IC 99-1 TO AFI 33-129, TRANSMISSION OF INFORMATION VIA THE INTERNET

1 AUGUST 1999

★SUMMARY OF REVISIONS

This change incorporates IC 99-1. It updates and/or establishes HQ USAF/SC, SAF/PA, SAF/AQ, HQ USAF functional manager, MAJCOM/FOA/DRU, and wing-level equivalent commander roles and responsibilities. It establishes a requirement to create multi-disciplinary review boards and conduct annual Web site reviews. Change also expands guidance on managing Web sites, updates required warning notice and banner wording, and adds guidance for republishing base newspapers on the Web. A (★) indicates revision from the previous edition.

★3.1. Headquarters United States Air Force, Director of Communications and Information (HQ USAF/SC) will:

★3.1.1. Develop policy and guidance governing use of the Internet.

★3.1.2. Develop policy and guidance on operation, maintenance, and security of the systems that facilitate the use of the Internet.

★3.1.3. Chair biennial policy review board to ensure policy is consistent with the needs of the Air Force.

★3.2.1. Develop policy and guidance governing the public communications program and the security and policy review program.

★3.2.2. Develop policy and guidance for the integration of public Web sites into Air Force public communications plans and programs.

★3.2.3. Serve as POC for developing a process for identifying appropriate information for posting to public Web sites.

★3.2.4. Develop guidelines and standards for the appearance and content of public Web sites.

★3.2.5. Establish and maintain a system to register Air Force Web sites that fulfill the Government Information Locator Service (GILS) requirements.

★3.2.6. Serve as POC for routine reports submitted by the Joint Web Risk Assessment Cell which will be monitoring compliance with applicable Department of Defense and Air Force policies and procedures.

★3.3. HQ USAF Functional Managers will:

★3.3.1. Conduct annual multi-disciplinary reviews of subordinate public Web sites. Site reviews will look for information that is considered sensitive from the operational, public affairs, acquisition, technology, privacy, legal, and security perspectives. These reviews will coordinate across organizational boundaries as necessary (both vertically and horizontally) to ensure critical information is consistently controlled. Where ANG units are involved, coordination must include the respective State Adjutant General.

★3.3.2. Determine the level of protection required when placing functional information on the Internet or when sending it by electronic mail (e-mail).

★3.4.1. Establish localized plans and procedures for the establishment, maintenance, and review of their Web sites.

★3.4.2. Develop effective operations security (OPSEC) programs to ensure critical information and OPSEC indicators are consistently controlled according to AFI 10-1101, *Operations Security*.

★3.4.3. Establish and maintain official public access Web sites outside the firewall and other controlled access Web sites inside the firewall for internal uses. Register these sites with Air ForceLINK and verify registration annually.

★3.4.4. Provide local index of subordinate Web sites by linking to Air ForceLINK.

★3.4.5. Ensure all public Web sites are reviewed by PA prior to their launch. ANG units will coordinate with their Public Affairs Officer (PAO) prior to their launch. Establish record of review and approval for all subordinate sites.

★3.4.6. Establish command-wide standards of appearance and function for public Web sites.

★3.4.7. Conduct annual multi-disciplinary reviews of subordinate public Web sites.

★3.12. Assistant Secretary of the Air Force, Acquisition (SAF/AQ) will establish, in coordination with SAF/PA, policy and guidance governing the review and release of information made available on public Web sites in the conduct of electronic commerce (e.g. Request for Proposals, Commerce Business Daily Notices, etc.).

★3.13. Wing-Level Equivalent Commanders will:

★3.13.1. Establish and maintain one official public access Internet site and separate, additional controlled access Web sites for internal use per wing-equivalent unit. Register these sites with Air ForceLINK and verify registration annually.

★3.13.2. Establish local clearance and approval procedures in accordance with AFI 35-205 for posting information to the Web. Review and approve in accordance with SAF/AQ guidance information made available on public Web sites for the conduct of electronic commerce.

★3.13.3. Maintain an index and registration for any necessary subordinate pages. Maintain a separate index for public access and restricted Web sites.

