APPENDIX A
GLOSSARY

Access – Access means to use. For example, programs can access memory, which means they read data from or write data to the main memory. More specifically, access often means to read data from or write data to a mass storage device.

Access Control – Access control refers to mechanisms and policies that restrict access to computer resources. An Access Control List (ACL) specifies what operations different users can perform on specific files and directories (assets).

Access Control ID (ACID) – ACID is the term CA Top Secret Software uses for user identification.

Adequate Security –Adequate security is security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Agency - An agency is any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency. 5 U.S.C. 552 (f) (1)

Appliances -A hardware-based device that performs one or more complex functions requiring sophisticated software and external controls. Examples include but are not limited to: firewalls, security policy manager, packet shapers, filtering/proxy devices, VPNs, network attached storage and routers.

Application - A system that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in an application might comprise other application programs, hardware, software, and telecommunications components. Applications can be either software or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Application Owner – The head(s) of an organizational segment(s) that is responsible for authorizing funding for the procurement, development, installation and/or maintenance of a software application running on a USDA Automated Information System and its environment.

Asset - A major application, general support system, high impact program, physical plant, mission critical system or logically related group of systems. An asset is also a physical or intangible item of value to an organization or individual.

Assurance : is the degree to which the purchaser of a system knows the security features and procedures being acquired will operate correctly and will be effective in the system environment.

Audit Trail – An audit trail is a series of records of computer events about an operating system, application or user activities. A computer system may have several audit trails, each devoted to a particular type of activity.

Authentication - Security measure designed to establish the validity of a transmission, message or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Automated Information System (AIS) - An AIS is any assembly of electronic equipment, hardware, software and firmware configured to collect, create, communicate, disseminate, process, store, and control data or information.

Availability – Assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.

Awareness – Awareness is a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of IT security.

Back-up Site (Alternate Site) – a facility that is able to support system operations in restoring critical systems to an acceptable level as defined in the DR plan. Sites are referred to as: cold, warm, hot, mobile, and mirrored.

Baseline - The baseline consists of an approved system requirements document and is initially known as the "requirements baseline". The requirements baseline is also the basis against which the system is authenticated. Each baseline is subject to configuration control and must be formally updated to reflect approved changes to the CI or system as it goes through the life cycle stages.

Baseline Security – Baseline security refers to the minimum security controls required for safeguarding an Information Technology (IT) system based on its identified needs for confidentiality, integrity and/or availability protection.

Breach - Any illegal penetration or unauthorized access to
a computer system that causes damage or has the potential to cause damage.

Business Impact Analysis (BIA) - An analysis of the business processes and interdependencies used to characterize contingency requirements and priorities in the event of a significant disruption of service. More information concerning the BIA can be found in NIST Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems.

Capital Planning and Investment Control (CPIC) – A systematic approach to selecting, managing, and evaluating information technology investments

Central Processing Unit (CPU) – The Central Processing unit is the brain of the computer. CPU is sometimes referred to simply as the processor or central processor. In terms of computing power, the CPU is the most important element of a computer system.

Certificate - A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

Certificate Authority (CA) - An authority trusted by one or more Users to issue and manage X.509 Public Key Certificates and Certificate Authority Revocation Lists.

Certificate Policy (CP) - A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates.

Certificate Revocation - Cancellation of a certificate prior to its designated expiration date. Reasons for revocation of a certificate include corruption, compromise or loss of a certificate, departure of the certificate holder or deactivation of the server where the certificate resides.

Certificate Revocation List (CRL) - An electronically signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.

Chain of Custody – The protection of evidence by each responsible party to ensure it against loss, breakage, alteration or unauthorized handling. This protection also includes properly securing, identifying, and dating evidence. Individuals place their initials and date on the container when the evidence is stored in a container or on the evidence in such a way that no damage is incurred.

Client – A term that refers to the client part of a client/server architecture. 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.

Client/Server Architecture - Network architecture in which each computer or process on the network is either a client or a server. Servers and mainframes are powerful computers or processes dedicated to managing disk drives (file servers, printers (print servers), or network traffic (network servers). Clients are PCs or workstations on which users run applications. Thin clients rely on servers and mainframes for resources, such as files, devices, and even processing power. Client-server architectures are sometimes called two-tier architectures.

CM Authority (CMA)- The agency CIO/Agency Head/ Site Executive decision-making authority that approves or disapproves proposed changes and exercises authority at the agency or site level via a Configuration Control Board (CCB).

CM Planning and Management- CM planning and management includes organizing, coordinating, and managing all of the tasks necessary to implement and conduct CM activities. CM planning and management occurs throughout all life-cycle phases of a system.

