command and Control (C&C or C2) network	A network of computers infected with malware that allows them to issue directives to other digital devices. C&C servers can create powerful networks of infected devices capable of carrying out distributed denial-of-	TechTarget

Term	Definition	Source
	service (DDoS) attacks, stealing data, deleting data or encrypting data in order to carry out an extortion scheme. A malicious network under a C&C server's control is called a botnet and the network nodes that belong to the botnet are sometimes referred to as zombies.	
Compensating Control	A cybersecurity control employed in lieu of a recommended control that provides equivalent or comparable control. See Cybersecurity Controls.	DOE
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. With integrity and availability, confidentiality is considered part of the CIA Triad, which represents the three most crucial components of information security.	NIST
Connectivity	The minimum number of nodes or links whose removal results in losing all paths that can be used to transfer information from a source to a sink.	ATIS
Contingency	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element.	NRECA / Cooperative Research Network
Credential	Information passed from one entity to another to establish the sender's access rights or to establish the claimed identity of a security subjective relative to a given security domain.	ATIS
Critical Assets	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would	NRECA / Cooperative

Term	Definition	Source
	affect the reliability or operability of the bulk electric system.	Research Network
Critical Electric Infrastructure Information (CEII)	Information related to or proposed to critical electric infrastructure, • Generated by or provided to the Federal Energy Regulatory Commission or other Federal agency other than classified national security information, • That is designated as critical electric infrastructure information by the Federal Energy Regulatory Commission or the Secretary of the Department of Energy pursuant to section 215A(d) of the Federal Power Act.	FERC
Critical Infrastructure	The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.	DHS
Cryptocurrency	A digital currency used as a medium of exchange, similar to other currencies. However, unlike other currencies, cryptocurrency operates independently of a central bank and uses encryption techniques and blockchain technology to secure and verify transactions. Examples include Bitcoin, Litecoin, Monero, Ethereum, and Ripple.	US-CERT
Cyber Asset	Programmable electronic devices, including the hardware, software, and data in those devices.	NRECA / Cooperative Research Network

Term	Definition	Source
Cyber Attack	An attempt to infiltrate information technology systems, computer networks, or individual computers with a malicious intent to steal information, cause damage, or destroy specific targets within the system.	Idaho National Laboratory
Cyber Information Sharing and Collaboration Program (CISCP)	A program of the U.S Department of Homeland Security that enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors.	DHS
Cyber Kill Chain	A theory developed by Lockheed Martin that identifies the various stages of a cyber attack: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C&C, and Actions on Objectives. Applying the theory helps cybersecurity professionals recognize and counteract attacks to protect their organization's assets.	SANS Institute
Cyber Mutual Assistance Program	A framework to provide emergency cyber assistance within the electric power and natural gas industries. The program is composed of industry cyber experts who can provide voluntary assistance to other participating entities in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.	Electricity Sector Coordinating Council
Cyber Security Incident Response Teams (CSIRTs)	A group of experts that assesses, documents, and responds to a cyber incident so that a network can not only recover quickly, but also avoid future incidents.	DHS
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks.	DOE
Cybersecurity Capability Maturity Model (C2M2)	A model that helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity capabilities.	DOE

Term	Definition	Source
Cybersecurity Controls	The management, operational, and technical methods, policies, and procedures—manual or automated—(i.e., safeguards or countermeasures) prescribed to protect the confidentiality, integrity, and availability of a system and its information.	DOE
Cybersecurity Incident	An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. A cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.	Presidential Policy Directive / PPD-41
Cybersecurity Risk Information Sharing Program (CRISP)	A public-private data sharing and analysis platform that facilitates the timely bi-directional sharing of unclassified and classified threat information among energy sector stakeholders.	DOE
Cyberspace	A global domain within the information environment consisting of the interdependent network of IT and ICS infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.	DOE
Darknets	Private, distributed file sharing networks where connections are made only between trusted peers. Darknets are distinct from other distributed networks as sharing is anonymous (i.e., IP addresses are hidden).	Cyber Risk Insurance Forum

