# Acronyms, Initialisms, and Abbreviations

**AAR**. After-Action Review

**ACL**: Access Control List. A list of entities, together with their access rights, that are authorized to have access to a resource. (NIST, 2020)

**IACET.** International Association for Continuing Education and Training

**APT**: Advance Persistent Threat. An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives. (NIST, 2020)

**BASE**: Basic Analysis and Security Engine

**BCP**: Business Continuity Plan. The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. (NIST, 2020)

**BIA**: Business Impact Analysis. An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (NIST, 2020)

**C&C**: Command and Control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (NIST, 2020)

**CCE**: Common Configuration Enumeration. A nomenclature and dictionary of software security configurations. (NIST, 2020)

**CCSMM**. Community Cybersecurity Maturity Model

**CDI**. Cyberterrorism Defense Initiative

**CfIA**. The University of Memphis Center for Information Assurance

**CI**: Critical Infrastructure. System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (NIST, 2020)

**CIA:** Central Intelligence Agency

**CIA**: C = Confidentiality assurance, I = Integrity assurance, A = Availability assurance (NIST, 2020)

**CIAS**. The Center for Infrastructure Assurance and Security

**CIKR**: Critical Infrastructure and Key Resources

**CIO**: 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. (NIST, 2020)

**CISA**: Cybersecurity and Infrastructure Security Agency

**CISO**: Chief 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. (NIST, 2020)

**CPG**. Comprehensive Preparedness Guide

**COOP**: Continuity of Operations Plan. A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. (NIST, 2020)

**CSF**: Cybersecurity Framework. A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. (NIST, 2020)

**CSIRT**: Computer Security Incident Response Teams. A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). (NIST, 2020)

**CTIIC**. Cyber Threat Intelligence Integration Center

**DAD**: Disclosure, Alteration, and Destruction

**DB**. Data Base

**DDoS**: Distributed Denial of Service. A denial of service technique that uses numerous hosts to perform the attack. (NIST, 2020)

**DHS**: U.S. Department of Homeland Security www.dhs.gov

**DISA**: Defense Information Systems Agency www.disa.mil

**DMZ**: Demilitarized Zone. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance 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. (NIST, 2020)

DNS. Domain Name System

**DoD**: Department of Defense. Lead Federal agency for homeland defense, including maritime interception, air patrols over U.S. airspace, landbased defense of critical infrastructure and key assets, and use of military forces to protect from attack when directed by the President or Secretary of Defense. (DHS Lexicon, 2020)

**DOE**. Department of Energy

**DOJ**. Department of Justice

**DoS**: Denial of Service. The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided). (NIST, 2020)

**DRaaS**. Disaster Recovery as a Service

**EMC**. Exchange Management Console

**EMC**. Emergency Management Coordinator

**EMP**. Electromagnetic Pulse

**EOC**: Emergency Operations Center. Physical location where the coordination of information and resources to support incident management activities normally takes place. (DHS Lexicon, 2020)

**EOP**. Emergency Operations Plan

**ERP**. Emergency Response Plan

**ESF**. Emergency Support Functions

**FBI**: Federal Bureau of Investigation (NIST, 2020)

**FEMA**: Federal Emergency Management Agency www.fema.gov (NIST, 2020)

**FERC**. Federal Energy Regulatory Commission

**FSE**. Full-Scale Exercise

**HSEEP**: Homeland Security Exercise and Evaluation Program. An abbreviation. https://hseep.dhs.gov/pages/1001_HSEEP7.aspx

**HTTP**: Hypertext Transfer Protocol. A standard method for communication between clients and Web servers. (NIST, 2020)

**HUMINT**: Human Intelligence

**IAP**. Incident Action Plan

**IC**. Incident Commander

**IC3**. Internet Crime Complaint Center

**ICP**. Incident Command Post

**ICS**. Incident Command System

**ICS-Cert**. Industrial Control Systems Computer Emergency Response Team

**IDS**: Intrusion Detection System. Software that looks for suspicious activity and alerts administrators. (NIST, 2020)

**IIS**: Internet Information Service

**IO**. Information Officer

**IP**: Internet Protocol. Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (NIST, 2020)

**IPv4**. Internet Protocol Version 4

**IPv6**. Internet Protocol Version 6

**IRAP**: Incident Recovery Action Plan

**IRC**. Internet Relay Chat

**ISACA**: Formerly known as the Information Systems Audit and Control Association, the acronym ISACA is now the proper name of an IT security and governance professional trade association.

