WORKSHOP GLOSSARY OF TERMS:

App: a web application, accessed over the Internet, for a mobile device (e.g., smartphone, tablet) that works much like user-installed software on a computer allowing the device to perform specific tasks.

Authentication: The process to verify that someone is who they claim to be when they try to access a computer or online service.

Backing up: To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.

Bandwidth: also called "data transfer rate," the amount of data that can be carried online from one point to another in a given time period, usually expressed in bits (of data) per second (bps) or bytes per second (Bps). Dial-up Internet accounts, which use a standard telephone line to connect to an Internet Service Provider (ISP), have a very narrow bandwidth (about 50 Kbps or 50,000 bits per second) and take a long time to download data. A broadband Internet account can move data at anywhere from 128 Kbps to 2,000 Kbps or more and can download large files, such as video files, much faster.

Blog: from "web log," a regularly updated personal journal, conversation, commentary, or news forum on virtually any topic that is published on the Web and may include text, hypertext, images, and links; typically displayed in reverse chronological order, blog posts invite comments from readers creating online communities of individuals with shared interests over time; updating a blog is "blogging," someone who keeps a blog is a "blogger," and blog entries are called "posts."

Botnet: a network of private computers, each of which is called a "bot," infected with malicious software (malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes; computers are typically infected when users open up an infected attachment or visit an infected website.

Bring Your Own Device (BYOD): The authorized use of personally owned mobile devices such as smartphones or tablets in the workplace.

Browser: short for Web browser, a software application that locates, retrieves, and displays information resources on the World Wide Web. An information resource is identified by a URL (Uniform Resource Locator), and may be a web page, image, video,

or other piece of content. Popular browsers include Microsoft Internet Explorer, Firefox, Google Chrome, and Apple Safari.

Byte: a unit of digital information commonly consisting of eight "bits" (a binary unit and the smallest increment of computer data) used as a measurement of computer memory size and storage capacity (usually in terms of MBs or "megabytes," and GBs or "gigabytes"). Bits and bit rates (bits over time, as in bits per second [bps]) are also commonly used to describe connection speeds. (See bandwidth.)

Category: The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."

Client: A piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

Cloud computing: a technology that uses the Internet and remote servers to maintain data and applications, allowing users to access applications without installation and access to their personal files from any computer with Internet access; centralizes storage, memory, processing, and bandwidth; examples include Yahoo email or Gmail with the software managed by the cloud service providers Yahoo and Google.

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 cybersecurity, national economic security, national public health or safety, or any combination of those matters.

Computer virus: a software program that is designed to replicate itself, spread from one computer to another, and interfere with computer operation; a computer virus may corrupt or delete data on a user's computer, use an email program to spread itself to other computers, or even erase everything on a user's hard disk. Computer viruses can be spread by attachments in email messages or instant messaging messages; disguised as attachments of images, greeting cards, or audio and video files, and hidden in illicit software or programs that are downloaded to a computer.

Computer actions:

* ***Clicking***—to tap on a mouse button, press it down, and immediate releasing it; to click on means to select a computer screen object by moving the mouse pointer to the object's position and clicking a mouse button; some operations require a double click, clicking a mouse button twice in rapid succession.
* ***Downloading***—the transmission of a file from one computer system to another; to download a file is to request it from one computer (or from a Web page) and to receive it on another computer. Uploading is the transmission of a file in the other direction, from one computer to another.

* ***Posting***—to publish a message in an online forum, such as a blog, or newsgroup; a post is a message published in an online forum or newsgroup.
* ***Logon***—also called logging in or on, the process used to get access to an operating system or application; most logon procedures require a user to have a user ID and a password.

Content management system: a software system that allows website publishing, editing, content storage and modification, database management, and site maintenance from a central Web page; allows multiple users with little knowledge of web programming or markup languages may collaborate to create and manage website content with relative ease.

Cookie: also referred to as an "HTTP cookie," is a small text file that contains a unique ID tag placed on the user's computer by a Web site to track pages visited on the site and other information; "tracking cookies" and "third-party tracking cookies" are used to compile long-term records of individuals' browsing histories.

CPU: the central processing unit, the "brain" of the computer, is the hardware within a computer system that carries out the instructions of a computer program by performing the basic arithmetic, logic, and other operations of the system; on personal computers, the CPU is housed in a single chip called a "microprocessor."

