Glossary

Active Directory: Microsoft's Active Directory (AD) is a centralized directory framework for the administration of network devices and users, including user identity management and authentication services. AD utilizes the Lightweight Directory Access Protocol (LDAP) along with domain and authentication services.

Advanced Persistent Threat: The Advanced Persistent Threat (APT) refers to a class of cyber threat designed to infiltrate a network, remain persistent through evasion and propagation techniques. APTs are typically used to establish and maintain an external command and control channel through which the attacker can continuously exfiltrate data.

Anti-virus: Anti-virus (AV) systems inspect network and/or file content for indications of infection by malware. Signature-based AV works by comparing file contents against a library of defined code signatures; if there is a match the file is typically quarantined to prevent infection, at which point the option to clean the file maybe available.

Application Monitor / Application Data Monitor: An application content monitoring system that functions much like an intrusion detection system, only performing deep inspection of a session rather than of a packet, so that application contents can be examined at all layers of the OSI model, from low level protocols through application documents, attachments, and so on. Application Monitoring is useful for examining industrial network protocols for malicious content (malware).

Application Whitelisting: Application Whitelisting (AW) is a form of whitelisting intended to control which executable files (applications) are allowed to operate. AW systems typically work by first establishing the "whitelist" of allowed applications, after which point any attempt to execute code will be compared against that list. If the application is not allowed, it will be prevented from executing. AW often operates at low levels within the kernel of the host operating system.

APT: See **Advanced Persistent Threat**.

Asset: An asset is any device used within an industrial network.

Attack Surface: The attack surface of a system or asset refers to the collectively exposed portions of that system or asset. A large attack surface means that there are many exposed areas that an attack could target, while a small attack surface means that the target is relatively unexposed.

Attack Vector: An attack vector is the direction(s) through which an attack occurs, often referring to specific vulnerabilities that are used by an attacker at any given stage of an attack.

auditd: Auditd is the auditing component of the Linux Auditing System, responsible for writing audit events to disk. The Linux Auditing System is a useful tool for monitoring file access and file integrity in Linux systems.

AV: See **Anti-virus**.

AWL: See **Application Whitelisting**.

Backchannel: A backchannel typically refers to a communications channel that is hidden or operates "in the background" to avoid detection, but is also used in reference to hidden or covert communications occurring back toward the originating sender, that is, malware hidden in the return traffic of a bidirectional communication.

Blacklisting (see "**Whitelisting**"): Blacklisting refers to the technique of defining known malicious behavior, content, code, and so on. Blacklists are typically used for threat detection, comparing network traffic, files, users, or some other quantifiable metric against a

relevant blacklist. For example, an intrusion prevention system (IPS) will compare the contents of network packets against blacklists of known malware, indicators of exploits, and other threats so that offending traffic (i.e. packets that match a signature within the blacklist) can be blocked.

CDA: See **Critical Digital Asset**.

CFATS: The Chemical Facility Anti-Terrorism Standard, established by the US Department of Homeland Security to protect the manufacture, storage, and distribution of potentially hazardous chemicals.

Compensating Controls: The term "compensating controls" is typically used within regulatory standards or guidelines to indicate when an alternative method than those specifically addressed by the standard or guideline is used.

Control Center: A control center typically refers to an operations center where a control system is managed. Control centers typically consist of SCADA and HMI systems that provide interaction with industrial/automated processes.

Correlated Event: A correlated event is a larger pattern match consisting of two or more regular logs or events, as detected by an event correlation system. For example, a combination of a network scan event (as reported by a firewall) followed by an injection attempt against an open port (as reported by an IPS) can be correlated together into a larger incident; in this example, an attempted reconnaissance and exploit. Correlated events may be very simple or very complex, and can be used to detect a wide variety of more sophisticated attack indicators.

Critical Cyber Asset: A critical cyber asset is a cyber asset that is itself responsible for performing a critical function, or directly impacts an asset that performs a critical function. The term "critical cyber asset" is used heavily within NERC reliability standards for Critical Infrastructure Protection.

Critical Digital Asset: A "critical digital asset" is a digitally connected asset that is itself responsible for performing a critical function, or directly impacts an asset that performs a critical function. The term "critical digital asset" is used heavily within NRC regulations and guidance documents. Also see: **Critical Cyber Asset**.