Term	Definition	Source
Defense-in-Depth	Cybersecurity strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.	DOE
Denial of Service (DoS)	A cyber attack that occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. A denial-of-service floods the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.	DHS
Distributed control system (DCS)	Control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit.	NIST
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which systems are connected.	NERC
Energy Assurance	An array of activities that support a robust, secure, reliable, and resilient energy infrastructure. These include energy emergency planning, preparedness, mitigation, and response	NASEO
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.	Idaho National Laboratory
Endpoint Protection/Security	A security approach that focuses on locking down endpoints—individual computers, phones, tablets, and	CSO Online

Term	Definition	Source
	other network-enabled devices—in order to keep networks safe.	
Exploit	A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.	Idaho National Laboratory
Firewall	A network security device that monitors incoming and outgoing network traffic and helps screen out hackers, viruses, and worms that try to reach a computer over the Internet. A firewall can be hardware, software, or both.	Cisco
Firmware	A software program or set of instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.	TechTerms
Fusion Centers	Primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among Federal, State, Local, Tribal, and Territorial (SLTT) partners. They provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. Fusion centers are owned and operated by State and Local entities with support from federal partners.	DHS
Gateway	An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.	CNSS

Term	Definition	Source
Homeland Security Information Network (HSIN)	A trusted network for homeland security mission operations to share sensitive but unclassified information. Federal, state, local, territorial, tribal, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and share the information they need to do their jobs and help keep their communities safe.	DHS
Honeypot	A trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.	Cyber Risk Insurance Forum
Human-Machine Interface (HMI)	The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.	NIST
Identity-Based Access Control	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user), where access authorizations to specific objects are assigned based on user identity.	NRECA / Cooperative Research Network
Impact	Damage to an organization's mission and goals due to the loss of confidentiality, integrity, or availability of system information or operations.	NRECA / Cooperative Research Network
Indicators of Compromise (IOC)	Forensic artifacts of an intrusion.	SANS Institute

Term	Definition	Source
Industrial Control System (ICS)	A general term that includes several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), Programmable Logic Controllers (PLC) and others often found in industrial and critical infrastructure sectors. An ICS consists of combinations of control components that act together to achieve an industrial objective.	Idaho National Laboratory
Industrial Control Cyber Emergency Response Team (ICS-CERT)	Operates within the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) to reduce risks to industrial control systems used within and across all critical infrastructure sectors. ISC-CERT collaborates law enforcement agencies and the intelligence community and coordinates efforts among Federal, State, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.	DHS
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.	NRECA / Cooperative Research Network
Information Sharing and Analysis Center (ISAC)	Sector-specific, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry.	DHS
Information System (IS)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Note: information systems also include specialized systems such	NRECA / Cooperative Research Network

Term	Definition	Source
	as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.)	
Information Technology (IT)	The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.	Merriam Webster Dictionary
InfraGard	A partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure.	Infragard
Integrity	Guarding against improper information modification or destruction; includes ensuring the non-repudiation and authenticity of information. With confidentiality and availability, integrity is considered part of the CIA Triad, which represents the three most crucial components of information security.	NRECA / Cooperative Research Network
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).	NIST
International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Standards	Standards that represent global consensus on a solution to a particular issue. They provide requirements, specifications, guidelines or characteristics to ensure that materials, products, processes and services are safe to use and fit for their purpose. Whenever possible, requirements are expressed in terms of performance rather than design or descriptive characteristics.	ISO