Cyberbullying: bullying that takes place using electronic technology, including the Internet, and related technologies to harm other people, in a deliberate, repeated, and hostile manner; may involve text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, Web sites, or fake profiles.

Cybersecurity: The process of protecting information by preventing, detecting, and responding to attacks.

Cybersecurity Event: A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). Cyberstalking—a criminal offense that involves using the Internet or other technology to stalk or harass an individual, a group of individuals, or an organization; it may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, or harassment.

Cyberspace: the global network of interdependent information technology infrastructures, telecommunications networks, and computer processing systems; a metaphor for describing the non-physical terrain created by computer systems, it has come to mean anything associated with the Internet and the diverse Internet culture.

Detect (NIST Function): Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Denial of Service Attack: type of online computer attack designed to deprive user or groups of users normally accessible online services; generally involves effort by hackers to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Digital: term commonly used in computing and electronics, describes any system in which data is converted to binary numeric form as in digital audio and digital photography; computers are digital machines because at their most basic level they can distinguish between just two values, 0 and 1, or off and on. All data that a computer processes must be encoded digitally as a series of zeroes and ones. The opposite of digital is analog; a typical analog device is a clock in which the hands move continuously around the face.

Digital Signature: an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document; can also be used to ensure that the original content of the message or document that has been sent is unchanged; often used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

DMZL: Segment of a network where servers accessed by less trusted users are isolated. The name is derived from the term “demilitarised zone”.

Domain Name System (DNS): a database system that translates Internet domain and host names to IP addresses; DNS automatically converts the name typed into a Web browser address bar to the IP addresses of Web servers hosting those sites.

Emai: short for electronic mail, the transmission of digital messages over. communications networks, including the Internet; consists of three components: the message envelope, the message header, and the message body.

Encryption: the conversion of digital information into a format unreadable to anyone except those possessing a “key” through which the encrypted information is converted back into its original form (decryption), making it readable again.

File Sharing: The practice of distributing or providing access to digital media, such as computer programs, multimedia (audio, images and video), documents or electronic books. File sharing may be achieved in a number of ways. Common methods of storage, transmission and dispersion include manual sharing utilizing removable media, centralized servers on computer networks, World Wide Web-based hyperlinked documents, and the use of distributed peer-to-peer networking.

Firewall: software or hardware that, after checking information coming into a computer from the Internet or an external network, either blocks the transmission or allows it to pass through, depending on the pre-set firewall settings, preventing access by hackers and malicious software ; often offered through computer operating systems.

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.”

Framework Core: A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes.

The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

Function: One of the main components of the NIST Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.

Geotagging: the process of adding geographical location, or label, to photographs, videos, website, SMS messages, QR Codes, or RSS feeds; a geotag usually consists of latitude and longitude coordinates, altitude, distance, place names, and other details about the origin of the media being tagged helping users find a variety of online location-specific information.

Global Positioning System (GPS): Space-based satellite navigation system that provides positioning, navigation, and timing/distance information; maintained by the United States government and freely accessible to anyone with a GPS receiver.
Hacker – Someone who seeks and exploits weaknesses in a computer system or computer network.

Hardware: specifically, computer hardware, is the collection of physical elements that comprise a computer system, including a CPU, monitor, keyboard, hard disk, and printer. In contrast, software (specifically, computer software) is a collection of computer programs, procedures, algorithms, and its documentation that provides instructions for telling a computer what to do and how to do it.

Hashtag: words or phrases prefixed with the symbol # (the pound sign); used to mark keywords or topics in a Tweet or social networking service.

Hyperlink: an element in an electronic document that links to another place in the same document or to an entirely different document; typically, you click on the hyperlink to follow the link. Hypertext is text with hyperlinks.

HTML: HyperText Markup Language is the main markup language for displaying web pages and other information that can be displayed in a web browser; HTML elements, which form the building blocks of all Web sites, consist of tags enclosed in angle brackets (e.g.,); browsers do not display the HTML tags, which provide instructions about the appearance and content of the page, but use the tags to interpret the content of the page.

HTTP: Hypertext Transfer Protocol, the foundation of data communication for the World Wide Web, defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when an URL is entered into a browser, an HTTP command is sent to the Web server directing it to retrieve and transmit the requested Web page.