**ISSA**: Information Systems Security Association. An abbreviation. A professional association for providers of IT security.

**IT**: Information Technology. Equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. (DHS Lexicon, 2020)

**JFO**: Joint Field Office

**JIC**. Joint Information Center

**JIT**. Just-In-Time

**JOC**. Joint Operations Center

**LEPC**. Local Emergency Planning Committees

**LNO**: Liaison Officer. Temporary detail of an employee to another agency to coordinate efforts of the parent organization. (DHS Lexicon, 2020)

**MACS**. Multiagency Coordination System

**MOU**: Memorandum of Understanding. A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes specific terms that are agreed to, and a commitment by at least one party to engage in action. It includes either a commitment of resources or binds a party to a specific action. (NIST, 2020)

**NCCIC**. National Cybersecurity and Communications Integration Center

**NCIJTF**. National Cyber Investigative Joint Task Force

**NCIRP**. National Cyber Incident Response Plan

**NCPC**. National Cybersecurity Preparedness Consortium

**NDRF**. National Disaster Recovery Framework

**NERC**. North American Electric Reliability Corporation

**NERRTC**. National Emergency Response and Recovery Training Center

**NIMS**. National Incident Management System

**NIPP**. National Infrastructure Protection Plan

**NIST**: (National Institute of Standards and Technology) www.nist.gov (NIST, 2020)

**NLE**. National Level Exercise

**NMAP**. Network Mapper

**NRF**. National Response Framework

**NTED**. National Training and Education Division

**NUARI**. Norwich University Applied Research Institutes

**NWS**. National Weather Service

**OE**. Operating Environment

**OSINT**. Open Source Intelligence

**PDD**. Presidential Decision Directive

**PIO**. Public Information Officer

**PNP**. Private Nonprofit

**POETE**. Plan, Organize, Equip, Train, Exercise

**PPD**. Presidential Policy Directive

**PURPA**. Public Utility Regulatory Policies Act

**IRAP**. Incident Recovery Action Plan

**RDP**. Remote Desk Protocol

**RISS**: Regional Information Sharing Systems. Secure national intranet to facilitate law enforcement communications and information sharing nationwide. (DHS Lexicon, 2020)

**RPC**: Remote Procedure Call

**SCADA**: Supervisory Control and Data Acquisition. 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, 2020)

**SCAN**. See, Contact, Ask, Notify

**SLA**: Service Level Agreement. Defines the specific responsibilities of the service provider and sets the customer expectations. (NIST, 2020)

**SMART**. Specific Measurable Achievable Realistic Time-phased

**SMTP**: Simple Mail Transport Protocol. An MTA protocol defined by IETF RFC 2821. SMTP is the most commonly used MTA protocol. (NIST, 2020)

**SO**. Safety Officer

**SOC**. State Operations Center

**SOP**: Standard Operating Procedure. A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event. (NIST, 2020)

**SP**. Special Publication

**TCP**: 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 hosts 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. (NIST, 2020)

**TEEX**. Texas A&M Engineering Extension Service

**TEWG**. Terrorism Early Warning Group

**THIRA**: Threat and Hazard Identification and Risk Assessment. Four-step common risk assessment process that helps the whole community including persons, businesses, faith-based organizations, non-profit groups, schools and academia, and all levels of government understand its risks and estimate capability requirements. (DHS Lexicon, 2020)

**US-Cert**. U.S. Computer Emergency Response Team

# Terminology

**Advanced Persistent Threat:** An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives. (NIST, 2020)

**Attack Vectors:** A path or means by which a cyber attacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable attackers to exploit system vulnerabilities, including the human element. Blackout. The complete loss of electrical power in a particular area, resulting from a natural or man-made disaster, or simply from an excess of energy demand over supply.

