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.

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

Automated Information System - 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.

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.

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.

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

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 - Protection of evidence by each responsible party to ensure against loss, breakage, alteration or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence. Individuals shall 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.

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.

Compromise – A compromise is to invade something 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 Policy - is senior management's directives to 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. Additionally, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy.

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 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.

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.

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.

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

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.

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 Major Software Applications (MSA) 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.

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.

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.

Encryption (PKI - General) - 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. To receive PKI encrypted data, a Key Pair must be generated within an encryption program. The Public Key portion of this pair is then deposited or "published" on a Public Key server, where anyone who wishes to send an encrypted message to its owner may retrieve it. The Private Key is kept and known solely to its owner. Possession of a person's Public Key does not make it possible to decipher that person's Private Key. A mathematical function transforms every character in a file into some other character. Encryption renders a file unintelligible. Decryption is a mathematical function that transforms every encrypted character in a file back to its original format.

Evasive – Material, which is characterized as, exhibiting evasion, intentionally vague, or ambiguous.

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 security policy and technology that defines the services and accesses permitted, and an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. 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.

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.

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

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

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

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.

Intranet – a "localized" network of computers used to electronically communicate usually within an agency, company or organization.

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 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 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.

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.

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.

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.

Major Application (MA) - MA is an application that requires special attention to security due to the risk and magnitude of the harm that would result on account of the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a MA might be constituted of many individual application programs and hardware, software and telecommunication components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

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 group of two or more computer systems linked together. Local-Area networks and Wide-Area Networks are two examples of networks.

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.

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.

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.

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.

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.

Privacy Information – 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.

If an individual chooses to provide USDA with personal information, as in an E-mail to the Secretary or by filling out a form with personal information and submitting it to the department through a Web site, agencies/mission areas will use that information only to respond to the E-mail or information request or if the information becomes part of USDA's official records. The Privacy Act governs any records retrieved by the use of a personal identifier.

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.

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)

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 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 state, RM is a total process of identifying, controlling, and mitigating information system related risks.

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.

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.

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."

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.

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

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

Systems - A system is a generic term used for brevity to mean either a major application or general support system.

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.

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.

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.

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.

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

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 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.

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.