§ 101.615 Definitions.

Unless otherwise specified, as used in this subpart:

Approved list means an owner or operator's authoritative catalog for products that meet cybersecurity requirements.

Backup means a copy of physical or virtual files or databases stored separately for preservation and recovery. It may also refer to the process of creating a copy.

Credentials means a set of data attributes that uniquely identifies a system entity such as a person, an organization, a service, or a device, and attests to one's right to access to a particular system.

Critical Information Technology (IT) or Operational Technology (OT) systems means any Information Technology (IT) or Operational Technology (OT) system used by the vessel, facility, or OCS facility that, if compromised or exploited, could result in a transportation security incident (TSI), as determined by the Cybersecurity Officer (CySO) in the Cybersecurity Plan. Critical IT or OT systems include those business support services that, if compromised or exploited, could result in a TSI. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party.

Cyber incident means an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system, or actually jeopardizes, without lawful authority, an information system.

Cyber Incident Response Plan means a set of predetermined and documented procedures to respond to a cyber incident. It is a document that gives the owner or operator or a designated CySO instructions on how to respond to a cyber incident and pre-identifies key roles, responsibilities, and decision-makers.

Cyber threat means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term ''cyber threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cybersecurity Assessment means the appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes identification of relevant vulnerabilities and threats and determining the extent to which adverse circumstances or events could result in operational disruption and other harmful consequences.

Cybersecurity Officer, or CySO, means the person designated as responsible for the development, implementation, and maintenance of the cybersecurity portions of the Vessel Security Plan (VSP), Facility Security Plan (FSP), or Outer Continental Shelf (OCS) FSP, and for liaison with the Captain of the Port (COTP) and Company, Vessel, and Facility Security Officers. The owner or operator may designate an alternate CySO(s) to assist with the duties and responsibilities of the CySO, including during periods when the CySO is on leave, unavailable, or unable to perform their duties. Hereafter, ''CySO'' will refer to both the CySO and the alternate CySO(s), as applicable.

Cybersecurity Plan means a plan developed as a part of the VSP, FSP, or OCS FSP to ensure application and implementation of cybersecurity measures designed to protect the owners' or operators' systems and equipment, as required by this part. A Cybersecurity Plan is either included in a VSP, FSP, or OCS FSP; as an annex to a VSP, FSP, or OCS FSP; provided in a separate submission from the VSP, FSP, or OCS FSP; or addressed through an Alternative Security Program.

Cybersecurity risk means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism. It does not include any action that solely involves a

violation of a consumer term of service or a consumer licensing agreement.

Cybersecurity vulnerability means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Encryption means any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

Executable code means any object code, machine code, or other code readable by a computer when loaded into its memory and used directly by such computer to execute instructions.

Exploitable channel means any information channel (such as a portable media device and other hardware) that allows for the violation of the security policy governing the information system and is usable or detectable by subjects external to the trusted user.

Firmware means computer programs (which are stored in and executed by computer hardware) and associated data (which is also stored in the hardware) that may be dynamically written or modified during execution.

Hardware means, collectively, the equipment that makes up physical parts of a computer, including its electronic circuitry, together with keyboards, readers, scanners, and printers.

Human-Machine Interface, or HMI, means the hardware or software through which an operator interacts with a controller for industrial systems. An HMI can range from a physical control panel with buttons and indicator lights to an industrial personal computer with a color graphics display running dedicated HMI software.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software data, applications, communications, and people. It includes the application of IT, OT, or a combination of both.

Information Technology, or IT, means any equipment or interconnected system or subsystem of equipment, used in the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Known Exploited Vulnerability, or KEV, means a computer vulnerability that has been exploited in the past.

Log means a record of the events occurring within an organization's systems and networks.

Multifactor authentication means a layered approach to securing data and applications for a system that requires users to present more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Network means information system(s) implemented with a collection of interconnected components. A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. A network consists of two or more computers that are linked in order to share resources, exchange files, or allow electronic communications.

Network map means a visual representation of internal network topologies and components.

Network segmentation means a physical or virtual architectural approach that divides a network into multiple segments, each acting as its own subnetwork, to provide additional security and control that can help prevent or minimize the impact of a cyber incident.

Operational Technology, or OT, means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a change through the monitoring or control of devices, processes, and events.

Patching means updating software and operating systems to address cybersecurity vulnerabilities within a program or product.

Penetration test means a test of the security of a computer system or software application by attempting to

compromise its security and the security of an underlying operating system and network component configurations.

Principle of least privilege means that an individual should be given only those privileges that are needed to complete a task. Further, the individual's function, not identity, should control the assignment of privileges.

Privileged user means a user who is authorized (and, therefore, trusted) to perform security functions that ordinary users are not authorized to perform.

Reportable cyber incident means an incident that leads to or, if still under investigation, could reasonably lead to any of the following: Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT system; Disruption or significant adverse impact on the reporting entity's ability to engage in business operations or deliver goods or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death; Disclosure or unauthorized access directly or indirectly of nonpublic personal information of a significant number of individuals; Other potential operational disruption to critical infrastructure systems or assets; or Incidents that otherwise may lead to a transportation security incident as defined in 33 CFR 101.105.

Risk means a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and the likelihood of occurrence.

Software means a set of instructions, data, or programs used to operate a computer and execute specific tasks.

Supply chain means a system of organizations, people, activities, information, and resources for creating computer products and offering IT services to their customers.

Threat means any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system through unauthorized access, destruction, disclosure, modification of information, or denial of service.

Vulnerability means a characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Vulnerability scan means a technique used to identify hosts or host attributes and associated vulnerabilities.

§ 101.620 Owner or operator.

(a) Each owner or operator of a U.S.-flagged vessel, facility, or OCS facility is responsible for compliance with the requirements of this subpart.

(b) For each U.S.-flagged vessel, facility, or OCS facility, the owner or operator must—

(1) Ensure a Cybersecurity Plan is developed, approved, and maintained;

(2) Define in Section 1 of the Cybersecurity Plan the cybersecurity organizational structure and identify each person exercising cybersecurity duties and responsibilities within that structure, with the support needed to fulfill those obligations;

(3) Designate, in writing, by name and by title, a Cybersecurity Officer (CySO) who is accessible to the Coast Guard 24 hours a day, 7 days a week, and identify how the CySO can be contacted at any time;

(4) Ensure that cybersecurity exercises, audits, and inspections, as well as the Cybersecurity Assessment, are conducted as required by this part and in accordance with the Cybersecurity Plan (see § 101.625(d)(1), (3), (6) and (7));

(5) Ensure that the U.S.-flagged vessel, facility, or OCS facility operates in compliance with the approved Cybersecurity Plan;

(6) Ensure the development, approval, and execution of the Cyber Incident Response Plan; and

(7) For entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16–1, ensure all reportable cyber incidents are reported to the National Response Center (NRC).