**Availability**: Ensuring timely and reliable access to and use of information. (NIST, 2020)

**Botnets:** (robot-networks) A network consisting of thousands of machines that have been infected with Trojan horse viruses and are now controlled by criminals.

**Brownout:** Where the voltage level is below the normal minimum level specified for the system. Systems supplied with three-phase electric power also suffer brownouts if one or more phases are absent, at reduced voltage, or incorrectly phased.

**Brute force attack:** In cryptography, an attack that involves trying all possible combinations to find a match. (NIST, 2020)

**Bulk Power System**: The part of the overall electricity system that includes the generation of electricity and the transmission of electricity over high-voltage transmission lines to distribution companies. This includes power generation facilities, transmission lines, interconnections between neighboring transmission systems, and associated equipment. It does not include the local distribution of the electricity to homes and businesses.

**Business Continuity Plan, BCP**: Pretty much the same as COOP, but COOP has traditionally been used by the public sector and Business Continuity in the private sector) Definition: An ongoing process to ensure that the necessary steps are taken to identify the impacts of potential losses and maintain viable continuity and recovery strategies and plans. (NFPA 1600 2019 edition)

**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.

**Capacity:** The amount of electric power delivered or required for which a generator, turbine, transformer, transmission circuit, station, or system is rated by the manufacturer.

**Circuit:** A dedicated single connection between two endpoints on a network. (NIST, 2020)

**Code:** 1. A set of instructions for a computer. 2. System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. (NIST, 2020)

**Community Cyber Security Maturity Model**: A community-based cyber security model that provides methods for communities to enhance their ability to successfully prevent, detect, respond to and recover from a cyber security incident.

**Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST, 2020)

**COOP:** Continuity of Operation Plan. A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. (NIST, 2020)

**Critical Infrastructure:** System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (NIST, 2020)

**Critical Infrastructure:** Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any federal, state, regional, territorial, or local jurisdiction. (DHS Lexicon, 2020)

**Criticality:** A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. (NIST, 2020)

**Cybersecurity**: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (NIST, 2020)

**Cyber Incident:** Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. See incident. See also event, security-relevant event, and intrusion. (NIST, 2020)

**Cyber Preparedness**: The process of ensuring that an agency, organization, or jurisdiction has developed, tested, and validated its capability to protect against, prevent, mitigate, respond to and recover from a significant cyber incident.

**Data Exfiltration**: Unauthorized copying, transfer, or retrieval of data from a computer, device, or server.

**DDoS:** Distributed Denial of Service. An abbreviation. A denial of service technique that uses numerous hosts to perform the attack. (NIST, 2020)

**Detect** (function). Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

**Disaster Recovery Plan, DRP**: An information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. (NIST, 2020)

**DoS** [attack]: An abbreviation. The prevention of authorized access to resources or the delaying of time-critical operations. Time-critical may be milliseconds or it may be hours, depending upon the service provided. (NIST, 2020)

**Electric Utility:** A corporation, person, agency, authority, or other legal entity or instrumentality that owns and/or operates facilities within the United States, its territories, or Puerto Rico for the generation, transmission, distribution, or sale of electric energy primarily for use by the public and files forms listed in the Code of Federal Regulations, Title 18, Part 141. Facilities that qualify as co-generators or small power producers under the Public Utility Regulatory Policies Act (PURPA) are not considered electric utilities.

**Emergency Operations Center** (EOC): Physical location where the coordination of information and resources to support incident management activities normally takes place may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level or organization within a jurisdiction. (DHS Lexicon, 2020)

**Emergency Operations Plan:** An EOP is a document that (1) assigns responsibility to Plan (EOP) organizations and individuals for carrying out specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency; (2) sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated; (3) describes how people and property will be protected in emergencies and disasters; (4) identifies personnel, equipment, facilities, supplies, and other resources available for use during response and recovery operations; and (5) identifies steps to address mitigation concerns during response and recovery activities.