Term	Definition	Source
Internet Protocol (IP)	Standard method for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.	NIST
Interoperability	The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together.	Rand Corporation
Joint Information Center (JIC)	A central location to facilitate operation of the Joint Information System (JIS) during and after an incident. The JIC enhances information coordination, reduces misinformation, and maximizes resources by co-locating Public Information Officers (PIOs) as much as possible.	FEMA
Joint Information System (JIS)	An incident response structure that can be leveraged for developing and delivering coordinated interagency messages, executing public information plans and strategies, advising an Incident Commander concerning public affairs issues, and controlling rumors and inaccurate information.	FEMA
Key Logger	A program designed to record the sequence of keys pressed on a computer keyboard. Such programs can be used to obtain passwords or encryption keys and thus bypass other security measures.	NIST
Least Privilege	The principle that users and programs should only have the necessary privileges to complete their tasks.	NIST
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Examples include viruses, worms, and Trojan horses, spyware and some forms of adware.	NIST

Term	Definition	Source
Management Controls	The security controls for IT and ICS that focus on the management of risk and security.	DOE
Man-In-The-Middle (MitM)	A type of cyber attack where an interloper inserts him- or herself between two communicating devices, without either side knowing.	US-CERT
National Cybersecurity and Communications Integration Center (NCCIC)	The cyber defense, incident response, and operational integration center of the U.S. Department of Homeland Security. The NCCIC's mission is to reduce the risk of systemic cybersecurity and communications challenges by serving as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating a 24/7 situational awareness, analysis, and incident response center.	DHS
National Institutes of Standards and Technology (NIST)	A federal agency within the U.S. Department of Commerce. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST is also responsible for establishing computer- and information technology-related standards and guidelines for federal agencies to use.	NIST
NIST Cybersecurity Framework (NIST CSF)	A voluntary framework consisting of standards, guidelines, and best practices to manage cybersecurity risk.	NIST
Need to Know	Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.	NIST
Network (computer network)	A network of data processing nodes interconnected for the purpose of data communication.	ATIS

Term	Definition	Source
North American Electric Reliability Corporation	A not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the bulk electric grid in North America.	NERC
NERC Critical Infrastructure Protection (NERC CIP)	A set of requirements designed to secure cyber assets required for operating North America's bulk electric system.	TechTarget
Operational Controls	The security controls for IT and ICS, implemented and executed primarily by people (as opposed to systems).	DOE
Operational Technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.	DOE
Packet	The sequence of binary digits transmitted and switched as a composite whole.	ATIS
Phishing	An attempt to trick people into divulging sensitive information such as usernames, passwords, or credit card numbers. Phishing is carried out by email, over the phone, or using a website. The motives are generally to steal money or a user's identity.	Symantec
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES cyber assets, BES cyber systems, or electronic access control or monitoring systems reside, and for which access is controlled.	NERC
Personally Identifiable Information (PII)	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect	DOL

Term	Definition	Source
	means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.	
Potential Impact	The loss of confidentiality, integrity or availability that might have: 1) a limited adverse effect; 2) a serious adverse effect; or 3) a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	NRECA / Cooperative Research Network
Privileged User	A user that is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.	NRECA / Cooperative Research Network
Programmable Logic Controller (PLC)	A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as input/output control, logic, timing, counting, communication, and data and file processing.	Idaho National Laboratory
Protected Critical Infrastructure Information Program (PCII)	A DHS-specific information protection program that enhances voluntary information sharing between infrastructure owners and operators and the government. PCII protections mean that homeland security partners	DHS

Term	Definition	Source
	can be confident that sharing their information with the government will not expose sensitive or proprietary data.	
Ransomware	A malicious form of software that locks a computer or files and requires money be paid to get the decryption code to unlock the device or the file.	Microsoft
Red Team/Blue Team	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture (i.e., the Red Team). The objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment	NIST
Remote Access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet)	NIST
Remote Access Trojan (RAT)	A malicious program that runs invisibly on host computers and permits an intruder to gain access and control from afar. Many RATs mimic legitimate functionality but are designed specifically for stealth installation and operation.	Microsoft
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	Presidential Policy Directive / PPD-21
Risk	The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.	US-CERT

