Appendix C: Glossary

Administrator privileges: Allow computer system-access to resources that are unavailable to most users. Administrator privileges permit execution of actions that would otherwise be restricted. *Source: NSA/CSS Confidence in Cyber Space*

Air-gapped environment: Security measure that isolates a secure network from unsecure networks physically, electrically, and electromagnetically. *Source: FFIEC Joint Statement - Destructive Malware*

Anomalous activity: The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. *Source: NIST: SP 800-94*

Antivirus/Antimalware software: A program that monitors a computer or network to identify all types of malware and prevent or contain malware incidents. *Source: NIST Guide to Malware Incident Prevention and Handling for Desktops and Laptops*

Asset: In computer security, a major application, general-support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems. *Source: NIST: CNSSI-4009*

Attack signature: A specific sequence of events indicative of an unauthorized access attempt. *Source: NIST: SP 800-12*

Authentication: The process of verifying the identity of an individual user, machine, software component, or any other entity. *Source: FFIEC Information Security Booklet*

Baseline configuration: A set of specifications for a system, or configuration item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and that can be changed only through change-control procedures. The baseline configuration is used as a basis for future builds, releases, or changes. *Source: NIST: SP 800-128*

Black holing: A method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. *Source: NCCIC/US-CERT DDoS Quick Guide*

Border router: A device located at the organization's boundary to an external network. *Source: NIST: SP 800-41*

Buffer overflow: A condition at an interface under which more input can be placed into a buffer or data-holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of a system. *Source: NISTIR 7298 Revision 2*

Business continuity: The ability to maintain operations and services—both technology and business—in the event of a disruption to normal operations and services. Ensures that any impact or disruption of services is within a documented and acceptable recovery time period and that system or operations are resumed at a documented and acceptable point in the processing cycle. *Source: FFIEC IT Examination Handbook Glossary*

Change management: The broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing, and implementation. *Source: FFIEC Operations Booklet*

CHIPS: A private-sector U.S.-dollar funds-transfer system, clearing and settling cross-border and domestic payments. *Source: CHIPS*

Cloud computing: Generally a migration from owned resources to shared resources in which client users receive information technology services on demand from third-party service providers via the Internet "cloud." In cloud environments, a client or customer relocate their resources—such as data, applications, and services—to computing facilities outside the corporate firewall, which the end user then accesses via the Internet. *Source: FFIEC Statement on Outsourced Cloud Computing*

Crisis management: The process of managing an institution's operations in response to an emergency or event that threatens business continuity. An institution's ability to communicate with employees, customers, and the media, using various communications devices and methods, is a key component of crisis management. *Source: FFIEC Business Continuity Planning Booklet*

Critical system [infrastructure]: The systems and assets, whether physical or virtual, that are so vital that the incapacity or destruction of such may have a debilitating impact. *Source: NICCS Glossary*

Cyber attack: Attempts to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information. *Source: FFIEC IT Examination Handbook Glossary*

Cyber event: A cybersecurity change or occurrence that may have an impact on organizational operations (including mission, capabilities, or reputation). *Source: NIST Cybersecurity Framework*

Cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein. *Source: NIST: CNSSI-4009*

Cyber threat: An internal or external circumstance, event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. *Source: NICCS Glossary*

Cybersecurity: The process of protecting consumer and bank information by preventing, detecting, and responding to attacks. *Source: Derived from NIST Cybersecurity Framework*

Data classification program: A program that categorizes data to convey required safeguards for information confidentiality, integrity, and availability; establishes controls required based on value and level of sensitivity. *Source: Derived from SANS Institute InfoSec Reading Room*

Database: A collection of data that is stored on any type of computer storage medium and may be used for more than one purpose. *Source: FFIEC IT Examination Handbook Glossary*

Data loss prevention (DLP): A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter. *Source: NSA/CSS Securing Data and Handling Spillage Events*

Data mining: The process or techniques used to analyze large sets of existing information to discover previously unrevealed patterns or correlations. *Source: NICCS Glossary*

Deep packet inspection: The capability to analyze network traffic to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations. *Source: NIST Guide to Intrusion Detection and Prevention Systems*