HTTPS: Hypertext Transfer Protocol Secure, provides secure communication over a network, such as the Internet; basically layers additional security measures over HTTP; used by financial and online commerce Web sites to ensure the security of private information.

Identify (NIST Function): Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

IP Address: a unique identifier in the form of a numerical label assigned to each device, such as a personal computer or server, participating in a network, such as the Internet.

Intellectual property: usually governed by patent, trademark, and copyright law, a set of rights that are recognized for owners of various property (e.g., machines, musical, literary and artistic works, discoveries and inventions, and applications); applicability to digital realm is hotly contested area of the law.

Internet: a worldwide collection of computer networks that use the standard Internet Protocol Suite to serve billions of users interconnected by a broad array of electronic, wireless, and optical networking technologies; the Internet carries an extensive range of information resources and services, including inter-linked hypertext documents of the World Wide Web and the infrastructure to support email.

Internet Service Provider (ISP): an organization, usually a private business, that provides personal and business computers access to the Internet; users usually pay a monthly fee to an ISP for this service.

Keylogger: also called keylogging and keystroke logging, is the action of tracking (or logging) the keys struck on a computer keyboard; usually runs hidden in the background and automatically records all keystrokes so that users are unaware of its presence and that their actions are being monitored.

Keyword: in computer programming, a word or identifier that has a particular meaning to the programming language; also a term that captures the essence of the topic of a document used by a search engine to retrieve online documents related to that term or terms.

Laptop: a personal computer for mobile use that integrates most of the typical components of a desktop computer (i.e., display, keyboard, touchpad); sometimes called notebook computers, notebooks, or netbooks.

Local Area Network (LAN): Communications network linking multiple computers within a defined location such as an office building.

Malware: short for malicious software, software that disrupts or damages a computer's operation, gathers sensitive or private information, or gains access to private computer systems; may include botnets, viruses, worms, Trojans, keyloggers, spyware, adware, and rootkits.

* ***Botnet***—a network of private computers, each of which is called a "bot," infected with malicious software (malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes.
* ***Virus***—type of malware that has a reproductive capacity to transfer itself from one computer to another spreading infections between online devices.

* ***Worm***—type of malware that replicates itself over and over within a computer.
* ***Trojan***—type of malware that gives an unauthorized user access to a computer.
* ***Spyware***—type of malware that quietly sends information about a user's browsing and computing habits back to a server that gathers and saves data.
* ***Adware***—type of malware that allows popup ads on a computer system, ultimately taking over a user's Internet browsing.
* ***Rootkit***—a type of malware that opens a permanent "back door" into a computer system; once installed, a rootkit will allow more and more viruses to infect a computer as various hackers find the vulnerable computer exposed and attack.

Mobile device: also called a handheld, handheld device, or handheld computer, a pint-sized computer device, typically having a display screen with touch input or a miniature keyboard; most common types are smartphones, PDA, pagers, and personal navigation devices.

Modem: an electronic device that converts a computer's digital signals into specific frequencies to travel over telephone or cable television lines; computers use modems to communicate with one another over a network; often used to link home computers to the Internet through an Internet Service Provider.

Network: also called a computer network, is a collection of computers interconnected by communication channels that allow sharing of resources (hardware, data, and software) and information; most common is the local area network or LAN, anywhere from a few computers in a small office to several thousand computer spread through dozens of buildings; a wide area network or WAN connects computers across multiple geographic locations, even on different continents.

NIST Framework: The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. The Framework was prepared by the National Institute of Standards and Technology (NIST).

Online gaming: any type of game played through the Internet, over a computer network, or on a video game console (e.g., Xbox 360 and Playstation 3); usually refers to video games played over the Internet, where multiple players are in different geographic locations.

Open source software: software often developed and distributed to users at no cost in a public, collaborative manner; permits users to study, change, improve, and at times also distribute the software.

Operating system: a set of software or software platform on top of which other programs, called application programs, can run.

Personal computer (PC): any general-purpose computer whose size, capabilities, and cost make it useful for individuals; PC software applications include, but are not limited to, word processing, spreadsheets, databases, databases, Web browsers, email, and games; may be a desktop computer, laptop, table, or a handheld PC. The term PC has been traditionally used to describe an "IBM-compatible" personal computer, in contrast to an Apple Macintosh computer.