Critical Infrastructure: Any infrastructure whose disruption could have severe impact on a nation or society. In the United States, Critical Infrastructures are defined by the Homeland Security Presidential Directive Seven as: Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Critical Manufacturing; Dams; Defense Industrial Base; Drinking Water and Water Treatment Systems; Emergency Services; Energy; Government Facilities; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials, and Waste; Postal and Shipping; Public Health and Healthcare; Telecommunications; and Transportation Systems.

Cyber Asset: A digitally connected asset; that is, an asset that is connected to a routable network or a Host. The term Cyber Asset is used within the NERC reliability standards, which defines a Cyber Asset as any Asset connected to a routable network within a control system; any Asset connected to a routable network outside of the control system; and/or any Asset reachable via dial-up.[1]

DAM: See **Database Activity Monitor**.

Data Diode: A data diode is a "one-way" data communication device, often consisting of a physical-layer unidirectional limitation. Using only 1/2 of a fiber optic "transmit/receive" pair would enforce unidirectional communication at the physical layer, while proper configuration of a network firewall could logically enforce unidirectional communication at the network layer.

Database Activity Monitor: A Database Activity Monitor (DAM) monitors database transactions, including SQL, DML, and other database commands and queries. A DAM may be network- or host-based. Network-based DAMs monitor database transactions by decoding and interpreting network traffic, while host-based DAMs provide system-level auditing directly from the database server. DAMs can be used for indications of malicious intent (e.g. SQL injection attacks), fraud (e.g. the manipulation of stored data), and/or as a means of logging data access for systems that do not or cannot produce auditable logs.

Database Monitor: See **Database Activity Monitor**

DCS: See **Distributed Control System**.

Deep-Packet Inspection: The process of inspecting a network packet all the way to the application layer (Layer 7) of the OSI model. That is, past datalink, network or session headers to inspect all the way into the payload of the packet. Deep-packet inspection is used by most intrusion detection and prevention systems (IDS/IPS), newer firewalls, and other security devices.

Distributed Control System: An industrial control system deployed and controlled in a distributed manner, such that various distributed control systems or processes are controlled individually. See also: **Industrial Control System**.

DPI: See **Deep Packet Inspection**.

Electronic Security Perimeter: An Electronic Security Perimeter (ESP) refers to the demarcation point between a secured enclave, such as a control system, and a less trusted network, such as a business network. The ESP typically includes those devices that secure that demarcation point, including firewalls, IDS, IPS, industrial protocol filters, application monitors, and similar devices.

Enclave: A logical grouping of assets, systems and/or services that defines and contains one (or more) functional groups. Enclaves represent network "zones" that can be used to isolate certain functions in order to more effectively secure them.

Enumeration: Enumeration is the process of identifying valid identities of devices and users in a network; typically as an initial step in a network attack process. Enumeration allows an attacker to identify valid systems and/or accounts that can then be targeted for exploitation or compromise.

ESP: See **Electronic Security Perimeter**.

EtherNet/IP: EtherNet/IP is a real-time Ethernet protocol supporting the Common Industrial Protocol (CIP), for use in industrial control systems.

Event: An event is a generic term referring to any datapoint of interest, typically alerts that are generated by security devices, logs produced by systems and applications, alerts produced by network monitors, and so on.

finger: The finger command is a network tool that provides detailed information about a user.

Function Code: Function Codes refer to various numeric identifiers used within industrial network protocols for command and control purposes. For example, a function code may represent a request from a Master device to a Slave device(s), such as a request to read a register value, to write a register value, or to restart the device.

HIDS: Host IDS. A Host Intrusion Detection System, which detects intrusion attempts via a software agent running on a specific host. A HIDS detects intrusions by inspecting packets and matching the contents against defined patterns or "signatures" that indicate malicious content, and produce an alert.

HIPS: Host IPS. A Host Intrusion Prevention System, which detects and prevents intrusion attempts via a software agent running on a specific host. Like a HIDS, a HIPS detects

intrusions by inspecting packets and matching the contents against defined patterns or "signatures" that indicate malicious content. Unlike a HIDS, a HIPS is able to perform active prevention by dropping the offending packet(s), resetting TCP/IP connections, or other actions in addition to passive alerting and logging actions.

HMI: A human–machine interface (HMI) is the user interface to the processes of an industrial control system. An HMI effectively translates the communications to and from PLCs, RTUs, and other industrial assets to a human-readable interface, which is used by control systems operators to manage and monitor processes.

Homeland Security Presidential Directive Seven: The United States Homeland Security Presidential Directive Seven (HSPD-7) defines the 18 critical infrastructures within the United States, as well as the governing authorities responsible for their security.