Defense-in-depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. *Source: NIST: CNSSI-4009*

Digital certificate: The electronic equivalent of an ID card that authenticates the originator of a digital signature. *Source: FFIEC IT Examination Handbook Glossary*

Disaster recovery plan: A plan that describes the process to recover from major processing interruptions. *Source: FFIEC IT Examination Handbook Glossary*

Distributed denial of service (DDoS): A type of attack that makes a computer resource or resources unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of the concerted efforts of a group that intends to affect an institution's reputation by preventing an Internet site, service, or application from functioning efficiently. *Source: FFIEC IT Examination Handbook Glossary*

Domain Name System Security Extensions (DNSSEC): A technology that was developed to, among other things, protect against such attacks by digitally 'signing' data so you can be assured it is valid. *Source: ICANN*

Encryption: A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appear as meaningless strings of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key. *Source: FFIEC IT Examination Handbook Glossary*

End of life: All software products have life cycles. End of life refers to the date when a software development company no longer provides automatic fixes, updates, or online technical assistance for the product. *Source: US-CERT alert TA-14-310A*

End-point security: Security controls that validate the security compliance of the client system that is attempting to use the SSL VPN. Endpoint security controls also include security protection mechanisms, such as Web browser cache cleaners, that remove sensitive information from client systems. *Source: NIST: SP 800-113*

Enterprise network: The configuration of computer systems within an organization. Includes local area networks (LAN), wide area networks (WAN), bridges, and applications. *Source: FFIEC IT Examination Handbook Glossary*

Enterprise-wide: An entire organization, rather than a single line of business or function. *Source: FFIEC IT Examination Handbook Glossary*

Exploit: A technique or code that uses a vulnerability to provide system access to the attacker. An exploit is an intentional attack to impact an operating system or application program. *Source: FFIEC IT Examination Handbook Glossary*

External connections: An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. *Source: NIST: SP 800-53*

FTP (file transfer protocol): A standard high-level protocol for transferring files from one computer to another, usually implemented as an application level program. *Source: National Telecommunications and Information Administration*

Financial Services Information Sharing and Analysis Center (FS-ISAC): A nonprofit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. *Source: Derived from FS-ISAC*

Firewall: Hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side. *Source: FFIEC IT Examination Handbook Glossary*

Frame relay: A high-performance WAN protocol that operates at the physical and data link layers of the open systems interconnect (OSI) reference model. Frame relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. Frame relay uses existing T1 and T3 lines and provides connection speeds from 56 Kbps to T1. *Source: FFIEC IT Examination Handbook Glossary*

Gap analysis: A comparison that identifies the difference between actual and desired outcomes. *Source: FFIEC IT Examination Handbook Glossary*

Governance: In computer security, the setting of clear expectations for the conduct (behaviors and actions) of the entity being governed and directing, controlling, and strongly influencing the entity to achieve these expectations. Governance includes specifying a framework for decision making, with assigned decision rights and accountability, intended to consistently produce desired behaviors and actions. *Source: FFIEC IT Examination Handbook Glossary*

Hypervisor: A piece of software that provides abstraction of all physical resources (such as central processing units, memory, network, and storage) and thus enables multiple computing stacks (consisting of an operating system, middleware and application programs) called virtual machines to be run on a single physical host. *Source: NIST SP 800-125a Draft*

Incident response plan: A plan that defines the action steps, involved resources, and communication strategy upon identifying a threat or potential threat event, such as a breach in security protocol, power or telecommunications outage, severe weather, or workplace violence. *Source: FFIEC IT Examination Handbook Glossary*

Information security: The result of any system of policies or procedures for identifying, controlling, and protecting information from unauthorized disclosure. Also, the processes by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations. *Source: FFIEC IT Examination Handbook Glossary*

Information systems: Electronic and paper-based systems. Electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems can include networks (computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems. Other examples are backup tapes, portable computers, personal digital assistants, media such as compact disks, micro drives, and diskettes, and media used in software development and testing. *Source: FFIEC Information Security Booklet*