**Emergency Support Functions** (ESFs): Used by the Federal Government and many State governments as the primary mechanism at the operational level to organize and provide assistance. ESFs align categories of resources and provide strategic objectives for their use. ESFs utilize standardized resource management concepts such as typing, inventorying, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.

**Fail Over:** A method of protecting computer systems from failure, in which standby equipment automatically takes over when the main system fails.

**Forensics:** The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (NIST, 2020)

**Fusion Center:** Physical or logical facility, encompassing all necessary infrastructure required to facilitate nationwide information-sharing between one or more federal, state, and/or local law enforcement entities, dedicated to the integration of multiple diverse data sources within a defined functional domain. (DHS Lexicon, 2020)

**Framework:** A layered structure indicating what kind of programs can or should be built and how they would interrelate. Some computer system frameworks also include actual programs, specify programming interfaces, or offer programming tools for using the frameworks. A framework may be for a set of functions within a system and how they interrelate; the layers of an operating system; the layers of an application subsystem; how communication should be standardized at some level of a network; and so forth. A framework is generally more comprehensive than a protocol and more prescriptive than a structure. (NIST, 2020)

**Generation:** The process of creating electric energy by transforming other forms of energy into electricity.

**Generator:** A machine that converts mechanical energy into electrical energy.

**Grid:** The network of interconnected electricity lines that transport electricity from power plants and other generating facilities to local distribution areas.

**Hacker:** Unauthorized user who attempts to or gains access to an information system. (NIST, 2020)

**Hactivist:** Computer hacker with a political agenda.

**Hazard:** Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

**Honeypot:** A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. (NIST, 2020)

**HTTP:** Hyper Text Transfer Protocol. An abbreviation. A standard method for communication between clients and Web servers. (NIST, 2020)

**Human Intelligence (HUMINT)**: Intelligence collected by human interaction in order to obtain critical and private information using various psychological deceptions.

**Identify (function):** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. (NIST, 2020)

**IIS:** Internet Information Service. An abbreviation. Server functions that provide web capability to machines running the Microsoft Windows operating system.

**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. (NIST, 2020)

**Indicators**: A sign that an incident may have occurred or may be currently occurring. (NIST, 2020)

**InfraGard:** Partnership between the FBI and businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. (DHS Lexicon, 2020)

**Infrastructure:** Framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (DHS Lexicon, 2020)

**Integrity**: Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. (NIST, 2020)

**Intelligence**: (1) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence. (NIST, 2020)

**Interconnection:** A common transmission line connecting two or more electric systems. Interconnections allow electricity to flow between the two systems, and facilitate the sale of electricity between the two regions served by the systems. (b) The synchronized grids in North America: the Eastern Interconnection, Western Interconnection, ERCOT, and Quebec Interconnection.

**Internet Information Service (IIS)**: An abbreviation. Server functions that provide web capability to machines running the Microsoft Windows operating system.

**Internet Protocol (IP):** Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (NIST, 2020)

**Internet Relay Chat:** Software making chat room conversations possible in real time.

**Interruptible Load:** Refers to program activities that, in accordance with contractual arrangements, can interrupt consumer load at times of seasonal peak load by direct control of the utility system operator or by action of the consumer at the direct request of the system operator. It usually involves commercial and industrial consumers. In some instances, the load reduction may be affected by direct action of the system operator (remote tripping) after notice to the consumer in accordance with contractual provisions. For example, loads that can be interrupted to fulfill planning or operation reserve requirements should be reported as “interruptible load.” interruptible load as defined here excludes direct load control and other load management. (Interruptible load, as reported here, is synonymous with “interruptible demand” reported to the North American Electric Reliability Council on the voluntary Form EIA-411, “Coordinated Regional Bulk Power Supply Program Report,” with the exception that annual peakload effects are reported on the Form EIA-861 and seasonal (i.e., summer and winter) peakload effects are reported on the EIA-411).

**IP Address**: Internet Protocol address is an identifying number for a piece of network hardware. An IP address allows a device to communicate with other devices over the Internet.