Phishing: sending emails that attempt to fraudulently acquire personal information, such as usernames, passwords, social security numbers, and credit card numbers, by masquerading as a trustworthy entity, such as a popular social website, financial site, or online payment processor; often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Platform: A platform is an underlying computer system on which application programs can run. On personal computers, Windows 2000 and the Mac OS X are examples of two different platforms.

Plug-ins: sometimes called add-ons, are software modules that add functionality to an application; commonly used in web browsers to play video, scan for viruses, and display new file types; well-known plug-in examples include Adobe Flash Player, QuickTime, and Microsoft Silverlight.

Point of Sale (POS) System: A computerized network operated by a main computer and linked to several checkout terminals. A retail point of sale system typically includes a cash register (which in recent times comprises a computer, monitor, cash drawer, receipt printer, customer display and a barcode scanner) and the majority of retail POS systems also include a debit/credit card reader.

Pop-ups: or pop-up ads, are a form of online advertising on the World Wide Web intended to attract web traffic or capture email addresses; created by advertisers, pop-ups generally appear unexpectedly in a small web browser window when a user is linking to a new Web site.

Pop-up blockers: a web browser feature, software, or application that allows users to limit or block pop-up ads; users may often set the preferred level of blocking, from total blocking to minimal blocking.

Protect (NIST Function): Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (NIST 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.

Respond (NIST Function): Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Management: The process of identifying, assessing, and responding to risk.

Router: A networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. The most familiar type of routers are home and small office routers that simply pass data, such as web pages, email, IM, and videos between the home computers and the Internet.

RSS: Really Simple Syndication is a family of web feed formats used to publish frequently updated works, such as blog entries, news headlines, audio, and video—in a standardized format; users subscribe to RSS feeds, which automatically send favorite content to users who have signed up for the feeds.

Search engine: program that searches documents for specified keywords and returns a list of the documents where the keywords were found; often used to describe systems, including Google, Bing, and Yahoo! Search that enable users to search for documents on the World Wide Web.

Security software: a generic term referring to any computer program that secures a computer system or computer network; the two main types of security software are virus protection software and software that removes adware and spyware (both require regular updating to remain effective).

Server: a computer program or physical computer that services other computers over a local network or the Internet; network servers typically are configured with additional processing, memory, and storage capacity; specific to the Web, a Web server is a computer program (housed in a computer) that serves requested HTML pages or files.

SMTP: Simple Mail Transfer Protocol is a protocol for sending e-email messages between servers.

Smart phone: handheld device built on a mobile computing platform that features, typically, a digital camera, video camera, Global Positioning System (GPS), e-mail, and all the features of a standard cell phone; usually equipped with a high-definition, touch pad screen and miniature keyboard, smartphone allows downloading of apps for a wide range of uses.

Social networking: using Internet-based tools that allow people to listen, interact, engage, and collaborate with each other; popular social networking platforms include Facebook, MySpace, YouTube, LinkedIn, and Twitter.

Software: specifically, computer software, is a collection of computer programs, procedures, algorithms, and its documentation that provides instructions for telling a computer what to do and how to do it. In contrast, hardware (specifically, computer hardware) is the collection of physical elements that comprise a computer system, including a CPU, monitor, keyboard, hard disk, and printer.

Spam: the use of electronic messaging systems to send unsolicited bulk messages (usually advertising or other irrelevant posts) to large lists of email addresses indiscriminately.

Spyware: a type of malware (malicious software) installed on computers that collects information about users without their knowledge; can collect Internet surfing habits, user logins and passwords, bank or credit account information, and other data entered into a computer; often difficult to remove, it can also change a computer's configuration resulting in slow Internet connection speeds, a surge in pop-up advertisements, and un-authorized changes in browser settings or functionality of other software.

SQL: structured query language, a special-purpose programming language designed for managing data in relational database management systems.

Subcategory: The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."

Syncing: the process of copying all electronic files and folders from one device to another (e.g., from a smartphone to a personal computer) through an Internet connection.

Tablet Computer: a kind of mobile computer, larger than a mobile phone or personal digital assistant, usually having a flat touchscreen or pen-enabled interface.
Twitter—an online social networking service that enables users to send and read text-based posts of up to 140 characters, known as "tweets."

Two-Factor Authentication: A security tool that uses multiple verification techniques to prove that the person attempting to log onto an account is really them. Also referred to as two-step or multi-factor verification, or 2FA.