Infrastructure: Systems technologies, including operations such as central computer processing, distributed processing, end-user computing, local area networking, and telecommunications. Includes the transmission media (e.g., voice, data, and video), routers, aggregators, repeaters, and other devices that control transmission paths; also includes the software used to send, receive, and manage transmitted signals. These operations often represent critical services to financial institutions and their customers. *Source: Based on FFIEC IT Examination Handbook Glossary*

Internet service provider (ISP): A company that provides its customers with access to the Internet (e.g., AT&T, Verizon, CenturyLink). *Source: FFIEC IT Examination Handbook Glossary*

Intrusion detection system (IDS): Software and hardware that detect and log inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses sensors to monitor packets on the network to which it is attached. *Source: FFIEC IT Examination Handbook Glossary*

Intrusion prevention systems (IPS): A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target. *Source: NISTIR 7298 Revision 2*

Life-cycle process: The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system. *Source: NIST System Development Life Cycle*

Malware: Designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs. *Source: FFIEC IT Examination Handbook Glossary*

Man-in-the-middle attack (MITM): Places the attacker's computer in the communication line between the server and the client. The attacker's machine can monitor and change communications. *Source: FFIEC IT Examination Handbook Glossary*

Metrics: A quantitative measurement. *Source: FFIEC IT Examination Handbook Glossary*

Mobile device: A portable computing and communications device with information-storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices. *Source: NISTIR 7298 Revision 2*

Multifactor authentication: The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric). *Source: NISTIR 7298 Revision 2*

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards; developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures. *Source: NIST*

Network: Two or more computer systems grouped together to share information, software, and hardware. *Source: FFIEC IT Examination Handbook Glossary*

Network activity baseline: A base for determining typical utilization patterns so that significant deviations can be detected. *Source: NIST: SP 800-61*

Network administrator: An individual responsible for the installation, management, and control of a network. *Source: FFIEC IT Examination Handbook Glossary*

Network diagram: A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or arrangement of a network, including its nodes and connecting communication lines. *Source: FFIEC IT Examination Handbook Glossary*

Operating system: A system that supports and manages software applications. Operating systems allocate system resources, provide access and security controls, maintain file

systems, and manage communications between end users and hardware devices. *Source: FFIEC IT Examination Handbook Glossary*

Outsourcing: The practice of contracting with another entity to perform services that might otherwise be conducted in-house. Contracted relationship with a third party to provide services, systems, or support. *Source: FFIEC IT Examination Handbook Glossary*

Patch: Software code that replaces or updates other code frequently to correct security flaws. *Source: FFIEC IT Examination Handbook Glossary*

Penetration test: The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others. *Source: FFIEC IT Examination Handbook Glossary*

Person-to-Person payments: Online payments using electronic messaging invoke a transfer of value between the parties over existing proprietary networks as "on-us" transactions. *Source: FFIEC IT Examination Handbook Glossary*

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—e-mail to request information from users or direct them to fake Web sites that request information. *Source: NIST: SP 800-83*

Principles of least privilege: The security objective of granting users only the access needed to perform official duties. *Source: NISTIR 7298 Revision 2*

Privileged access: Individuals with the ability to override system or application controls. *Source: FFIEC Information Security Booklet*

Real-time network monitoring: Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access. *Source: NISTIR 7298 Revision 2*

Red team: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The red team's objective is to improve enterprise information assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders in an operational environment. *Source: NIST: CNSSI-4009*

Remote access: The ability to obtain access to a computer or network from a remote location. *Source: FFIEC IT Examination Handbook Glossary*

Remote deposit captures (RDC): A service that enables users at remote locations to scan digital images of checks and transmit the captured data to a financial institution or a merchant that is a customer of a financial institution. *Source: FFIEC IT Examination Handbook Glossary*

Removable media: Portable electronic storage media, such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device and which is used to store text, video, audio, and image information. Such devices have no independent

processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar storage devices. *Source: NIST: CNSSI-4009*

Resilience: The ability of an organization to recover from a significant disruption and resume critical operations. *Source: FFIEC IT Examination Handbook Glossary*

Resilience testing: Testing of an institution's business continuity and disaster recovery resumption plans. *Source: FFIEC IT Examination Handbook Glossary*