★3.13.4. Ensure all public Web sites are reviewed by the wing PA prior to their launch. ANG units will include coordination with the PA for their respective Adjutants General. Establish a record of review and approval for all subordinate sites.

★3.13.5. Conduct annual multi-disciplinary reviews of subordinate public Web sites.

★3.14. Multi-Disciplinary Review Boards will consist of representatives from Communications and Information, Public Affairs, Legal, Contracting, and Operations as well as any other representatives necessary to address questions concerning the sensitivity of information on a public Web site. The site reviews will review publicly accessible Web sites to ensure information that is sensitive from the operational, public affairs, acquisition, technology, privacy, legal, or security perspective does not appear on the public Web site.

★7.2. Public Access Web Sites. Public Web sites exist as part of the Air Force's public communications program and contribute to the overall image of the Air Force, increased public trust and support, airmen morale and readiness, and global influence and deterrence. "Public access information" refers to information approved for "unlimited" worldwide access and distribution on the Internet. Public access information has no access or security controls to limit access to the information. Because public Web sites have global distribution, you must clear the information in accordance with AFI 35-205 and DoDD 5230.9. Public Web sites will not contain any classification or markings. Only information made available on public Web sites for the conduct of electronic commerce is exempt from coordination with local PAOs prior to its public release.

★7.2.2. Approval to Establish a Public Web Site. Approval authority for establishing public Web sites should correspond to existing authority to make public release of information (normally the wing commander). Organizations seeking to establish a public Web site must justify a wide public audience and coordinate with local PA (and in the case of ANG units, the State PAO) and SC prior to receiving release authority (generally unit commander) approval. Only information intended for unlimited distribution is appropriate for public Web sites. The decision to establish a public Web site must weigh the value added by the site to the Air Force public image and public communications program against the maintenance costs and potential security risks.

★7.6. Republishing of Base Newspapers on the Web. Base newspapers are established according to DoD Instruction (DODI) 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*, June 16, 1997; and AFI 35-301, *Air Force Base Newspapers and Commercial Enterprise Publications Guidance and Procedures*. Though generally public domain, base newspapers exist as part of the Air Force's internal information program. While the publishing of base newspapers constitutes public release of information, the distribution is limited. Publishing on an unlimited access Web site constitutes global release. Therefore, some information appropriate for base newspapers is not appropriate for public access Web sites. You may reproduce the content of base newspapers for the Web if that content meets the restrictions provided in DoD's Interim Policy, *Web Site Administration Policies & Procedures*, November 25, 1998. These restrictions include prohibitions against posting names, locations, and specific identifying information about family members of DoD employees and military personnel. You must review all stories against Part V of the DoD policy prior to posting to public Web sites.

★8.1.2.1. Errors Generated by Restricted Pages. Errors generated by public attempts to access restricted pages should redirect the public to the root public page and should not include language like "Access Denied" or "Forbidden." Make redirection from restricted sites as transparent as possible to the public.

★8.2.1. External Links.

★8.2.1.1. The ability to hyperlink to sources external to your organization is a fundamental part of the WWW and can add significant value to the functionality of publicly accessible Air Force Web sites. Air Force activities will establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web pages. Guidelines should consider the informational needs of personnel and their families, mission-related needs, and public communications and community relations' objectives. Ensure guidelines are consistent with the following considerations:

★8.2.1.1.1. Links to non-DoD Web resources should support the organization's mission. Review external links periodically to ensure their continued suitability. If the content of a linked external site becomes questionable or objectionable, remove the link.

★8.2.1.1.2. In accordance with DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998, do not provide product endorsements or preferential treatment on publicly accessible official DoD Web sites.

★8.2.1.1.3. You may not accept payment of any kind in exchange for a link placed on an organization's publicly accessible official DoD Web site.

★8.2.1.1.4. In accordance with DoD 5500.7-R, publicly accessible DoD Web sites shall not require or encourage users to choose any specific browser software. Use text or hyperlinked text to direct visitors to software download sites. Graphics or logos depicting companies or products shall not appear on publicly accessible DoD Web sites.

