U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave. SE
Washington DC 20593-7318
Staff Symbol: CG-FAC

NVIC 02-24
February 21, 2024

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-24

Subj: REPORTING BREACHES OF SECURITY, SUSPICIOUS ACTIVITY, TRANSPORTATION SECURITY INCIDENTS, AND CYBER INCIDENTS

Ref: (a) Title 33, Code of Federal Regulations, Subchapter H (Maritime Security)
(b) 46 United States Code (USC) § 70103(c)(3)(A)
(c) Title 33, Code of Federal Regulations, Part 6 (Protection and Security of Vessels, Harbors, Ports, and Waterfront Facilities
(d) National Information Sharing Environment (ISE) for Suspicious Activity Reporting, Version 1.5 (ISE-FS-200)
(e) Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) provides guidance for complying with reporting requirements for Breaches of Security (BOS), Suspicious Activity (SA), Transportation Security Incidents (TSI), and Cyber Incidents. The cyber incident guidance in this NVIC supports the reporting requirements in Part 6 of Title 33 of the Code of Federal Regulations (33 CFR Part 6) that applies to any vessel, harbor, port, or waterfront facility (hereafter referred to as MTS stakeholders). The BOS, SA, and TSI guidance in this NVIC supports the reporting requirements applicable to Maritime Transportation Security Act (MTSA)-regulated entities subject to 33 CFR Part 101.305.

2. DISCLAIMER. This NVIC is intended only to provide clarity regarding existing requirements under the law and regulation. It does not change any legal requirement and does not impose new requirements on the public. MTS stakeholders may use a different approach, if that approach satisfies applicable legal requirements (*i.e.,* this NVIC does not represent a minimum requirement for compliance).

3. BACKGROUND.

   a. Under MTSA and MTSA-implementing regulations, MTSA-regulated entities are required to report BOS, SA, and TSI to the Coast Guard. CG-5P Policy Letter 08-16 provided guidance as well as specific examples of BOS and SA, including those involving computer systems and networks, to help industry meet MTSA reporting requirements.

   b. On February 21, 2024, the Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States amended 33 CFR Part 6. Among other provisions, it added a definition for “cyber incident” and created a requirement to report evidence of an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility to the Coast Guard, the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA). The broad applicability of 33 CFR Part 6 and the new definition of a cyber incident created an overlap with existing MTSA reporting requirements. This NVIC provides clarification on the reporting requirements identified in 33 CFR Part 101 and 33 CFR Part 6.

4. DIRECTIVES AFFECTED: CG-5P Policy Letter 08-16 is hereby cancelled.

5. ACTION. U.S. Coast Guard Captains of the Port (COTP), Area Maritime Security Committees (AMSC), MTS stakeholders, and MTSA-regulated entities may use this guidance when considering BOS, SA, TSI, and cyber incident reporting. This NVIC will be distributed by electronic means only. It is available by accessing the Coast Guard Maritime Industry Cybersecurity Resource Center website.

   a. An owner or operator of a vessel, facility, or Outer Continental Shelf (OCS) facility that is required to maintain an approved security plan in accordance with MTSA (i.e., MTSA-regulated entities) and its implementing regulations in 33 CFR Parts 104, 105, or 106 of Reference (a) shall, without delay, report activities that may result in a TSI to the National Response Center (NRC), including BOS or SA as required by 33 CFR Part 101.305. The purpose of this requirement is to provide the Coast Guard opportunity to understand and respond to potential or actual threats to the port area upon receipt of an NRC report, and to assess the adequacy of security plans to prevent a TSI. Additionally, IAW Reference (b), the security plan shall "be consistent with the requirements of the National Transportation Security Plan and Area Maritime Transportation Security Plans." The COTP will affirm consistency to help ensure alignment of BOS and SA communication procedures within FSPs throughout their area of responsibility.

   b. Evidence of sabotage, subversive activity, or an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility, including any data, information, network, program, system, or other digital infrastructure thereon or therein, shall be reported immediately to the FBI, CISA, and to the COTP, or to their respective representatives, in accordance with section 6.16-1 of Reference (c). The purpose of this requirement is to provide the FBI, CISA, and Coast Guard the opportunity to understand and respond to potential or actual threats to the MTS upon receipt of a report, and determine appropriate actions.