URL: the Uniform Resource Locator is the global address of documents and other resources on the World Wide Web; a URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer or server on the Internet, and a pathname, a hierarchical description that specifies the location of a file on that computer or server.

USB Flash Drive: also called a jump drive or thumb drive, is a data storage device that is typically removable (plugged into a USB/Universal Serial Bus port on a personal computer) and rewritable, and physically much smaller than a floppy disk.

USB Port: Universal Serial Bus port, a single, standardized way to connect devices (modems, printers, scanners, digital cameras, etc.) to a personal computer.

Virtual Private Network (VPN): Links between computers or local area networks across different locations using a wide area network that cannot access or be accessed by other users of the wide area network.

Virus: Malware that is loaded onto a computer and then run without the user's knowledge or knowledge of its full effects.

Voice chat: a modern form of communication using the Internet through services such as Skype, Yahoo! Messenger, AOL Instant Messenger, or Windows Live Messenger.

VoIP: Voice over Internet Protocol, a technology that allows voice calls using a broadband Internet connection instead of a regular (or analog) phone line.
Vulnerability -- A flaw or weakness that can be used to attack a system or organization.

Wi-Fi: a technology that allows an electronic device (personal computer, video game console, smartphone, tablet, digital audio player) to exchange data wirelessly (using radio waves) over a computer network.

Wi-Fi Hotspot: a wireless access point to the Internet or other computer network over a wireless local area network through the use of a router connected to a link to an Internet service provider; frequently found in coffee shops and other public establishments, a hotspot usually offers Internet access within a range of about 65 feet (20 meters) indoors and a greater range outdoors; many smartphones provide built-in ability to establish a Wi-Fi hotspot.

Webcam: a video camera that feeds images in real time to a computer or computer network; can be used to establish video links permitting computers to act as videophones or videoconference stations; also used for security surveillance, video broadcasting, and social videos (such as many viewed on YouTube).

Worm: Malware that replicates itself so it can spread to infiltrate other computers.
WWW—the World Wide Web (commonly known as "the Web" or the "Information Superhighway"), a vast collection of linked files accessed over the Internet using a protocol called HTTP (Hypertext Transfer Protocol); the system supports documents specially formatted in a markup language called HTML (Hyper Text Markup Language) that supports links to other documents, as well as graphics, audio, and video files. With an Internet "web browser," one can view "web pages" that may contain text, images, video, and other multimedia, and "navigate" between them via "hyperlinks." World Wide Web is not synonymous with the Internet. The WWW is just one of many applications of the Internet and computer networks.

Web server: computer hardware and software that runs a website and is always connected to the Internet; using HTTP (Hypertext Transfer Protocol), a Web server delivers Web pages to browsers and other data files to Web-based applications; every Web server has an IP address and often a domain name.

Website: a collection of specially formatted, related Web files (or pages) on a particular subject or organization that are stored on a computer known as a web server and accessible through a network such as the Internet; include a beginning file called a home page; a web page can contain any type of content, including text, color, graphics, animation, and sound.

ZIP: a file format used for data compression and archiving; a zip file contains one or more files that have been compressed to make file size considerably smaller than the original file; the zipped version of files have a .zip file extension; can significantly reduce e-mail transmission time and save on storage space.

ACRONYMS:

BYOD Bring Your Own Device

CBBB Council of Better Business Bureaus

CCS Council on CyberSecurity

COBIT Control Objectives for Information and Related Technology

DCS Distributed Control System

DHS Department of Homeland Security

EO Executive Order

FCC Federal Communications Commission

FTC Federal Trade Commission

ICS Industrial Control Systems

IEC International Electrotechnical Commission

IR Interagency Report

IDS Intrusion Detection System

IPS Intrusion Prevention System

ISA International Society of Automation

ISAC Information Sharing and Analysis Center

ISO International Organization for Standardization

ISP Internet Service Provider

IT Information Technology

LAN Local Area Network

NCSA National Cyber Security Alliance

NIST National Institute of Standards and Technology

POS Point of Sale

RFI Request for Information

RMP Risk Management Process

SCADA Supervisory Control and Data Acquisition

SP Special Publication

SQL Structured Query Language

VPN Virtual Private Network

Council of Better Business Bureaus, Inc.
3033 Wilson Blvd.
Suite 600
Arlington, VA 22201
bbb.org