Host: A host is a computer connected to a network, that is, a Cyber Asset. The term differs from an Asset in that hosts typically refer to computers connected to a routable network using the TCP/IP stack—that is, most computers running a modern operating system and/or specialized network servers and equipment—while an Asset refers to a broader range of digitally connected devices, and a Cyber Asset refers to any Asset that is connected to a routable network.[2]

HSPD-7: See **Homeland Security Presidential Directive Seven**.

IACS: Industrial Automation Control System. See **Industrial Control System**.

IAM: See **Identity Access Management**.

ICCP: See **Inter Control Center Protocol**.

ICS: See **Industrial Control System**

Identity Access Management: Identity access management refers to the process of managing user identities and user accounts, as well as related user access and authentication activities within a network, and a category of products designed to centralize and automate those functions.

IDS: Intrusion Detection System. Intrusion detection systems perform deep-packet inspection and pattern matching to compare network packets against known "signatures" of malware or other malicious activity in order to detect a possible network intrusion. IDS operates passively by monitoring networks either in-line or on a tap or span port, and providing security alerts or events to a network operator.

IEC: See **International Electrotechnical Commission**.

IED: See **Intelligent Electronic Device**.

Industrial Control System: An industrial control system (ICS) refers to the systems, devices, networks, and controls used to operate and/or automate an industrial process. See also: **Distributed Control System**.

Intelligent Electronic Device: An intelligent electronic device (IED) is an electronic component (such as a regulator and circuit control) that has a microprocessor and is able to communicate, typically digitally using fieldbus, real-time Ethernet, or other industrial protocols.

Inter-Control Center Protocol: The Inter-Control Center Protocol (ICCP) is a real-time industrial network protocol designed for wide-area intercommunication between two or more control centers. ICCP is an internationally recognized standard published by the International Electrotechnical Commission (IEC) as IEC 60870-6. ICCP is also referred to as the Telecontrol Application Service Element-2 or TASE.2.

International Electrotechnical Commission: The International Electrotechnical Commission (IEC) is an international standards organization that develops standards for the purposes of consensus and conformity among international technology developers, vendors, and users.

International Standards Organization: The International Standards Organization (ISO) is a network of standards organizations from over 160 countries, which develops and publishes standards covering a wide range of topics.

IPS: Intrusion Prevention System. Intrusion protection systems perform the same detection functions of an IDS, with the added capability to block traffic. Traffic can typically be blocked by dropping the offending packet(s), or by forcing a reset of the offending TCP/IP session. IPS works in-line, and therefore may introduce latency.

ISO: See **International Standards Organization**.

LDAP: See **Lightweight Directory Access Protocol**.

Lightweight Directory Access Protocol: The Lightweight Directory Access Protocol (LDAP) is a standard published under IETF RFC 4510, which defines a standard process for accessing and utilizing network-based directories. LDAP is used by a variety of directories and IAM systems.

Log: A log is a file used to record activities or events, generated by a variety of devices, including computer operating systems, applications, network switches and routers, and virtually any computing device. There is no standard for the common format or structure of a log.

Log Management: Log management is the process of collecting and storing logs for purposes of log analysis and data forensics, and/or for purposes of regulatory compliance and accountability. Log management typically involves collection of logs, some degree of normalization or categorization, and short-term (for analysis) and long-term storage (for compliance).

Log Management system: A system or appliance designed to simplify and/or automate the process of log management. See also: **Log Management**.

Master Station: A master station is the controlling asset or host involved in an industrial protocol communication session. The master station is typically responsible for timing, synchronization, and command and control aspects of an industrial network protocol.

Metasploit: Metasploit is a commercial exploit package, used for penetration testing.

Modbus: Modbus is the Modicon Bus protocol, used for intercommunication between industrial control assets. Modbus is a flexible master/slave command and control protocol available in several variants including Modbus ASCII, Modbus RTU, Modbus TCP/IP, and Modbus Plus.

Modbus ASCII: A Modbus variant that uses ASCII characters rather than binary data representation.

Modbus Plus: A Modbus extension that operates at higher speeds, which remains proprietary to Shneider Electric.

Modbus RTU: A Modbus variant that uses binary data representation.

Modbus TCP: A Modbus variant that operates over TCP/IP.

NAC: See **Network Access Control**.

NEI: The Nuclear Energy Institute is an organization dedicated to and governed by the United States nuclear utility companies.

NERC: See **North American Electric Reliability Corporation**.

NERC CIP: The North American Electric Reliability Corporation reliability standard for Critical Infrastructure Protection.