   c. The maritime industry continues to expand its use of networked technology, which creates efficiencies but also increases threats and vulnerabilities to MTS stakeholders and MTSA-regulated entities through telecommunications equipment, computers, and networks. Due to the increasing reliance on telecommunications equipment, computers, and networked systems for controlling physical operations, a growing portion of all security risks has a network or computer nexus. Maintaining the security of these systems, including reporting cyber incidents, is vital to maintaining the security of the MTS.

   d. Plausible terrorist attack scenarios include combined cyber and physical incidents. MTS stakeholders, including those that are MTSA-regulated, should consider this possibility when evaluating a security incident, including the possibility that a cyber incident is a precursor to a physical attack, or that cyber related BOS and SA may be an attempt by actors to identify weaknesses or to plan for later attacks.

e. The target and intent of malicious cyber activity can be difficult to discern. The fact that business and administrative systems may be connected to operational, industrial control and security systems further complicates this matter. The Coast Guard strongly encourages MTS stakeholders to minimize, monitor, mitigate, and wherever possible, eliminate any such connections.

f. The U.S. Coast Guard handles all reports of security incidents as Sensitive Security Information (SSI), in accordance with 49 CFR part 1520, which includes requirements for proper information marking and storage. The information is therefore not subject to routine public disclosure. The U.S. Coast Guard will share the information with other agencies on a need to know basis and in accordance with applicable laws and policies.

6. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The Office of Environmental Management, Commandant (CG-47) reviewed this NVIC and the general policies contained within, and determined that this policy falls under the Department of Homeland Security (DHS) categorical exclusion A3. This NVIC will not result in any substantial change to existing environmental conditions or violation of any applicable federal, state, or local laws relating to the protection of the environment. It is the responsibility of the action proponent to evaluate all future specific actions resulting from this policy for compliance with the National Environmental Policy Act (NEPA), other applicable environmental requirements, and the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 (series).

b. This NVIC will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policy in this NVIC must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Department of Homeland Security (DHS) and Coast Guard NEPA policy, and compliance with all other applicable environmental mandates.

7. RECORDS MANAGEMENT CONSIDERATIONS. This NVIC has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not create significant or substantial change to existing records management requirements.

8. FORMS/REPORTS. None.

9. DISCLAIMER. This policy is not a substitute for applicable legal requirements, nor is itself a rule. It provides operational guidance for U.S. Coast Guard personnel and the maritime

industry. It does not impose legally binding requirements on any party outside of the U.S. Coast Guard.

10. QUESTIONS. Questions concerning this policy should be directed to the U.S. Coast Guard Office of Port and Facility Compliance (CG-FAC) at portfacilitycyber@uscg.mil.

W.R

W. R. Arguin
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Prevention Policy

Encl: (1) MTS Stakeholder and MTSA-Regulated Entity Reporting Guidance
(2) Glossary of Terms

ENCLOSURE (1) TO NAVIGATION AND VESSEL INSPECTION CIRCULAR 02-24

MTS Stakeholder and MTSA-Regulated Entity Reporting Guidance

1. DISCUSSION. The following criteria describe U.S. Coast Guard requirements and amplifying guidance for reporting BOS, SA, TSI, and cyber incidents. No description could cover all possible incidents and events. When in doubt about whether a situation meets the reporting criteria, affected entities should make a report as described in 33 CFR 101.305 and 33 CFR 6.16-1, as applicable.

   a. Cyber Incident

      (1) **This section applies to MTS stakeholders (any vessel, harbor, port, or waterfront facility).**

      (2) Reference (c), as amended by Reference (e), defines a cyber incident as an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

      (3) Based on the broad definition, for the purposes of reporting to the U.S. Coast Guard, MTS stakeholders should report those incidents that lead to or, if still under investigation, could reasonably lead to any of the following:

         (a) A substantial loss of confidentiality, integrity, or availability of information systems, networks, or operational technology;

         (b) A disruption or significant adverse impact on the MTS Stakeholder’s or MTSA-regulated entity’s ability to engage in business operations or deliver goods, or services;

         (c) Disclosure or unauthorized access directly or indirectly to non-public personal information; or

         (d) Potential operational disruption to other critical infrastructure systems or assets.

