Common Cyber Security Language

Term	Definition
Access	The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.
Accessibility	Information is available and easily usable (formatted for convenient and immediate use).
Accuracy	The closeness between an estimated result and the (unknown) true value.
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
Automatic Train Protection (ATP)	A wayside and/or on-board train system to apply emergency brakes if a signal is missed by the train operator.
Automatic Train Supervision (ATS)	Provides advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.
Black-box	A device that records information, which cannot be changed or manipulated in any manner. The information recorded is used for forensic purposes. It is used in the same sense of an aviation flight recorder.
CJIS Security Policy	The Criminal Justice Information Services (CJIS) Security Policy provides appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. The policy also provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI.
Coherence	The degree to which data that are derived from different sources or methods, but which refer to the same phenomenon, which are similar.
Commercial-off-the-Shelf (COTS)	Products that are readily available commercially and may be used “as is.”
Communications-based Train Control (CBTC)	A continuous, automatic train control system that relies on wayside data communications and/or GPS for position sensing and uses the “moving block” principle for safe train separation rather than fixed blocks with track circuits.
Comparability	The degree to which data can be compared over time and domain.
Configuration Management	A practice and process of handling hardware, software and firmware changes systematically so that a device or system maintains its integrity over time.
Consequence	The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society.
Countermeasure	Action, measure, or device intended to reduce an identified risk.
Critical infrastructure	Systems and assets, whether physical or virtual, so vital to the United States 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.
Critical Infrastructure Owners and Operators	Those entities responsible for day-to-day operation and investment of a particular-lar critical infrastructure entity. (Source: Adapted from the 2009 NIPP).
Critical Infrastructure Partner	Governmental entities, public and private sector owners and opera-tors and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation’s critical infrastructure.
Criticality	Importance to a mission or function, or continuity of operations.
Cryptography	A way to encode (hide) information such that the sender intends that only the recipient should understand the message.
Cyber Incident	An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.
Cyber System	Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services; examples include business systems, control systems, and access control systems.

Cybersecurity	The full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.
Cybersecurity (USCG-Specific)	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.
Cyclic Redundancy Check (CRC)	An error detection code used in digital networks to detect accidental changes in data during transmission or storage.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Deterrent	Measure that discourages, complicates, or delays an adversary's action or occurrence by instilling fear, doubt, or anxiety.
Electronic Security Perimeter (ESP)	Adapted from NERC-CIP electric power regulations, a logical perimeter drawn around electronic assets in a security zone to separate it from other zones.
Emergency Cutoff (blue light) system	A safety system installed at passenger stations that cuts off traction power and notifies the control center that power has been cut at this location.
Enterprise Risk Management	Comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.
Enterprise Zone	The zone of a transit agency that handles its routine internal business processes and other non-operational; non-fire, life-safety; and non-safety-critical information.
Evaluation	Process of examining, measuring and/or judging how well an entity, procedure, or action has met or is meeting stated objectives.
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity frame-work; and promote and incentivize the adoption of strong cybersecurity practices.
Fail-safe	A device that fails in a manner that protects the safety of personnel and equipment.
FedRAMP	The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Fiber-optic Strand	A portion of a cable in a fiber-optic network. Each strand carries information unique to it and is isolated from all the other strands.
Fire Life-Safety Security Zone (FLSZ)	A zone containing systems whose primary function is to warn, protect or inform in an emergency. It contains systems such as fire alarms and emergency ventilation.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Human-machine Interface (HMI)	The control interface between humans and machines.
Incident	An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyber attacks, cyber failure/accident, and other occurrences requiring an emergency response.
Information sharing	The process through which information is provided by one entity to one or more other entities to facilitate decision-making under conditions of uncertainty.
Inputs	Resources invested into the program or activity being measured, such as funds, employee-hours, or raw materials.