Term	Definition	Source
Risk Management	The process of controlling risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, 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 and privacy state of the information system.	NIST
Risk severity	A combination of the likelihood of a damaging event actually occurring and the assessed potential impact on the organization's mission and goals if it does occur.	NRECA / Cooperative Research Network
Role-based access control	Access permission based on users' roles and typically reflect the need to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.	NRECA / Cooperative Research Network
Sandbox	A system that allows an untrusted software application to run in a highly controlled environment where the application's permissions are restricted. In particular, an application in a sandbox is usually restricted from accessing the file system or the network.	NIST
Sensitive Information	Information of which the loss, misuse, unauthorized access or modification could adversely affect the organization, its employees or its customers.	NRECA / Cooperative Research Network
Significant Cyber Incident	A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests,	Presidential Policy

Term	Definition	Source
	foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.	Directive / PPD-41
Social Engineering	Psychological manipulation of people into divulging sensitive information or performing certain actions.	Symantec
Sunshine Laws	Open government laws that foster an informed citizenry by providing the public access to government documents and meetings.	NCSL
Supervisory Control and Data Acquisition (SCADA)	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.	NIST
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.	NIST
Technical Controls	Security controls for IT and ICS implemented and executed primarily through mechanisms contained in hardware, software, or firmware.	DOE

Term	Definition	Source
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations through an IT and ICS via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	DOE
Threat Actor/Agent	An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.	US-CERT
Traffic Light Protocol (TLP)	A set of designations used to ensure that sensitive information is shared appropriately. It employs four colors to indicate expected sharing boundaries by the recipient(s). **RED**: information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. **AMBER**: information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. **GREEN**: information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. **WHITE**: information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	US-CERT
United States Computer Emergency Readiness Team (US-CERT)	A partnership between the U.S. Department of Homeland Security and the public and private sectors, established to protect the nation's internet infrastructure. US-CERT coordinates defenses against and responses to cyber attacks across the nation.	NIST

Term	Definition	Source
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.	CNSS
Vulnerability	A specific weakness in an information system, system security procedures, internal controls, or implementation that a threat source could exploit.	NIST
Watering Hole Attack	A security exploit where the attacker infects websites frequently visited by members of a targeted group being attacked, with a goal of infecting a computer used by one or more of the targeted group members when they visit the infected website.	NIST
Whitelist	A list of entities considered trustworthy and granted access or privileges.	US-CERT
Worm	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.	CNSS
Zero-Day Attack/Exploit	An attack that exploits a previously unknown hardware, firmware, or software vulnerability.	NIST
Zero Trust	A security concept centered on the belief that organizations should not automatically trust anything *inside* or *outside* its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.	CSO Online

Notable cybersecurity events that impacted or had the potential to impact the safe, reliable operation of critical infrastructure assets are summarized in the table that follows. Links to the original source documents are included in footnotes. This table will be updated as warranted.

Timeline of Significant Cybersecurity Related Events and Incidents		
Date	**Event/Incident**	**Description**
March 2007	Aurora	Aurora was the demonstration of a control system software vulnerability that could be exploited to physically destroy power grid equipment. Specifically, researchers at Idaho National Labs used a virus to manipulate systems that controlled a diesel generator. The test involved opening and closing circuit breakers in a manner that resulted in an out-of-synchronism or out-of-phase condition. This condition placed stress upon the mechanical components of rotating equipment in the generator, causing that equipment to fail before protection relays could respond. [1] Comprehensive mitigation techniques include protection and control, electronic and physical security, monitoring, training, risk assessment, and information protection.[2]
June 2010	Stuxnet	Stuxnet is a sophisticated computer worm that exploited multiple zero-day software vulnerabilities to infect computers and spread. Its purpose was to cause real-world physical effects. Specifically, Stuxnet targeted centrifuges used to produce enriched uranium, which powers nuclear weapons and reactors. [3]

[1] http://www.thepresidency.org/sites/default/files/pdf/Final%20Grid%20Report_1.pdf.
[2] https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6452_MythReality_MZ_20110217_Web2.pdf?v=20181015-210359.
[3] https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