**Kerberos Pass the Ticket**: A widely used authentication protocol developed at MIT. In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user (Alice) who wishes to communicate with another user (Bob) authenticates to the KDC and the KDC furnishes a "ticket" to use to authenticate with Bob. (NIST, 2020)

**Lateral Movement**: Progressively moving through a network performing internal reconnaissance to better understand the structure, software, services, and data on the network. Includes activities related to reconnaissance, credentials stealing, and infiltrating other computers or systems.

**Malware:** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (NIST, 2020)

**Man-In-The-Middle Attack**: A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. (NIST, 2020)

**Metadata**: Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).Multiagency. The combination of facilities, equipment, personnel, coordination system procedures, and communications integrated into a common system with responsibility for coordination of assisting agency resources and support to agency emergency operations. (NIST, 2020)

**National Preparedness Goal**: A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

**National Preparedness System**: An organized process for everyone in the whole community to move forward with their preparedness activities and achieve the National Preparedness Goal.

**Nation-state** (or nation-state actors): Those geopolitical entities with acknowledged legal sovereignty of their domain(s), and the power associated thereof.

**Network Traffic:** Computer network communications that are carried over wired or wireless networks between hosts. (NIST, 2020)

**Neuro-Linguistic Hacking**: Face-to-face social engineering using psychological manipulation to gain someone's trust and obtain information.

**Obfuscation**: Actions taken to avoid detection.

**Open Source Intelligence (OSINT)**: Data collected from publicly available sources.

**Outage:** The period during which a generating unit, transmission line, or other facility is out of service.

**Pass-the-Hash**: Method of authenticating as a user without having access to the user'scleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash.

**Password Cracking**: The process of recovering secret passwords stored in a computer system or transmitted over a network. (NIST, 2020)

**Payload:** Consists of the information passed down from the previous layer. (NIST, 2020)

**Phishing:** Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (NIST, 2020)

**Ping:** An operation in IP communication whereby an ICMP packet is sent to a host of unknown status, in order to determine various information from the "echo" of the packet.

**Port:** The entry or exit point from a computer for connecting communications or peripheral devices. (NIST, 2020)

**Port scans:** A technique that sends client requests to a range of service port addresses on a host. (NIST, 2020)

**Precursors**: A sign that an attacker may be preparing to cause an incident. (NIST, 2020)

**Pretexting**: The practice of presenting oneself as someone else in order to obtain private information.

**Privilege Escalation**: The exploitation of a bug or flaw that allows for a higher privilege level than what would normally be permitted. (NIST, 2020)

**Prod:** Production Server.

**Protect (function):** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. (NIST, 2020)

**Rainbow Tables**: Pre-computed tables filled with hash values that are pre-matched to possible plaintext passwords. The Rainbow Tables essentially allow attackers to reverse the hashing function to determine what the plaintext password might be. The plaintext password may not even be the same password created by the user, but as long as the hash is matched, it doesn't matter what the original password was.

**Ransomware**: A form of malicious software—malware—that encrypts documents on a PC or even across a network. Victims can often only regain access to their encrypted files and PCs by paying a ransom to the criminals behind the ransomware.

**Reconnaissance:** The efforts of threat actors to gain as much information about an individual, organization and IT systems as possible before launching an attack.

**Recover (function):** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

**Reliability:** Electric system reliability has two components—adequacy and security. Adequacy is the ability of the electric system to supply to aggregate electrical demand and energy requirements of the customers at all times, taking into account scheduled and unscheduled outages of system facilities. Security is the ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements.

**Respond (function):** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. (NIST, 2020)

**Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (NIST, 2020)

**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. (NIST, 2020)

**Rootkit:** A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means. (NIST, 2020)

**RPC:** (Remote Procedure Call) An abbreviation. Function that allows a program to conduct activity in another address space without specific user direction to do so.