Interdependency	Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions.
Intrusion	An unauthorized act of bypassing the security mechanisms of a network or information system.
IPSec	A suite of protocols for securing Internet Protocol communications that authenticates and encrypts each IP packet in a communication session.
ISO 27001	A standard created by the International Standards Organization (ISO) to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)".
Loss of control	Sharing with inappropriate entities (i.e., unauthorized users) and sharing for inappropriate purposes (i.e., unauthorized uses).
Malware	Short for malicious software. Software created and used by people, usually with bad intentions to disrupt computer operations or obtain, without consent, confidential information.
Man-in-the-middle (MitM)	A type of cyber-attack where an interloper inserts him- or herself in-between two communicating devices, without either side being aware of the interloper.
Mitigation	Capabilities necessary to reduce loss of life and property by lessening the impact of disasters.
National Cyber Investigative Joint Task Force	The multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from Federal agencies, including DHS, and from State, local, and international law enforcement partners.
National Cybersecurity and Communications Integration Center	The national cyber critical infrastructure center, as designated by the Secretary of Homeland Security, which secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and SLTT entities; coordinates with international partners; and coordinates the Federal Government mitigation and recovery efforts for significant cyber and communications incidents.
Network Resilience	The ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands.
Operationally Critical Security Zone (OCSZ)	A security zone containing systems necessary for proper operation of rail transit, such as SCADA, dispatch and ATS.
Operations Control Center	A central location that monitors, and in some cases controls, some portion of a transportation system. It may handle just one system or many systems simultaneously.
Outcomes	Events, occurrences or changes in condition that indicate programmatic progress, brought about at least in part through outputs.
Outputs	Completed or delivered products or services generated through inputs.
Patch Management	A regular, coordinated method for equipment vendors to update software and firmware fixes for their digital equipment at transit agencies in a timely and responsible manner.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, etc.
Performance management	The use of performance information to affect programs, policies, or any other organization actions aimed at maximizing the benefits of public services.
Performance measurement	Regular measurement of the results (outcomes) and efficiency of services or programs.
PIV-I	PIV Interoperable (PIV-I) cards are smartcards issued by Non-Federal Issuers that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Department or Agency.
Prevention	Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism.
Processes	The steps that turn inputs into outputs.
Programmable Logic Controller (PLC)	An industrial computer used for automation of mechanical processes.

Recommended Practice	An APTA Recommended Practice represents a common viewpoint of those parties concerned with its provisions. The application of a Recommended Practice is voluntary.
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.
Recovery	Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.
Recovery	The activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.
Redundancy	Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.
Regional	Entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between critical infrastructure owners and operators, government, and other key stakeholders within the given location.
Relevance	The degree to which the product meets user needs for both coverage and content.
Residual Risk	Risk that remains after risk management measures have been implemented.
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
Risk	The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.
Risk Assessment	Product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.
Risk Avoidance	Strategies or measures taken that effectively remove exposure to a risk.
Risk Communication	Exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk.
Risk Management	The process of identifying, assessing, and responding to risk.
Risk Management	The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.
Safety Critical Security Zone	The zone that contains vital signaling, interlocking and ATP within rail transit.
Safety Critical Security Zone (SCSZ)	The zone that contains vital signaling, interlocking and ATP within rail transit.
SCADA	A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.
Secure Hash Algorithm (SHA):	A family of cryptographic hash functions used to calculate a unique sum for a digital file to be used to check for later file modifications.
SSAE 16	Statement on Standards for Attestation Engagements (SSAE) 16 reporting can help service organizations comply with Sarbanes Oxley's requirement to show effective internal controls covering financial reporting.
SSI	Sensitive Security Information (SSI) is a specific category of sensitive but unclassified (SBU) information that is governed by Federal law. SSI is information obtained or developed which, if released publicly, would be detrimental to transportation security. At TSA, the goal is to release as much information as possible publicly without compromising security.
STRIDE	Defines a Microsoft method to classify computer security threats. The acronym stands for Spoofing of an id, Tampering with data, Repudiation, Information disclosure (breach), Denial of service, and Elevation of privilege.
System	Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.
Threat	A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Timeliness	Information is current (it should be released as close as possible to the period to which the information refers).
Track Circuit	An electrical circuit designed to indicate the presence or absence of a train in a specific section of track.
Transportation Security Incident	A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. In this paragraph, the term "economic disruption" does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employee-employer dispute.
Trusted (network)	Network of an organization that is within the organization's ability to control or manage. Further, it is known that the network's integrity is intact and that no intruder is present.
Unauthorized Access	Any access to an information system or network that violates the owner or operator's stated security policy.
Uncertainty	The state of being not known, indeterminate, questionable, variable.
Vector (for cyber-attack)	The path an attacker takes to attack a network.
Virtual Private Network	A computer network in which some of the connections are virtual circuits instead of direct connections via physical wires within some larger network, such as the internet.
Vital Signaling	The portion of a railway signaling network that contains vital equipment.
Vital-programmable Logic Controller (vital-PLC)	A PLC with fail-safe functions intended for safety-critical signaling and interlocking applications in rail transit.
Vulnerability	A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
White-listing	Describes a list or register of entities that are granted certain privileges, services, mobility, access or recognition.
Wi-Fi	In the broadest sense, all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