★8.2.1.1.5. Organizations considering the use of "frames" technology to connect to external sites should consult legal counsel concerning trademark and copyright issues before establishing such links. Where “frames” technologies are used, Web site owners will ensure “frames” are not continued when links external to the site are activated.

★8.2.1.1.6. Organizations are encouraged to link to authorized activities in support of the organization’s mission, such as the Army and Air Force Exchange Service, the Navy Exchange Service Command, and the Marine Corps Exchange. If these sites contain commercial advertisements or sponsorships, the appropriate disclaimer shall be given.

★8.2.1.1.7. When external links to non-government Web sites are included, the MAJCOM commander, or its subordinate organization, is responsible for ensuring that a disclaimer is made that neither Air Force nor the organization endorses the product or organization at the destination, nor does the Air Force exercise any responsibility over the content at the destination. This includes credits given to contractors who produce Air Force Web sites.

★8.2.1.1.8. Once the decision is made to include a link to one non-DoD site, the organization may have to link to all similar sites.

★8.2.1.1.9. Refrain from having pointers on public access pages that reference information that is outside the mission or functional area of the OPR. In most cases, home pages should refer or point only to parent commands and/or subordinate units. Installation home pages should provide pointers to base organizations as well as to the MAJCOM-level home page. Similarly, organizational home pages should have pointers up and down the chain of command.

★8.2.1.1.10. Public Web sites should not link to sites that are restricted from the public. Under certain circumstances, it may be appropriate to establish a link to a log-on site (password interface or other control mechanism) provided details about the site’s controlled content are not revealed.

★8.2.1.3. Display the following disclaimer when linking to external sites: "The appearance of hyperlinks does not constitute endorsement by the U.S. Air Force of this Web site or the information, products, or services contained therein. For other than authorized activities such as military exchanges and morale, welfare and recreation sites, the U.S. Air Force does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site." This disclaimer may appear on the page or pages listing external links or through an intermediate "exit notice" page generated by the server machine whenever a request is made for any site other than an official DoD Web site (usually the .mil domain).

★**13. Warning Notices and Banners**. Ensure warning notices and banners are present on each home page. Tailor public site banners to the audience and type of information presented. Limited access sites must use the exact banner wording found in paragraph 13.2.

★13.1. Public Pages. Public pages will have a banner prominently displayed or announced on at least the first page of all major sections of each Web site. Providing a statement such as “Please read this privacy and security notice” linked to the actual notice is satisfactory. Organizations shall avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or “warning” signs. If the Web site collects any information on usage or other log files, notify visitors what information is collected, why it is collected, and how it is used. Agencies subject to DoDD 5240.1, *DoD Intelligence Activities*, April 25, 1988, must comply with its provisions. Guidance on required text of the privacy and security notice for public access pages follows:

★13.1.1. Privacy and Security Notice.

★13.1.1.1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The notice shall be approved by the appropriate local legal authority before use:

Link from Index.html pages -- "Please read this privacy and security notice."

( ) - indicates sections to be tailored at the installation level

[ ] - indicates hyperlinks

* - indicates information located at the hyperlink destination indicated

PRIVACY AND SECURITY NOTICE

1. (Web site name) is provided as a public service by the ([unit or installation]).

2. Information presented on (Web site name) is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. [Information concerning visitors’],* use of this site is collected for analytical and statistical purposes, such as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Raw data logs will only be used to identify individual users and their usage habits for authorized law enforcement investigations or national security purposes. These logs are scheduled for regular destruction in accordance with [National Archives and Records Administration Guidelines]

6. Unauthorized attempts to deny service, upload information, change information, or to attempt to access a non-public sites from this service are strictly prohibited and may be punishable under Title 18 of the U.S. Code to include the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward

them to us using the (Unit or Installation) [Comment Form]

* Link from above - "information is collected" to the following text:

NOTE: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected.