April 2013	Metcalf Incident	The Metcalf incident refers to a physical attack on a 500kV electric substation in Metcalf, Calif. During the attack, multiple individuals outside the substation reportedly shot at the HV transformer radiators with .30 caliber rounds, causing them to leak cooling oil, overheat, and become inoperative. [4]
June 2014	Havex	Havex is a remote access trojan (RAT) that was part of a widespread espionage campaign targeting ICS across numerous critical infrastructure industries, including energy. Researchers attributed the campaign to a hacking group referred to as "Dragonfly" and "Energetic Bear," since linked to Russian Intelligence Services.[5] Users were infected with Havex via watering hole attacks. Once installed, the malware collected data about the ICS environment and reported back to the attackers via C&C servers. This attack suggests that the attackers had direct interest in controlling ICS environments. [6],[7]
December 2015	Cyber Attack on the Ukrainian Power Distribution Grid	On December 23, 2015, a coordinated cyber attack was launched on three electricity distribution companies (oblenergos) in Ukraine, during which attackers remotely controlled SCADA distribution management systems, causing power outages to approximately 225,000 customers for three hours.[8] The attacks required the companies to move to manual operations in response.[9] This attack was the first known instance of using malware to generate a real-world power outage.[10]

[4] https://fas.org/sgp/crs/homesec/R43604.pdf.
[5] https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/havex.
[6] https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01.
[7] https://www.f-secure.com/weblog/archives/00002718.html.
[8] https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[9] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.
[10] https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/.

		The attacks were linked to a Russian group known as Sandworm.[11]
December 2016	CRASHOVERRIDE/ Industroyer	CRASHOVERRIDE/Industroyer is a first-of-its-kind, ICS-tailored malware framework designed and deployed to attack electric grids. It leverages knowledge of grid operations and ICS network communications to cause impact.[12] CRASHOVERIDE/Industroyer was used in a cyber attack that de-energized a transmission-level substation in Kiev, Ukraine, on December 17, 2016. The attack was similar to one against three Ukrainian electric distribution companies in 2015, which rendered substation devices inoperable and prevented engineers from remotely restoring power. Researchers suggests that components in the CRASHOVERIDE/ Industroyer malware are far more advanced than the malware used in the 2015 attack.[13],[14],[15] ICS security firm Dragos, Inc. tracked the adversary behind CRASHOVERRIDE/Industroyer to Electrum, a hacker group with direct ties to the Russian Sandworm team.[16]
November 2017	TRITON/TRISIS	Triton/TRISIS is malware that targets Schneider Electric Triconex Safety Instrumented System (SIS) controllers. A SIS is an autonomous control system that monitors industrial processes and detects and prevents dangerous physical events. For example, a SIS will safely shut down rotating machinery when a

[11] https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html.
[12] https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.
[13] https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.
[14] https://arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet.
[15] https://www.eset.com/int/industroyer/.
[16] https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.

		dangerous condition is detected. Each SIS in unique. [17] [18] Triton/TRISIS is the first ever publicly known ICS-tailored malware to target safety instrumented systems. [19] It was discovered when cybersecurity firm Mandiant responded to a cyber incident at a critical infrastructure organization in the Middle East. The malware appears to have been deployed manually after a threat actor familiar with the proprietary Triconex system gained remote access to a SIS engineering workstation and attempted to reprogram the SIS controllers, inadvertently causing the automatic shutdown of the associated industrial process. The attacker may have been attempting to develop the capability to cause physical damage to the organization's equipment. [20] This activity has not been attributed to any particular threat actor, although nation state sponsorship is suspected.[21]

[17] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.
[18] https://dragos.com/wp-content/uploads/TRISIS-01.pdf.
[19] https://dragos.com/wp-content/uploads/TRISIS-01.pdf.
[20] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.
[21] https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton?rq=Trisis.