TSA Cybersecurity Lexicon (October 22, 2024)

Any person required by a TSA-issued regulation, Security Directive, or security program to apply terms as defined in the TSA Cybersecurity Lexicon is required to use the most current version of the following terms and definitions.

Term	Definition
Authorized representative	For TSA's cybersecurity requirements, an "authorized representative" is a person who is not a direct employee of the owner/operator but is authorized to act on the owner/operator's behalf to perform measures required by the security program. The term authorized representative includes agents, contractors, and subcontractors. This term does not include Managed Security Service Providers.
Business critical functions	Owner/operator's determination of capacity or capabilities to support functions necessary to meet operational needs and supply chain expectations.
Critical Cyber System	Any Information Technology or Operational Technology system used by the owner/operator that, if compromised or exploited, could result in an operational disruption incurred by the owner/operator. Critical Cyber Systems include those business support services that, if compromised or exploited, could result in operational disruption. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party.
CISA	The Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security.
Cybersecurity Architecture Design Review	A technical assessment based on government and industry-recognized standards, guidelines, and best practices that evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. These reviews must be designed to be applicable to the owner/operator's Information Technology and Operational Technology systems.
Cybersecurity incident	An occurrence that, without lawful authority, jeopardizes or is reasonably likely to jeopardize 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 on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as, malicious, suspicious, or benign).
Information technology system	Any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of an owner/operator subject to TSA's Cybersecurity Requirements to operate and/or maintain.
Interdependencies	Relationships of reliance within and among Information Technology and Operational Technology systems that must be maintained for those systems to operate and provide services.
Least privilege	Persons and programs operate using the minimum level of access, permissions, and system resources necessary to perform the function.
Managed Security Service Provider	For purposes of TSA's cybersecurity requirements, a person who is not a direct employee of the owner/operator, but who provides one or more services or capabilities that the owner/operator is using to perform measures required by the TSA. Managed Security Service Providers generally provide a logical service or capability. Managed Security Service Providers are not authorized representatives.
Memorized secret authenticator	A type of authenticator comprised of a character string intended to be memorized by, or memorable to, the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process.
Operational disruption	A deviation from or interruption of business critical functions that results from a compromise or loss of data, system availability, system reliability, or control of systems.

Operational technology system	A general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.
Phishing	Tricking individuals into disclosing sensitive information through deceptive computer-based means such as internet web sites or e-mails using social engineering or counterfeit identifying information.
Reportable cybersecurity incident	Incidents involving systems that the owner/operator has responsibility to operate and/or maintain including: a. Unauthorized access of an Information Technology or Operational Technology system; b. Discovery of malicious software that impacts the confidentiality, integrity, or availability of an Information Technology or Operational Technology system; c. Activity resulting in a denial of service to any Information Technology or Operational Technology system; and/or d. Any other cybersecurity incident that results in, or has the potential to result in, operational disruption affecting the owner/operator's Information Technology or Operational Technology systems; other aspects of the owner/operator's systems or facilities, critical infrastructure or core government functions; or national security, economic security, or public health and safety.
Security orchestration, automation, and response (SOAR)	Capabilities that enable owner/operators to collect inputs monitored by the security operations team. For example, alerts from the security information and event management system and other security technologies, where incident analysis and triage can be performed by leveraging a combination of human and machine power, help define, prioritize and drive standardized incident response activities. These capabilities allow an owner/operator to define incident analysis and response procedures in a digital workflow format.
Shared account	An account that is used by multiple individuals with a common authenticator to access systems or data. A shared account is distinct from a group account, which is a collection of user accounts that allows administrators to group similar user accounts together in order to grant them the same rights and permissions. Group accounts do not have common authenticators.
Spam	Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Tor, also known as The Onion Router	Software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. Tor software obfuscates a user's identity from anyone seeking to monitor online activity (such as nation states, surveillance organizations, information security tools). This deception is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol address of a Tor exit node, as opposed to the address of the user's computer.
Trust relationship	An agreed upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets. This term refers to trust relationships between system elements implemented by hardware, firmware, and software.
Unauthorized access	Access from an unknown source; access by a third party or former employee; an employee accessing systems for which he or she is not authorized. This term may include a non-malicious policy violation such as the use of shared credential by an employee otherwise authorized to access it.

TSA has developed this list of terms and definitions to provide a controlled vocabulary applicable to TSA's cybersecurity requirements. In general, the use of a standard lexicon reduces the possibility of misinterpretations when communicating cybersecurity definitions and terminology. As the meaning of cybersecurity terms can change over time based on emerging technology and capabilities, TSA is maintaining this list of terms and definitions separate from a specific regulation.