      (4) Note that routine spam, phishing attempts, and other nuisance events that do not breach a system's defenses may not need to be reported as cyber incidents. Similarly, accidental violations of acceptable use policies, such as plugging in an unauthorized USB drive, is not considered a reportable cyber incident. Such occurrences, however, should be monitored for unusual activity such as escalation of efforts, and may be considered suspicious activities whose reporting is detailed in the next section.

      (5) The Coast Guard recognizes that the cyber domain includes countless malicious but low-level events that are normally addressed via standard anti-virus programs and similar protocols. MTS stakeholders should report events that are out of the ordinary in terms of sophistication, volume, or other factors which, from the operator's perspective, raise suspicions and may result in a TSI.

b. Breach of Security (BOS)

(1) This section applies to MTSA-regulated entities.

(2) Reference (a) defines a BOS as, "an incident that has not resulted in a TSI, in which security measures have been circumvented, eluded, or violated." For purposes of this guidance, this definition includes a breach of telecommunications equipment, computer, and network system security measures where those systems conduct or support functions described in Vessel Security Plans (VSPs), or Facility Security Plans (FSPs), or where successful defeat or exploitation of the systems could result or contribute to a TSI.

(3) BOS incidents may include, but are not limited to, any of the following:

(a) Unauthorized access to restricted or secure areas, as indicated in the VSP, or FSP;

(b) Unauthorized circumvention of security measures, including host and network defenses performing access control;

(c) Intrusion into telecommunications equipment, computer, and networked systems having a connection to security plan functions (for example, access control, cargo control, monitoring), unauthorized root or administrator access to security and industrial control systems, successful phishing attempts or malicious insider activity that could allow outside entities access to internal IT systems that are linked to the MTS, or those that could otherwise result in a TSI; or

(d) Instances of viruses, Trojan Horses, worms, zombies or other malicious software that have a widespread impact or adversely affect the information or operational technology of one or more on-site mission critical servers that are linked to security functions or could otherwise result in a TSI; or

(e) Any denial of service attacks that adversely affect or degrade access to critical services that are linked to security functions or could otherwise result in a TSI.

(4) Note that routine spam, phishing attempts, and other nuisance events that do not breach a system's defenses are not considered a BOS. Such occurrences, however, should be monitored for unusual activity such as escalation of efforts, and may be considered suspicious activities whose reporting is detailed in the next section.

c. Suspicious Activity (SA)

(1) This section applies to MTSA-regulated entities.

(2) Reference (a) describes SA as "an activity that may result in a TSI." Reference (d) defines SA as, "observed behavior reasonably indicative of pre-operational planning related to terrorism or criminal activity."

(3) SA may include, but is not limited to, any of the following:

(a) Unfamiliar persons in areas that are restricted to regular employees;

(b) Unauthorized personnel accessing IT spaces.

(c) Potentially dangerous devices found by screeners prior to loading persons or cargo or items found on or near the facility that seem out of place.

(d) Vehicles parked or standing for excessive amounts of time near the facility perimeter;

(e) Unusual behavioral patterns, such as:

  i. Walking slowly in a deliberate fashion towards a potential target;

  ii. Inappropriately dressed (for example, wearing excessive clothing as to conceal something, or looking out of place);

  iii. Not responding to verbal interaction;

  iv. Excessive nervousness or “doomsday” talk;

  v. Excessive questions;

  vi. Lack of photo identification;

  vii. Agitation or rage;

  viii. Picture taking, especially if the suspect has been asked earlier not to take photos;

  ix. Note taking or drawing;

  x. Taking measurements; or

  xi. Attempting to access unauthorized areas.

(f) Unauthorized Unmanned Aircraft System (UAS) activity including, but not limited to:

  i. Reconnaissance and surveillance activities, indicated by repeated activities at a particular place and time (for example, fly-overs, hovering at low altitudes, and prolonged time on station); or

  ii. Testing of facility security protocols using UAS, indicated by flying by a target, moving into sensitive areas, and observing the reaction of security personnel (for example, the time it takes to respond to an incident or the routes taken to a specific location).

(g) Cybersecurity related SA and nuisance events present additional vulnerabilities, and stakeholders should distinguish untargeted cyber incidents from targeted incidents on computer related systems. Persistent scanning of networks, SPAM e-mail, and similar unsophisticated events could be part of the normal information technology landscape, but should be monitored for signs of escalation or as part of larger malicious efforts.