CM Program Library- A CM Program Library is a location that contains software code, system technical documentation and the official master copies of all configuration items baselines or pointers to their location. CM program libraries may be established at the office, agency, site, or system program/project organizational level. Efficient operation of the library is enhanced if automated tools are available.

CM Specialist (CMS) - The person is responsible for management and operation the CM system. A CMS ensures that appropriate CM plans and procedures are developed and implemented; ensures that all requests for changes are processed properly; provides reports on the status of all configuration items and proposed system changes, and controls all of the configuration baseline items.

Common Criteria (CC) – CC was developed by NSA and NIST, in cooperation with the National Information Assurance Partnership (NIAP), as a security evaluation scheme that enables vendors of IT systems to provide C2 equivalent protection capabilities and Is an international standard.

Compromise – A compromise is the unauthorized disclosure, modification, substitution, or use of sensitive information or to invade system by getting around its security. A computer has been compromised, for example, when a Trojan horse has been installed.

Compromise of Integrity – A compromise of integrity is any unauthorized modification of the correctness of information or data.

Computer Associates Access Control Facility 2 (CA-ACF-2) –
CA- ACF-2 is one of several types of security access control software used to provide minimum standard protection in IBM and IBM Compatible mainframe environments.

Computer Room – The physical space that houses any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.

Computer Security Incident – A computer security incident is any adverse event whereby some aspect of a computer system is threatened: loss of data confidentiality, disruption of data or system integrity, disruption or denial of availability. Some examples are listed below:

Intrusion of computer systems via the network (often referred to as "hacking");
The occurrence of computer viruses and/or resulting damage;
Unusual or suspicious probes for vulnerabilities via the network to a range of computer systems (often referred to as scans);
Unusual processes, not installed by USDA, running on server.

Within the computer security arena, these events are often simply referred to as "incidents". The definition or identification of an incident may vary for each USDA agency or mission area depending on the situation. However, the following categories (also defined in this section) are generally applicable: Compromise of Integrity, Denial of service, Misuse, Damage, and Intrusions.

Computer Security Policy - Senior management's directives that create a computer security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Policy may also refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy.

Computer System – This term applies to any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. This includes computers, ancillary equipment, software, firmware, and similar procedures, services, including support services and related resources as defined by regulations issued by the Administrator for the General Services Administration.

Confidentiality – A security requirement that private or sensitive Information not be disclosed to unauthorized individuals.

Configuration Auditing/Verification - The Configuration Audit and Verification process is used to verify a product's performance requirements have been achieved by the product/system design and have been accurately documented.

Configuration Change Control - The configuration control process manages the current configuration baseline, which results from the configuration identification process.

Configuration Control Authority - The project or system manager decision-making authority that approves or disapproves proposed changes and exercises authority at the project/system level, within the scope of their charter, via a Configuration Control Board (CCB).

Configuration Control Board (CCB)- A CCB is composed of management, technical and user representatives who recommend approval or disapproval of proposed changes to a CI and its current approved configuration documentation and manage Configuration Item (CI) baselines.

Configuration Identification- The Configuration Identification documents the products of system engineering and the approved configuration of the physical and functional characteristics of the system or product. In addition, Configuration Identification provides unique product and document identifiers and establishes baselines for Government/ contractor configuration control.

Configuration Item (CI)- A CI is an aggregation of hardware and/or software that satisfied an end use function and is designated by the Government for separate configuration management.

Configuration Management (CM)- CM is a process of reviewing and controlling the components of an Information Technology System throughout its life to ensure that they are well defined and cannot be changed without proper justification and full knowledge of the consequences. CM ensures that the hardware, software, communications services and documentation for a system can be accurately determined at any time.

Configuration Status Accounting - This process provides visibility into status and configuration information concerning the product, system, and its documentation. CSA tracks configuration documentation changes and documents the configuration of items. These records include both current and historical information to ensure trace ability from the initial requirements.

Contingency Planning – Refers to the dynamic development of a coordinated recovery strategy for IT systems or application, operations, and data after a disruption. The planning process requires several steps: develop policy; conduct business impact analysis (BIA); identify preventive controls; develop recovery strategies; develop contingency plan; test and exercise the plan; train personnel; and maintain the plan.

Contingency Planning Coordinator – A delegated individual who designates appropriate teams to implement the recovery strategy. Each team should be trained and ready to deploy in the event of a disruptive situation requiring plan activation.

Controlled Access Protection (C2) – C2 is a standard that is applied to operating system software to provide a required minimum level of security. This standard is the highest government rating for business computing products and requires that the system have discretionary resource protection and auditing capability.