Network Access Control: Network Access Control (NAC) provides measures of controlling access to the network, using technologies, such as 802.1X (port network access control), to require authentication for a network port to be enabled, or other access control methods.

Network Whitelisting: (see "**Whitelisting**")

NIDS: Network IDS. A network intrusion detection system detects intrusion attempts via a network interface card, which connects to the network either in-line or via a span or tap port.

NIPS: Network IPS. A network intrusion prevention detection system detects and prevents intrusion attempts via a network-attached device using two or more network interface cards to support inbound and outbound network traffic, with optional bypass interfaces to preserve network reliability in the event of a NIPS failure.

NIST: The National Institute of Standards and Technology. NIST is a nonregulatory federal agency within the United States Department of Commerce, whose mission is to promote innovation through the advancement of science, technology, and standards. NIST provides numerous research documents and recommendations (the "Special Publication 800 series") around information technology security.

nmap: Nmap or "Network Mapper" is a popular network scanner distributed under GNU General Public License GPL-2 by nmap.org.

North American Electric Reliability Corporation: The North American Electric Reliability Corporation is an organization that develops and enforces reliability standards for and monitors the activities of the bulk electric power grid in North America.

NRC: See **Nuclear Regulatory Commission**.

Nuclear Regulatory Commission: The United States Nuclear Regulatory Commission (NRC) is a five-member Presidentially appointed commission responsible for the safe use of radioactive materials including but not limited to nuclear energy, nuclear fuels, radioactive waste management, and the medical use of radioactive materials.

OSSIM: OSSIM is an Open Source Security Information Management project, whose source code is distributed under GNU General Public License GPL-2 by AlienVault.

Outstation: An outstation is the DNP3 slave or remote device. The term outstation is also used more generically as a remote SCADA system, typically interconnected with central SCADA systems by a Wide Area Network.

PCS: Process Control System. See **Industrial Control System**.

Pen test: A Penetration Test. A method for determining the risk to a network by attempting to penetrate its defenses. Pentesting combines vulnerability assessment techniques with evasion techniques and other attack methods to simulate a "real attack."

PLC: See **Programmable Logic Controller**.

Process Control System: See **Industrial Control System**.

Profibus: Profibus is an industrial fieldbus protocol defined by IEC standard 61158/IEC 61784-1.

Profinet: Profinet is an implementation of Profibus designed to operate in real time over Ethernet.

Programmable Logic Controller: A programmable logic controller (PLC) is an industrial device that uses input and output relays in combination with programmable logic in order to build an automated control loop. PLCs commonly use Ladder Logic to read inputs, compare values against defined set points, and (potentially) write to outputs.

Project Aurora: A research project that demonstrated how a cyber-attack could result in the explosion of a generator.

RBPS: Risk Based Performance Standards are recommendations for meeting the security controls required by the Chemical Facility Anti-Terrorism Standard (CFATS), written by DHS.

Red Network: A "red network" typically refers to a trusted network, in contrast to a "black network," which is less secured. When discussing unidirectional communications in critical networks, traffic is typically only allowed outward from the red network to the black network, to allow supervisory data originating from critical assets to be collected and utilized by less secure SCADA systems. In other use cases, such as data integrity and fraud prevention, traffic may only be allowed from the black network into the red network, to prevent access to classified data once they have been stored.

Remote Terminal Unit: A remote terminal unit (RTU) is a device combining remote communication capabilities with programmable logic for the control of processes in remote locations.

RTU: See **Remote Terminal Unit**.

SCADA: See **Supervisory Control and Data Acquisition**.

SCADA-IDS: SCADA aware Intrusion Detection System. An IDS designed for use in SCADA and ICS networks. SCADA-IDS devices support pattern matching against the specific protocols and services used in control systems, such as Modbus, ICCP, DNP3, and others. SCADS-IDS is passive, and is therefore suitable for deployment within a control system, as it does not introduce any risk to control system reliability.

SCADA-IPS: SCADA aware Intrusion Prevention System. An IPS system designed for use in SCADA and ICS networks. SCADA-IPS devices support pattern matching against the specific protocols and services used in control systems, such as Modbus, ICCP, DNP3, and others. SCADA-IPS is active and can block or blacklist traffic, making it most suitable for use at control system perimeters. SCADA-IPS is not typically deployed within a control system for fear of a false-positive disrupting normal control system operations.

Security Information and Event Management: Security information and event management (SIEM) combines security information management (SIM or log management) with security event management (SEM) to provide a common centralized system for managing network threats and all associated information and context.