(h) In contrast, targeted incidents may be large, sustained attacks on important cyber systems in an apparent attempt to exploit them for nefarious purposes. Spear phishing campaigns, a marked increase in network scanning, or other attacks may be considered SA if the volume, persistence, or sophistication of the attacks is out of the ordinary.

(i) Unsuccessful but apparently targeted incidents may be SA if they threaten systems that could contribute to a TSI, have a link to the MTSA-regulated portion of the facility or are otherwise related to systems, personnel, and procedures addressed by security plans or MTSA requirements.

d. Transportation Security Incident (TSI)

(1) This section applies to MTSA-regulated entities.

(2) Reference (a) defines TSI as “a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area”.

(3) Cyber incidents that clearly target or otherwise affect business or administrative systems, even without directly affecting operational technology or industrial control systems, that result in a transportation system disruption or economic disruption may still be considered a TSI depending on the potential or resulting impact.

e. Reporting Procedures

(1) BOS or SA

(a) MTSA-regulated entities must report a BOS or SA to the National Response Center (NRC), without delay, at 1-800-424-8802. MTSA-regulated entities may also make reports directly to the local COTP; however, this does not relieve an owner or operator from the requirement to notify the NRC in accordance with 33 CFR part 101.305.

(b) MTS stakeholders (any vessel, harbor, port, or waterfront facility) are encouraged to report activities that may result in a transportation security incident to the National Response Center.

(2) TSI

(a) MTSA entities regulated under 33 CFR Part 104 or 105 shall, without delay, report a TSI to the local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center.

(b) MTSA entities regulated under 33 CFR Part 106 shall, without delay, report a TSI to their cognizant District Commander and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center.

(3) Cyber Incidents

(a) Unless otherwise reported as a BOS, SA, or TSI per reference (a), reports of sabotage, subversive activity, or actual or threatened cyber incidents must be made to the FBI, CISA, and COTP, or their respective representatives, per reference (c).

(b) **For the purposes of cyber incident reporting in accordance with Reference (c), a notification to the NRC is recommended and, if it is confirmed that**

the resulting NRC report will be or has been sent to the relevant COTP, the submission of a separate report to the COTP is not necessary.

(4) When reporting security incidents, owners and operators should be prepared to provide the following information:

(a) Reporting source information;

(b) Incident location, including physical address;

(c) Type of facility, vessel, port, or harbor; and

(d) Brief summary of activity and its impact or potential consequence(s).

(5) The purpose of reporting is to promote security, and in some cases it may therefore be appropriate for an organization to provide only the most basic information to the NRC, COTP, FBI, CISA, and other organizations with a need to know. The details of any security vulnerabilities revealed by the event need not be discussed during an initial report. The Coast Guard will work with the reporting source and with other appropriate authorities to assess and respond to the report.

(6) Prohibited Items List: As part of the Cruise Ship Terminal Screening Program, 33 CFR § 105.515 provides regulations pertaining to a Prohibited Items List (PIL). The PIL consists of dangerous substances and devices that the Coast Guard prohibits onboard any cruise ship through terminal screening operations. The owner or operator of a cruise ship terminal must obtain the PIL from the Coast Guard and the list must be present at each screening location during screening operations. If any of the prohibited items are found by screeners during the security screening, then that incident would be classified as "SA." However, if any of the prohibited items are found after security screening procedures by facility personnel, then security measures were circumvented and that incident would be classified as a "BoS".

(7) Unauthorized UAS Activity: All unauthorized UAS activity over a MTSA-regulated facility or vessel should be closely observed, documented and reported to local law enforcement and to the NRC as SA. If the UAS lands or crashes on or into a regulated facility or vessel, the incident shall be considered a BoS. Both types of incidents (SA and BoS) shall be reported to the NRC. The Coast Guard highly recommends that the Facility Security Officer (FSO) or the Vessel Security Officer (VSO) also report the incident to local law enforcement if the UAS is not following Federal Aviation Administration (FAA) enforceable regulations. Before reporting the incident, review FAA regulations to make sure there is a violation. In some cases, flying a UAS over a MTSA-regulated facility or vessel is not in violation of FAA regulations. FSOs/VSOs can report the violation(s) to the FAA at https://www.faa.gov/uas/contact_us/report_uas_sighting.

f. Other Critical Infrastructure and Cyber Incident Resources

(1) The U.S. Coast Guard has established Marine Transportation System Cyber Specialists in each COTP, District, and Area Office. These members are available to further aid in the coordination of efforts to improve cyber resiliency in the MTS.