**Sandbox:** A system that allows an untrusted application to run in a highly controlled environment where the application's permissions are restricted to an essential set of computer permissions. In particular, an application in a sandbox is usually restricted from accessing the file system or the network. A widely used example of applications running inside a sandbox is a Java applet. (NIST, 2020)

**SCADA. Supervisory Control and Data Acquisition.** 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, 2020)

**Scanning:** Sending packets or requests to another system to gain information to be used in a subsequent attack. (NIST, 2020)

**Secondary Device:** A device placed by perpetrators at the scene of an incident specifically designed to harm responders.

**Spoof/Spoofing/Spoofed:** 1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. (NIST, 2020)

**SQL Injection**: Attacks that look for web sites that pass insufficiently-processed user input to database back-ends. (NIST, 2020)

**Staging Targets**: The initial victims targeted to help infiltrate the intended target's system.

**Steganography**: Embedding data within other data to conceal it. (NIST, 2020)

**Strategy:** Statement of a course of action(s) to be taken in order to execute task(s), achieve objective(s) or goal(s), fulfill mission(s), or realize end state(s) based on existing or expected resources. (DHS Lexicon, 2020)

**Substation:** Facility equipment that switches, changes, or regulates electric voltage.

**System (Electric):** Physically connected generation, transmission, and distribution facilities operated as an integrated unit under one central management or operating supervision.

**System Operator:** System operators are the "airplane pilots of the electricity grids," working at various industry control centers. They monitor and control the electricity network in real time, to maintain its integrity and regulate generating supplies to keep them balanced with customer demand. Balancing authorities, transmission operators, generator operators, and reliability coordinators are all considered system operators.

**Tactics:** Actions or plans to achieve objectives.

**Tailgating**: Also known as "piggybacking" involves an attacker gaining entry into a restricted area without proper authorization by following authorized personnel.

**Targeted Attacks**: A malicious attack targeted to a specific person, organization, system or software.

**Terrorism:** Premeditated threat or act of violence, against persons, property, environmental, or economic targets, to induce fear or to intimidate, coerce or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (DHS Lexicon, 2020)

**Transmission System (Electric):** An interconnected group of electric transmission lines and associated equipment for moving or transferring electric energy in bulk between points of supply and points at which it is transformed for delivery over the distribution system lines to consumers, or is delivered to other electric systems.

**Trigger:** 1) A set of logic statements to be applied to a data stream that produces an alert when an anomalous incident or behavior occurs 2) An event that causes the system to initiate a response. Note: Also known as triggering event. (NIST, 2020)

**Trojan Horse:** A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (NIST, 2020)

**Unified Command:** Authority structure in which the role of incident commander is shared by two or more persons, each having authority in a different responding agency. Each agency that is part of the Unified Command still maintains its own authority, responsibility, and accountability. (DHS Lexicon, 2020)

**Untargeted Attacks**: Attacks of opportunity that are not targeted at any particular person or organization. Attackers are attacking as many devices, services, organizations and people as possible.

**Vector:** An approach used to penetrate a computer system's security or propagate malicious software.

**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. (NIST, 2020)

**Vishing:** A social engineering attack in which the victim is convinced to give up information over a telephone (often involving Voice Over IP (VoIP) technology).

**Visibility:** A property of openness and accountability throughout the supply chain. (NIST, 2020)

**VoIP:** A term used to describe the transmission of packetized voice using the internet protocol (IP) and consists of both signaling and media protocols. (NIST, 2020)

**Vulnerability scans:** A technique used to identify hosts/host attributes and associated vulnerabilities. (NIST, 2020)

**War dialing:** War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

**War Driving:** The act of using a portable computer device to locate wireless network when in a moving vehicle.

**Whole Community:** Contains two main guidances: Involving people in the development of the national preparedness documents. Ensuring their roles and responsibilities are reflected in the content of the materials.

**Wi-Fi Spoofing:** Creating a WiFi network that looks and acts like a legitimate network byt is setup by an attacker for malicious purposes.

**Zero-day attack:** An attack that exploits a previously unknown hardware, firmware, or software vulnerability. (NIST, 2020)

**Zero-day exploit:** An exploit that takes advantage of a security risk on the same day that this risk becomes public.