A Note on the Common Cyber Language: The resources on this page have been submitted by the Common Language Initiative Team, a subcommittee of the Transportation Systems Sector Cyber Working Group (TSSCWG). While they represent a small fraction of the available documents and tools available to the Transportation Systems Sector, and the Cyber Security Community as a whole, they stand out to the individuals/modes of transportation that submitted them. Over time, this living document will be revisited to add/remove terminology and/or references to ensure its relevance. For questions or recommendations on the Common Language, please email CyberSecurity@tsa.dhs.gov.

Additional Resources

Website/Document Name	Cyber Security Language Resources
2013-2023 Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy	**http://trbcybersecurity.erau.edu/files/Transportation-Standards-Plan.pdf**
American Institute of Certified Public Accountants (AICPA)	http://ssae16.com/SSAE16_overview.html
Committee on National Security Systems- CNSS Instruction No. 4009- National Information Assurance (IA) Glossary	http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf
Cyber Risk and Insurance Forum (CRIF) Cyber Security Glossary	http://www.cyberriskinsuranceforum.com/content/cyber-security-glossary
Federal Bureau of Investigation (FBI)	https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center
Federal CIO Council	https://cio.gov/wp-content/uploads/downloads/2012/09/PIV_Interoperabillity_Non-Federal_Issuers_May-2009.pdf
General Services Administration (GSA)	http://www.fedramp.gov/
Glossary- McAfee for Consumer	http://home.mcafee.com/virusinfo/glossary?ctst=1#A
Glossary of Key Information Security Terms	http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Glossary- Symantec Enterprise	http://www.symantec.com/security_response/glossary/
Honeywell Industrial Cyber Security Glossary	https://www.honeywellprocess.com/en-US/online_campaigns/IndustrialCyberSecurity/Pages/glossary.html
International Standards Organization (ISO)	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
ISACA- Cybersecurity Fundamentals Glossary	http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Joint Publication 3-12®- Cyberspace Operations	http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)- Cyber Definitions	https://ccdcoe.org/cyber-definitions.html

NICCS- A Glossary of Common Cybersecurity Terminology	http://niccs.us-cert.gov/glossary
NIPP 2013- Partnering for Critical Infrastructure Security and Resilience	http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf
NIST- Framework for Improving Critical Infrastructure Cybersecurity	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
PCI Security Standards Council	https://www.pcisecuritystandards.org/security_standards/
Presidential Policy Directive- Critical Infrastructure Security and Resilience (PPD-21)	https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
Presidential Policy Directive- National Preparedness (PPD-8)	http://www.dhs.gov/presidential-policy-directive-8-national-preparedness
Radio Technical Commission for Aeronautics (RTCA)- SC-216 Aeronautical Systems Security	http://www.rtca.org/content.asp?pl=108&sl=33&contentid=82
Risk Steering Committee- DHS Risk Lexicon	http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf
Roadmap to Secure Control Systems in the Transportation Sector	https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/TransportationRoadmap20120831.pdf
SANS- Glossary of Security Terms	https://www.sans.org/security-resources/glossary-of-terms/
The University of Texas at Austin- Cyber Security Glossary Terms	http://www.utexas.edu/its/glossary/secure
The University of Texas at Austin- Identity and Cybersecurity Terms	https://identity.utexas.edu/everyone/glossary-of-identity-and-cybersecurity-terms
Transportation Security Administration	https://www.tsa.gov/sites/default/files/assets/pdf/ssi/ssi_reg_5-18-04.pdf
United States Coast Guard Cyber Strategy	https://homeport.uscg.mil/cgi-bin/st/portal/uscg_docs/MyCG/Editorial/20150706/CG_Cyber_Strategy_Final.pdf?id=0f151e6b1eb70b5aa8e5776e0e07d0c2c353f8e4&user_id=087c7ada72ee5d101ec55060bf4af6ce

Online Communities

Organization	Website
NIEM- National Information Exchange Model <REGISTRATION REQUIRED>	**https://www.niem.gov/communities/emc/Pages/emerging-communities.aspx**
NIEM- National Information Exchange Model	https://www.niem.gov/communities/emc/cyber/Pages/about-cyber.aspx