To learn more about these Cyber Specialists, contact your local Coast Guard COTP. A port directory can be found on the Coast Guard's Homeport website.

(2) The local U.S. Coast Guard COTP may request assistance from U.S. Coast Guard cyber specialists and U.S. Coast Guard Cyber Command (CGCYBER). CGCYBER provides operational cyber prevention and response capabilities through the Cyber Protection Teams (CPT) and the Maritime Cyber Readiness Branch (MCRB). In the event of a cyber incident, upon official request, CGCYBER can provide support to Sector Commanders and other units in evaluating technical matters relating to cyber reports, their potential impact on the MTS, and whether an incident reaches the threshold of a BOS or SA. The CGCYBER 24x7 watch can be reached at (202) 372-2904 or CyberWatch@uscg.mil. To promote clear communications, this NVIC includes a glossary of common cyber terms. Additional cyber-related information can be found on the Coast Guard's Maritime Industry Cybersecurity Resource Center website.

(3) In addition to the reporting requirements of 33 CFR 101.305 and 33 CFR 6.16-1, MTS stakeholders and MTSA-regulated entities may be subject to additional reporting requirements issued by other agencies such as the Cybersecurity and Infrastructure Security Agency (CISA).

(a) CISA Central is CISA's hub for tracking threats and emerging risks to our nation's critical infrastructure. They are a resource for critical infrastructure partners and stakeholders to engage with CISA. CISA Central can be reached 24x7 at report@cisa.gov or (888) 282-0870.

(b) CISA Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with United States Computer Emergency Readiness Team (US-CERT). CISA offers a wide range of free products and services to support the ICS community's cybersecurity security risk management efforts. A full list of service offerings with additional details for each service can be found at CISA's Security Offerings. ICS-CERT has also published best practices that can be found at the ICS Recommended Practices website.

(4) The FBI InfraGard program provides members of the critical infrastructure community a means to share information to prevent, protect, and defend against hostile acts against Critical Infrastructure and Key Resources.

(5) The National Suspicious Activity Reporting (SAR) Initiative provides information and resources related to SA reporting. The SAR Initiative is a joint collaborative effort by DHS, the FBI, and state, local, tribal and territorial law enforcement partners. Note that this is a source of information, not a reporting center.

(6) The U.S. Coast Guard encourages MTS stakeholders and MTSA-regulated entities to participate in their local AMSC. These committees are the best place to collaborate with colleagues at the port level for security and information sharing, including the resources, services and capabilities of other federal, state, local and private sector partners. To learn more about the AMSC, contact your local Coast Guard COTP.

#

ENCLOSURE (2) TO NAVIGATION AND VESSEL INSPECTION CIRCULAR 02-24

Glossary of Terms

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.

Cyber Incident — An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Cybersecurity — The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

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.

Cyber Threat — 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 via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Industrial Control System (ICS) — An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. ICSs include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.

Information System — 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 in the application of information and operational technologies.

Intrusion — Any set of actions that attempts to compromise the integrity, confidentiality, or availability of a resource.

Intrusion Detection Systems (IDS) — A security service that monitors and analyzes network or system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Malicious Cyber Activity — Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

Malware — Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

MTS Stakeholders — Vessels, harbors, ports, and waterfront facilities, including MTSA-regulated entities.

Network Defense — The programs, activities, and the use of tools necessary to facilitate them conducted on a computer, network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users for the primary purpose of protecting 1) that computer, network, or system; 2) data stored on, processed on, or transiting that computer, network, or system; or 3) physical and virtual infrastructure controlled by that computer, network, or system. Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners.

Phishing — Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Spear Phising — Highly targeted phishing attack, targeted at an individual by including key information about them.

Suspicious Activity — Observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

Threat — An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. Note: The specific causes of asset loss, and for which the consequences of asset loss are assessed, can arise from a variety of conditions and events related to adversity, typically referred to as disruptions, hazards, or threats. Regardless of the specific term used, the basis of asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions.

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.

Unauthorized Access — A person gains logical or physical access without permission to a network, system, application, data, or other resource.

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 email programs to spread itself to other computers, or even erase everything on a hard disk.

Worm — A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Zombie — A program that is installed on a system to cause it to attack other systems.