Cookie – a small piece of information that may be sent to a computer connected to the Internet to track a user's Web browsing habits. There are two types of cookies: a session cookie is a line of text temporarily stored in a computer Random Access Memory that is never written to a drive and is destroyed as soon as the browser is closed; a persistent cookie is a more permanent line of text that gets saved by a browser to a file on the hard drive that can be used to track a user's browsing habits.

Copyright - Copyright is the ownership of an intellectual property within the limits prescribed by a particular nation's or international law. In the United States, for example, the copyright law provides that the owner of a property has the exclusive right to print, distribute, and copy the work and permission must be obtained by anyone else to reuse the work in these ways. The notion of freedom of information and the ease of posting, copying and distributing messages on the Internet may have created a false impression that text and graphic materials on World Wide Web sites, posting in "usenet" news groups and messages distributed through e-mail lists and other electronic channels are exempt from copyright statues. In the United States, copyright is a protection provided under title 17 of the U.S. Code, articulated in the 1976 Copyright Act. Copyright of a creative work extends 50 years beyond the lifespan of its author or designer. Works afforded copyright protection include literature, journalistic reports, musical compositions, theatrical scripts, choreography, artistic matter, architectural designs, motion pictures, computer software, multimedia digital creations, and audio and video recordings. Copyright protection encompasses Web page textual content, graphics, design elements, as well as postings on discussion groups.

Countermeasures and Controls – Countermeasures and controls refer to the procedures or techniques used to prevent the occurrence of a security incident, detect when an incident is occurring or has occurred, and provide the capacity to respond to or recover from a security incident. Basically, they are intended to protect the assets and availability of an IT system. (Synonymous with safeguards)

Cross-certification - The process in which each CA signs another's certificate to signify trust. This is a peer-to-peer certification.

Cryptography - The science and practice that embodies principles, means and methods for the transformation of information to hide its content, prevent its undetected modification, and prevent its unauthorized use.

Customer Information Control System (CICS) – A system that was originally developed to provide transaction processing for IBM. It controls the interaction between the application and users; CISC also lets the programmer develop screen displays without detailed knowledge of the terminal being used.

Damage – Damage is the unauthorized deliberate or accidental modification, destruction or removal of information or data from a computer system.

Database Management System (DBMS) – A collection of programs that enables the storage, modification and extraction of information from a database. There are many different types of DBMS programs ranging from small systems that run on personal computers to huge systems that run on mainframes.

Data Encryption Standard (DES) – A DES key consists of 64 binary digits of which 567 are randomly generated and used directly by the algorithm. (FIPS 46-3) A Data Encryption Standard (DES) is a U.S. Government-approved, symmetric cipher, encryption algorithm used by business and civilian government agencies. The Advanced

Encryption Standard (AES) is designed to replace DES. The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. Triple DES (see glossary entry below), however, is still considered to be secure.

Data Integrity - The state that exists when computerized data or information is the same as that in the source documents or code and has not been exposed to accidental or malicious alteration or destruction.

Data Key - A cryptographic key which is used to transform data (e.g., encrypt, decrypt, authenticate).

Decryption - The process of transforming encrypted data into plain or readable information.

Demilitarized Zone (DMZ) - A demilitarized zone serves as connection points for computer systems that need to be accessible either externally or internally, but due to the inherent risks associated with public connectivity, should not be placed on the internal protected network. The DMZ sits between the public Internet and the internal networks.

Denial of Service – Denial of service is an inability to utilize system resources due to unavailability; for example, when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with external messages or "a system manager and all other users become locked out of a UNIX system, which has been changed to single user mode."

Designated Accrediting Authority (DAA) – From a security perspective, all USDA General Support Systems (GSS) and Software Applications are required to undergo a security certification process and be accredited by a Designated Accrediting Authority (DAA) prior to being placed in operation. This individual is the agency management official who formally authorizes a system's operation in writing and explicitly accepts any risks associated with that system. The implementation of a formal configuration management process is a requirement for system accreditation.

Device – A piece of hardware that performs a specific function related to or included in an IT system, usually a General Support System, with a minimum of intervention. Examples include but are not limited to: network switches, CSU/DSUs, printers and routers.

Digital Certificate (Public Key) - An attachment to an electronic message used for security purposes. A digital certificate is used to verify that a user sending a message, or accessing a site on the Internet, is who he or she claims to be. Digital certificates are obtained from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the user's Public Key and other identifying information.

Digital Signature - The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.

Digital Subscriber Line (DSL) - DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone line. A DSL line can simultaneously carry both data and voice signals, and the data part of the line is continuously connected.

Discretionary Access Control (DAC) - DAC is an access policy in which the system owner restricts access to system objects such as files, directories, devices, databases, and programs, based on the identity of the users and/or groups to which they belong.