Risk assessment: A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat. *Source: FFIEC IT Examination Handbook Glossary*

Risk management: The total process required to identify, control, and minimize the impact of uncertain events. The objective of a risk management program is to reduce risk and obtain and maintain appropriate management approval. *Source: FFIEC IT Examination Handbook Glossary*

Rlogin: Remote login. A UNIX utility that allows a user to login to a remote host on a network, as if it were directly connected, and make use of various services. Remote login is an information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. *Source: NIST Electronic Authentication Guidance*

Rogue wireless access: An unauthorized wireless node on a network. *Source: NISTIR 7298 Revision 2*

Router: A hardware device that connects two or more networks and routes incoming data packets to the appropriate network. *Source: FFIEC IT Examination Handbook Glossary*

Sandbox: A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. *Source: NIST: CNSSI-4009*

Security log: A record that contains login and logout activity and other security-related events and that is used to track security-related information on a computer system. *Source: NIST: SP 800-92*

Security posture: The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, and policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. *Source: NISTIR 7298 Revision 2*

Sensitive customer information: A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes

any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number. *Source: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*

Server: A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing. *Source: FFIEC IT Examination Handbook Glossary*

Service-level agreement (SLA): An agreement that details of the responsibilities of an IT service provider, the rights of the service provider's customers, and the penalties assessed when the service provider violates any element of the SLA. SLAs also identify and define the service, plus the supported products, evaluation criteria, and quality of service customers should expect. SLAs are typically measured in terms of metrics. Examples include processing completion times and systems availability times. *Source: FFIEC IT Examination Handbook Glossary*

Social engineering: A general term for trying to trick people into revealing confidential information or performing certain actions. *Source: NIST SP 800-114*

Spear phishing: An attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network. *Source: Guidelines for Secure Use of Social Media by Federal Departments and Agencies*

SQL injection attack: An exploit of target software that constructs structure query language (SQL) statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended. SQL injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as ability to add or modify data in the database. *Source: MITRE Common Attack Pattern Enumeration and Classification*

System development life-cycle process: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. *Source: NIST System Development Life Cycle*

T1: A special type of telephone line for digital communication and transmission. T1 lines provide for digital transmission with signaling speed of 1.544 Mbps (1,544,000 bits per second). This is the standard for digital transmissions in North America. Usually delivered on fiber optic lines. *Source: FFIEC IT Examination Handbook Glossary*

Telnet: An interactive, text-based communications session between a client and a host. It is used mainly for remote login and simple control services to systems with limited resources or to systems with limited needs for security. *Source: Guide to Industrial Control Systems (ICS)*

Security **Third-party relationship:** Any business arrangement between a financial institution and another entity, by contract or otherwise. *Source: OCC Bulletin 2013-29*

Third-party payment processor: Bank customers that provide payment-processing services to merchants and other business entities. *Source: FFIEC BSA/AML Manual*

Third-party service provider: Any type of company, including affiliated entities, non-affiliated entities, and alliances of companies providing products and services to the financial institution. Other terms used to describe service providers include vendors, subcontractors, external service providers, application service providers, and outsourcers. *Source: FFIEC IT Examination Handbook Glossary*

Threat intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making. *Source: SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project*

Token: A small device with an embedded computer chip that can be used to store and transmit electronic information. *Source: FFIEC IT Examination Handbook Glossary*

Trusted zone: A channel in which the end points are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include secure socket layer, internet protocol security and a secure physical connection. *Source: CNSSI Glossary*

US-CERT: The U.S. Computer Emergency Readiness Team, part of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center. US-CERT is a partnership between the Department of Homeland Security and the public and private sectors, established to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation. *Source: US-CERT*

Virtual machine: A software emulation of a physical computing environment. *Source: Webster's Dictionary*

VPN (virtual private network): A computer network that uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. *Source: FFIEC IT Examination Handbook Glossary*

Vulnerability: A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing. *Source: FFIEC IT Examination Handbook Glossary*

Zero-day attack: An attack on a piece of software that has a vulnerability for which there is no known patch. *Source: DHS Continuous Diagnostics and Mitigation*