SERCOS III: SERCOS III is the latest version of the Serial Realtime Communications System, a real-time Ethernet implementation of the popular SERCOS fieldbus protocols.

Set Points: Set points are defined values signifying a target metric against which programmable logic can operate. For example, a set point may define a high temperature range, or the optimum pressure of a container, and so on. By comparing set points against sensory input, automated controls can be established. For example, if the temperate in a furnace reaches the set point for the maximum temperature ceiling, reduce the flow of fuel to the burner.

SIEM: See **Security Information and Event Management**.

Situational Awareness: Situational Awareness is a term used by the National Institute of Standards and Technology (NIST) and others to indicate a desired state of awareness within a network in order to identify and respond to network-based attacks. The term is a derivative of the military command and control process of perceiving a threat, comprehending it, making a decision and taking an action in order to maintain the security of the environment. Situational Awareness in network security can be obtained through network and security monitoring (perception), alert notifications (comprehension), security threat analysis (decision making), and remediation (taking action).

Smart-listing: A term referring to the use of blacklisting and whitelisting technologies in conjunction with a centralized intelligence system, such as a SIEM in order to dynamically adapt common blacklists in response to observed security event activities. See also: **Whitelisting** and **Blacklisting**.

Stuxnet: An advanced cyber-attack against an industrial control system, consisting of multiple zero-day exploits used for the delivery of malware that then targeted and infected specific industrial controls for the purposes of sabotaging an automated process. Stuxnet is widely regarded as the first cyber-attack to specifically target an industrial control system.

Supervisory Control And Data Acquisition: Supervisory Control and Data Acquisition (SCADA) refers to the systems and networks that communicate with industrial control systems to provide data to operators for supervisory purposes, as well as control capabilities for process management.

TASE.1: See **Telecontrol Application Service Element-1**.

TASE.2: See **Telecontrol Application Service Element-2**.

Technical Feasibility/Technical Feasibility Exception (TFE): The term "Technical Feasibility" is used in the NERC CIP reliability standard and other compliance controls to indicate where a required control can be reasonably implemented. Where the implementation of a required control is not technically feasible, a Technical Feasibility Exception can be documented. In most cases, a TFE must detail how a compensating control is used in place of the control deemed to not be feasible.

Telecontrol Application Service Element-1: The initial communication standard used by the ICCP protocol. Superseded by **Telecontrol Application Service Element-2**.

Telecontrol Application Service Element-2: The Telecontrol Application Service Element-2 standard or TASE.2 refers to the ICCP protocol. See also: **Inter Control Center Protocol**.

Unidirectional Gateway: A network gateway device that only allows communication in one direction, such as a Data Diode. See also: **Data Diode**.

User Whitelisting: The process of establishing a "whitelist" of known valid user identities and/or accounts, for the purpose of detecting and/or preventing rogue user activities. See also: **Application Whitelisting**.

VA: See **Vulnerability Assessment**.

Vulnerability: A vulnerability refers to a weakness in a system that can be utilized by an attacker to damage the system, obtain unauthorized access, execute arbitrary code, or otherwise exploit the system.

Vulnerability Assessment: The process of scanning networks to find hosts or assets, and probing those hosts to determine vulnerabilities. Vulnerability assessment can be automated using a vulnerability assessment scanner, which will typically examine a host to determine the version of the operating system and all running applications, which can then be compared against a repository of known software vulnerabilities to determine where patches should be applied.

Whitelists: Whitelists refer to defined lists of "known good" items: users, network addresses, applications, and so on, typically for the purpose of exception-based security where any item not explicitly defined as "known good" results in a remediation action (e.g. alert and block). Whitelists contrast blacklists, which define "known bad" items.

Whitelisting: Whitelisting refers to the act of comparing an item against a list of approved items for the purpose of assessing whether it is allowed or should be blocked. Typically referred to in the context of Application Whitelisting, which prevents unauthorized applications from executing on a host by comparing all applications against a whitelist of authorized applications.

Zone: A zone refers to a logical boundary or enclave containing assets of like function and/or criticality, for the purposes of facilitating the security of common systems and services. See also: **Enclave**.

ENDNOTES

1. North American Reliability Corporation. Standard CIP-002-4 - Cyber Security - Critical Cyber Asset Identification. [document on the Internet]. February 3, 2011 [cited 2011 March 3] Available from: http://www.nerc.com/files/CIP-002-4.pdf.
2. Ibid.