Disruption – An unplanned event that causes the General Support System or Application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Education – IT security education focuses on developing the ability and vision to perform complex, multi-disciplinary activities and the skills needed to further the IT security profession. Education activities include research and development to keep pace with changing technologies and threats.

Electronic Record - Any record that is created, used, maintained, transmitted, and disposed of in electronic form. Such records may be stored in computer memory (random access memory) or on flexible disks. Offices may or may not have non-record paper copies of electronic records. Electronic records are also referred to as machine-readable records because they require machine processing for conversion to human-readable form. Examples of these types of records include those on magnetic tapes, disks and drums, video files, optical disks, and floppy disks.

Employee Owned Equipment - Personal computing equipment owned and maintained by the employee, but used for official USDA business under an approved telework arrangement.

Encryption – is the process of transforming readable information into cipher text, which cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The use of encryption/decryption is as old as the art of communication. A cipher, often incorrectly called a "code," can be employed to keep unauthorized parties from obtaining the contents of transmissions. PKI encryption uses two separate but related keys, a Key Pair, in a process known as asymmetric encryption. One key, the Public Key, is used to encrypt a message or Internet session. The sender’s Private Key attaches a separate digital signature to the data. The second key, or Private Key, is also used to decrypt a message or session.

Evasive – A term used to classify material, which is characterized as, exhibiting evasion, intentionally vague, or ambiguous.

Exposure -A measure of the potential risk to an IT system from both external and internal threats.

Extranet – An extranet is the extension of an organization’s intranet out onto the Internet. This is in contrast to, and usually in addition to, the organization’s public web site that is accessible to everyone. The difference can be somewhat blurred but generally an extranet implies real-time access through a firewall of some kind. Selected customers, suppliers and mobile workers can access the company’s private data and application via the World Wide Web.

Federal Bridge Certification Authority (FBCA) - The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Agency Principle Certification Authorities.

Federal Computer System – This terms applies to a computer system operated by a Federal agency or a contractor of a Federal agency or other organization that processes information using a computer system on behalf of the government to accomplish a Federal function. This includes automatic data processing equipment.

Federal Operator – A Federal operator is any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service.

Firewall - A firewall is a security policy and technology that defines the services and accesses permitted and the implementation of that policy in terms of a network configuration. The main purpose of a firewall is to restrict access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they are examined and evaluated. A USDA firewall must use stateful inspection technology that is aware of the content and state of connection. This technology, which denies all traffic unless it is specifically allowed, employs rules targeted squarely at implementing security decisions at all levels; effectively log activities; filters throughout all levels of the protocol stack; tracks valid active sessions, and processes/filters/tracks high level applications such as electronic mail, file transfer and hyper-text transmission.

Functional Requirement: an expressed need for a system to exhibit specific, often quantified, behaviour as a result of its interaction with its operational environment.

General Support System (GSS) - GSS is a collection of interconnected information resources or computing environments under the same direct management control, which shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications , facilities, and people, and provides support for a variety of users and common applications. A general support system, for example, can be a local area network (LAN) including smart terminals that support a branch office, a backbone network (e.g., agency-wide), communications network, departmental processing center including its operating system and utilities, tactical radio network, office automation and electronic mail services, or share information processing service organization. A general support system can also host one or more major applications.

Government Owned Equipment - Personal computing equipment owned and maintained by the USDA, but used for official USDA business under an approved telework arrangement.

Grantee – One to whom a grant is made. In USDA, grant agreements are made with individuals, entities, and academic institutions to perform scientific research and other studies as authorized by law.

Guidance –Interim documents designed and issued to control or govern security behavior. Guidance provides policy and procedures to be used until a subject specific directive is published.

Hackers/Crackers – The term "hacker" is used to describe any individual who attempts to compromise the security of an IT system, especially those whose intention is to cause disruption or obtain unauthorized access to data. A "cracker" is any individual who used advanced knowledge of networks or the Internet to compromise network security.

Harm – Harm is to damage, injure or impair Information Technology (IT) systems using electronic methods.

Homepage – is the first page (i.e., the opening screen) of a Web site.

Host- A computer that acts as a source of information or signals. The term can refer to almost any kind of computer, from a centralized mainframe that is a host to its terminals, to a server that is host to its clients, to a desktop personal computer (PC) that is host to its peripherals. In network architectures, a client station (user's machine) is also considered a host because it is a source of information to the network in contrast to a device such as a router or switch that directs traffic.

Hotfix- Microsoft's term for a bug fix, which is accomplished by replacing one or more existing files in the operating system or application with revised versions.

IBM UNIX System Services – Unix System Services provide all of the capabilities and flexibility of UNIX in the z/OS/OS390 IBM operating system.

Incident Handling - This refers to the actions taken to resolve the incident.

Incident Oversight – This process is the ongoing surveillance of the networks and systems to spot new vulnerabilities and take corrective actions in advance of incidents.

Incident Reporting - This involves formal acknowledgement that a computer incident occurred.

Incident Response – This process is the analysis of how the incident happened and how to handle the situation so that it does not reoccur.

Individual - means a citizen of the United States or an alien lawfully admitted for permanent residence.

Individual Accountability - requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information – means any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

Information Technology (IT) – IT refers to computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software.

IT System: A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization.

Intranet – Intranet is a network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like many other Web sites but the firewall surrounding an intranet fends off unauthorized access. Like the Internet itself, intranets are used to share information.

Integrity – Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

Internet - A worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange (Also know as: cyberspace or the World Wide Web). Anyone with a computer can access the Internet through an Internet Service Provider (ISP).

Internet Control Message Protocol (ICMP) – Internet Control Message Protocol is an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Protocol (IP) address – A numeric address allocated to identify nodes on a TCP/IP network. These addresses can be statically or dynamically allocated. The current addressing scheme on the Internet is know as IPV4.

Interoperability - Interoperability means that the technology used by two certifying authorities can work together.

Intruder - An intruder is a person who is the perpetrator of a computer security incident. Intruders are often referred to as "hackers" or "crackers." Hackers are highly technical experts who penetrated computer systems; the term Crackers refers to the experts with the ability to "crack" computer systems and security barriers. Most of the time "cracker" is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within USDA or attacking from the outside of Department.

Intrusion – Intrusion is an unauthorized, inappropriate or illegal activity by insiders or outsiders that can be considered a penetration of a system.

Inventory – The process of making a detailed list of equipment in one's possession.

Isolation Zone – An Isolation Zone is logically and physically restricted space that may contain sensitive equipment such as firewalls, Intrusion Detection Systems (IDS), or network nodes.

IT Investment – An expenditure of money and/or resources for IT and IT-related products or services involving managerial, technical, or organizational risks for which there are expected benefits to the organization's performance.

IT Related Risk - The net mission impact considering (1) the probability that a particular threat source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur.

IT Security - IT Security is a technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. (Synonymous with Automated Information System Security, Computer Security, Information Systems Security, and Cyber Security)

IT Security Literacy – IT Security Literacy is the first solid step of the IT security training level where knowledge is obtained through training that can be directly related to the individual's role in his or her specific organization.

IT Security Program - A program established, implemented and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored or disseminated in its Information Technology systems. (Synonymous with Automated Information System Security Program, Computer

Security Program, Information Systems Security Program, and Cyber Security)

Job Function – Job functions are the duties specific to a job title.

Key Pair - Two mathematically related keys having the properties that one key can be used to encrypt a message that can only be decrypted using the other key, and even knowing one key, it is computationally infeasible to discover the other key.

LAN Room – A room that contains equipment used to support Local Area Networks (LAN). Most LANs connect workstations and personal computers that span a relatively small area such as a single building or complex.

Learning Continuum – A learning continuum is a representation in which the common characteristic of learning is presented as a series of variations from awareness through training to education.

Least Privilege – Least privilege is the practice of granting users only those accesses required to perform their official duties.

Levels of Concern - An expression of the criticality/sensitivity of an IT system in the areas of confidentiality, integrity, availability, and exposure, expressed qualitatively as high, moderate or low. The level of concern indicates the extent to which security controls must be applied to an IT system based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs.

Level of Consequence - The impact an incident has on an organization. Impact includes: loss of data; the cost to a USDA agency or mission area; negative consequences to the organization (e.g. damage to reputation); and the magnitude of damage that must be corrected.

Life cycle: a set of processes and their temporal relationships that describe a continuous flow of actions and states associated with the existence of system. The linear sequence of phases of a system's existence that span an initiating action to a closing action, with an implied future re-execution of the sequence.

Mainframe – A very large and expensive computer capable of supporting hundreds, or even thousands, of users simultaneously. In the hierarchy that starts with the simple microprocessor at the bottom and moves to supercomputers at the top, mainframes are just below supercomputers. In some ways, mainframes are more powerful because they support more simultaneous programs. Unisys and IBM are the largest manufacturers of mainframes.

Maintain - Under the Privacy Act, maintain means to keep, collect, use or disseminate. 5 U.S.C. 552 (a) (3)

Major Information System – An information system that requires special management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant role in the administration of agency programs, finances, property or other resources.

Management Controls – Controls that focus on the management of the Computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the application or general support system.

Mass Storage – Mass storage refers to various techniques and devices for storing large amounts of data.

Misuse - Unauthorized use of an account by an intruder (or insider)constitutes misuse.

Mitigation – The process of moderating in force or intensity; alleviate.

Multiple Virtual Storage (MVS) – Multiple Virtual Storage refers to the operating system for older IBM mainframes. MVS was first introduced in 1974 and continues to be used, although it has been largely superseded by IBM's new operating system, OS/390.

Need-to-Know - The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person's duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency or a foreign government.

Network – A network is a group of two or more computer systems linked together. Local-Area networks and Wide-Area Networks are two examples of networks.

Network Administrator (Local or site) - A person who manages a local area network, communications, or other IT resources within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

Network Node – Computers on a network are sometimes called nodes. A node can be a computer, or some other device, such as a printer. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address.

Non-repudiation - Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity, date/time transmitted, and the validity of content that the transaction took place. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.

Object Reuse – Object Reuse is capability and assurance that a storage object or device (memory, disk, tape, cartridge/cassette, and CD-ROM) storing sensitive data or information has been cleared of the information before it is used for other purpose.

Operating System - The master control program that runs the computer. The first program loaded when the computer is turned on, its main part, the "kernel," resides in memory at all times. The operating system sets the standards for all application programs that run in the computer. The applications "talk to" the operating system for all user interface and file management operations.

Operational Controls - Address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to technical controls).

Operator of a Federal computer system – means a Federal agency , contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function.

OS-390 – The OS-390 is IBM's newest operating system that superseded MVS.

Ownership – Ownership is the responsibility for the security of an IT system or asset that must be assigned to a single, identifiable entity, and to a single senior official within that entity. This approach minimizes the potential for unauthorized activities, and maximizes the potential that the individual knows and understands the nature of threats and vulnerabilities associated with the use or maintenance of an IT system.

Patch - A patch (sometimes called a "fix") is a quick repair job for a piece of programming. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's website. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and track the installation of patches.

Peer-to-Peer – A communications model in which each party has the same capabilities and either party can initiate a communications session. In some case peer-to-peer communications is implemented by giving each communication node both server and client capabilities.

Peer-to-Peer Software – Software programs that can link your computer to other computers across the Internet for the purpose of sharing files, music and videos. They traditionally by-pass security controls and client/server networks that exist in business and government offices. A number of software programs even allow the sharing of computers.

Personal Papers - Personal papers are documentary materials, or any reasonably differentiable portion thereof, of a private or nonpublic character that do not relate to, or have an effect upon, the conduct of agency business. If information about private matters and agency business appears in the same document, the document shall be copied at the time of receipt, with the personal information deleted, and treated as a Federal record.

Phase (CPIC) – The CPIC process is a circular flow of USDA's IT Investments through five sequential phases: Pre-Select, Select, Control, Evaluate, and Steady State.

Phase: a characteristic, primary period in the sequence of events that comprise the life cycle of an information technology system.

Physical Security – Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes and accidental damage. It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control and appropriate protection from intruders.

Plain text -Unencrypted information or data sent in a transmission.

Plan Maintenance – As a general rule, plans should be updated at least semi-annually, when significant change occurs in the IT system or when problem are identified through testing. Contact lists and the emergency call tree should be reviewed and updated frequently.

Point of Presence (POP) - A physical layer within a local access and transport area (LATA) at which an inter-LATA carrier establishes itself for the purpose of obtaining access and to which the local exchange carrier provides access services.

Pornography – Pornography is written, graphic or other forms of communication pertaining to obscenity, which is objectionable or offensive to accepted standards of decency and is usually intended to excite lascivious feelings.

Preventive Measures – A risk management process implemented to identify, control and mitigate risk or threats to an IT system in order to reduce or eliminate vulnerabilities and the consequences of threats.

Privacy Act Record - [the substance of a record i.e.,]any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Privacy Information – [the substance of record, i.e.,] any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
The following are the approved types of information that can be collected from visitors to USDA Web sites:

- Internet domain and IP Address from which they access our web site;
- Type of browser and operating system used to access our site;
- Pages they visit; and
- The address of another web site from which the visitor linked to the USDA Web site.

Private Key - (1) The key of a signature key pair typically used to decrypt a publicly encrypted digital signature. (2) The key of an encryption pair that is used to decrypt confidential information. This key is not made publicly available and must be kept secret.

Proprietary – Privately owned and controlled information disclosure of which may result in personal suit or agency liability.

Proxy Server – A proxy server sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Public Key - (1) The key of a signature pair typically used to encrypt a digital signature meant to be decrypted by the private key. (2) The key of an encryption pair that is used to encrypt confidential information. This key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure (PKI) - A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Record – "All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included." (44 USC 3301)

Recovery Objective – An objective expressed in the delivery of products or services to which an IT system must be recovered in order to meet full business objectives.

Recovery Time Objective – A time metric derived from the Business Resumption Plan developed by the business owner.

Registration Authority (RA) - An entity that is responsible for identification and authentication of individuals requesting the certificate, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Regulation – A principle, rule or law designed to control or govern behavior or a governmental order having the force of law.

Resource Access Control Facility (RACF) – One of several types of security access control software used to provide minimum standard protection in IBM/IBM Compatible mainframe environments.

Risk - is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Assessment (RA) - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate the impact.

Risk Management (RM) - An ongoing process of assessing the risks to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk. Simply stated, RM is a total process of identifying, controlling, and mitigating information system related risks.

Roles and Responsibilities – Roles and Responsibilities are the functions performed by someone in a specific situation and obligations, tasks or duties for which that person is accountable.

Root Certificate Authority - A 'root certificate authority' certifies other certificate authorities (subordinate CAs), helping ensure they are competent to issue certificates and that their certificates can be trusted. Specifically, the Root CA is the trusted entity responsible for establishing and managing a PKI domain by issuing CA certificates to entities authorized and trusted to perform CA functions.

Routine Use – With respect to the disclosure of a record, routine use is the use of such record for a purpose, which is compatible with the purpose for which it was collected. Agencies must publish in the Federal Register uses for each of its systems of records and provide a list of routine uses to any individual from whom they seek to collect personal information.

Rules of Behavior - are the rules that have been established and implemented concerning use of, security controls, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability.

Secure Compartmented Information Facility (SCIF) - A facility where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or processed. There are two types of SCIF's: working areas and storage areas. All SCIFs must be accredited by the Central Intelligence Agency and comply with the rigid physical security standards set forth in CIA Directive 1/21. Additional information on SCIFs can be obtained from that directive.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) – Secure Socket Layer is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:." TLS is an Internet standard based on SSL version 3.0. There are only very minor differences between SSL and TLS.

Security Analysis – A formal analysis conducted by the agency Information Systems Security Program Manager , in conjunction with the business owner or developer, for the purpose of determining the importance of information, assessing risks, formulating mitigation strategies, and other measures needed to safeguard the IT Investment.

Security Training – Security training is the sum of the processes used to impart a body of knowledge associated with IT security to those who use, maintain, develop or manage IT systems.

Security Vulnerability – A weakness in the software and/or hardware design that allows circumvention of the system security.

Sensitive Information - Sensitive Information means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

Sensitivity - In an information technology environment, which consists of the system, data, and applications, sensitivity must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

Server – A server is a computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks.

Service Pack- A collection of software patches or “Roll-up” of existing patches that is applied to an installed application. It is either downloaded from the vendor’s website or distributed via Compact Disk-Read Only Memory (CD-ROM). When executed, it modifies the application in place.

Site Executive – A site executive is the executive level management authority at the National Information Technology Center (NITC) and the National Finance Center (NFC).

Stateful Inspection – A firewall architecture that works at the network layer and is also referred to as dynamic packet filtering. Unlike static packet filtering, which examines a packet based on the information in the header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid.

Statistical Record – A statistical record is a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or part in making any determination about an identifiable individual.

Strategic Investment Criteria – Criteria used by an Executive Working Group (EWG) and the Executive Information Technology Investment Review Board (EITIRB) during the annual investment review cycle. Each criteria details materials that are reviewed, evaluation factors and rating award basis for project components required.

Storage Device – A device capable of storing data. The term usually refers to mass storage devices, such as disk and tape drives.

System - A system is a generic IT term used for brevity to mean either an application or general support system. A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization.

System Administrator – An individual responsible for maintaining a multi-user computer system, including a Local Area Network (LAN). Small organizations may have just one system administrator, whereas larger enterprises usually have a whole team of system administrators.

System Development Life Cycle – The course of developmental changes through which a system passes from its conception to the termination of its use and subsequent salvage. There are many models for the IT system life cycle but most contain five basic phases: Initiation, development/acquisition, implementation, operation, and disposal.

System of Records - A system of records means a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Privacy Act, 5 U.S.C. 552 a (a) (5)

System Operational Status - is either (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

System Owner – The head(s) of an organizational segment(s) who is responsible for providing funding for the procurement, installation, or maintenance of an Automated Information System (AIS) and its environment.

Teams - Groups comprised of critical IT and business function personnel with various skills, knowledge, and ability to perform necessary functions in order to recover critical IT systems and business functions during a major disruption or event.

Technical Controls - consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Telecommunications Room – A room that contains equipment used to support the transmission of telecommunications services. This room is also referred to as the telephone room.

Testing – A mandatory requirement for all plans to validate and evaluate plan procedures and the ability of recovery teams to implement the plan. It identifies any deficiencies in the plan that should be addressed during plan maintenance.

Threat – A threat is circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste and abuse. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, denial of service, packet replay/modification.

Timeliness – Concept that material should be sufficiently current to ensure that any determination based on the record will be accurate and fair.

Time Sharing Operation (TSO) – Time-sharing refers to the use of a computer by more than one user; literally, users share the computer's time. Almost all mainframes and minicomputers are time-sharing systems.

Time-Stamp - A digitally time stamped assertion of the date and Time a digital document was created.

Training – Training is teaching people the knowledge and skills that will enable them to do their job more effectively. Training is the next step beyond awareness and most commonly involves formal instruction on how to perform specific tasks.

Transmission Control Protocol/Internet Protocol (TCP/IP) - TCP and IP were developed by a Department of Defense (DOD) research project to connect a number different networks designed by different vendors into a network of networks (the "Internet"). It was initially successful because it delivered a few basic services that everyone needs (file transfer, electronic mail, remote logon) across a very large number of client and server systems. The IP component provides routing from the department to the enterprise network, then to regional networks, and finally to the global Internet today. The same features of TCP/IP that allow for global connectivity presents an increasing threat to networks that operate without adequate network security policies and protection from the Internet.

Triple DES - a key that consists of three DES keys, also referred to as a key bundle. (FIPS 46-3) An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than AES.

Trusted computer system - A system that employs sufficient Hardware and software assurance measures to allow its use for processing a range of sensitive information. A system believed to enforce a given set of security attributes to a stated degree of assurance.

Unclassified Information - agency information that is not considered classified or sensitive, but requires some level of protection along at least one of the dimensions of confidentiality, integrity or availability (i.e., agency forms, local databases).

Uniform Resource Locator (URL) - URL is the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

User – A human or IT entity that accesses the computer assets in order to perform a specific function.

Valid Audit Trail – A valid audit trail is one that collects a record of who, what, when and where an access event occurred.

Virtual Memory (VM) – Virtual memory is random access memory (RAM) combined with space reserved on a hard disk system (commonly called a swap file) that expands the available physical memory of a system. Support for virtual memory is provided by most modern operating systems.

Virtual Private Network (VPN) - A virtual private network is a logical network that is established, at the application layer of the Open System Interconnection (OSI) model, over an existing physical network and typically does not include every node present on the physical network. Authorized users are granted access to the logical network. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Virtual Storage Access Method (VSAM) - VSAM is a file management system used on IBM mainframes. VSAM speeds up access to files by using an inverted Index of all records added to each file.

Virtual Telecommunications Access Method (VTAM) – The software used to interconnect IBM computers.

Vulnerability - A security exposure or improper configuration in an operating system or other system software or application software component that allows the security policy to be violated. A flaw or weakness that may allow harm to occur to an automated information system or activity. A condition or weakness in security procedures, technical, management or physical controls that could be exploited by a threat.

Web Agent – A Web agent is typically a transparent, single pixel gif (a common Web graphic format) located on an external Web site this is referenced by Web page code. Because the agent records a “hit” on the log files of the remote server, the operators of the remote server can track browsing. Such agents frequently appear in banner ads or in Web page JavaScript code. Agents do not normally carry data like cookies and they are almost undetectable without examining the Web page code. (There are methods to embed information within the graphic file that is undetectable by normal software.)

Web browser – software that allows a user to locate, view, and access information on the Internet via the use of a graphical interface.

Web Farm – A web farm is an integrated collection of firewalls, switches, servers, backup libraries and other components that are precisely focused to develop and maintain a secure, scalable, and redundant web delivery infrastructure. Web farms provide high-speed access to Internet and Intranet users, robust security features, common web services, a dedicated operations staff and standard policies/procedures in the delivery of web products and services.

World Wide Web – a network that offers access to websites all over the world using a standard interface for organizing and searching.

Worm - A type of malicious code particular to networked computers. It is a self replicating program (unlike a virus which needs a host program) which works its way through a computer network exploiting vulnerable hosts, replicating and causing whatever damage it was programmed to do.

X.509 Certificate - X.509 Certificates are a Federal government standard used to ensure that Internet transmissions, whether data messages such as email, or secure web sessions, cannot be deciphered if intercepted. A certificate contains identifying information about the certificate's owner, a digital signature unique to the owner, as well as an encrypted public key. A Public Key that matches the owner's Private Key is included. It also contains the identification and signature of the Certificate Authority (CA) that issued the certificate and the period of time the certificate is valid. Certificates ensure that the receiver can verify the identity of the sender.

z/OS- z/OS is a secure, scalable, high performance enterprise IBM operating system that can be used to build and deploy Internet and Java-enabled applications, providing a comprehensive and diverse application execution environment. IBM bases Z/OS on 64-bit z/architecture.