Example: Information Collected from (DefenseLINK) for Statistical Purposes

Below is an example of the information collected based on a standard request for a World Wide Web document:

xxx.yyy.com -- [28/Jan/1997:00:00:01 -0500] "GET/DefenseLINK/news/nr012797.html HTTP/1.0" 200 16704

Mozilla 3.0/www.altavista.digital.com

xxx.yyy.com (or 123.123.23.12)-- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (**....com**) the requester is coming from a commercial address. Depending on the requester’s method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[28/Jan/1997:00:00:01 -0500] -- this is the date and time of the request.

"GET /DefenseLINK/news/nr012797.html HTTP/1.0" -- this is the location of the requested file on (DefenseLINK).

200 -- this is the status code - 200 is OK - the request was filled.

16704 -- this is the size of the requested file in bytes.

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages.

www.altavista.digital.com - this indicates the last site the person visited, which indicates how people find (DefenseLINK).

Requests for other types of documents use similar information. No other user-identifying information is collected.

★13.2. Limited Pages. Each page of a Web site restricted from public access will clearly state its restriction. Use the following words: “This site is intended for the use of the Air Force [or more restrictive audience] only. Do not reproduce or distribute the content of this site to a wider audience without coordination with the information owner and your unit public affairs office.” The page must also display the following banner: “This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes." Preface limited access information covered by AFI 61-204, *Disseminating Scientific and Technical Information*, with the appropriate distribution statement.

★14.1. Maintaining Registration with Air ForceLINK and Notice of URL Changes and Deletions. Web page administrators are required to ensure the currency of their registration with Air ForceLINK. Post changes to or deletions of public Web sites in advance. The change or deletion of public Web sites without prior notice detracts from the Air Force image unless the Web site must be changed or deleted due to security or operational needs.

Attachment 1

★GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

★DoDI 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*, June 16, 1997

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoDD 5230.9, *Clearance of DoD Information for Public Release*, April 9, 1996

★DoDD 5240.1, *DoD Intelligence Activities*, April 25, 1988

★DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998

★DoD Interim Policy, *Web Site Administration Policies & Procedures*, November 25, 1998

FIPS 140-1, *Security Requirements for Cryptographic Modules*

FIPS 192, *Application Profile for the Government Information Locator Service (GILS)*

OMB 95-01, *Establishment of the Government Information Locator Service*

Article 92, Uniform Code of Military Justice

Computer Fraud and Abuse Act of 1986

AFI 10-1101, *Operations Security*

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 31-401, *Information Security Program Management*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 33-103, *Requirements Development and Processing*

AFI 33-113, *Managing Messaging and Data Processing Centers*

AFI 33-114, *Software Management*

AFI 33-115V1, *Network Management*

AFI 33-127, *Electronic Messaging Registration and Authority*

AFPD 33-2, *Information Protection*

AFMAN 33-223, Identification and Authentication

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 33-322, *Records Management Program*

AFMAN 33-323, *Management of Records*

AFPD 35-2, *Public Communications Programs*

AFI 35-205, *Air Force Security and Policy Review Program*

AFI 35-206, *Media Relations*

★AFI 35-301, *Air Force Base Newspapers and Commercial Enterprise Publications Guidance and Procedures*

AFPD 37-1, *Air Force Information Management* (will be converted to AFPD 33-3)

AFMAN 37-126, *Preparing Official Communications* (will convert to AFMAN 33-326)

AFI 37-131, *Freedom of Information Act Program* (will convert to AFI 33-331)

AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332)

AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339)

AFPD 61-2, *Management of Scientific and Technical Information*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFSSI 5004 Vol I, *The Certification and Accreditation (C&A) Process*

AFSSI 5024Vol III, *Designated Approving Authority Guide*

Abbreviations and Acronyms

AFCA	Air Force Communications Agency
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFMAN	Air Force Manual
AFPD	Air Force Policy Directive
AFRES	Air Force Reserve
AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Memorandum
AIS	Automated Information System
ANG	Air National Guard
BNCC	Base Network Control Center
CSO	C4 Systems Officer

CSSO	C4 Systems Security Officer
DAA	Designated Approving Authority
DoD	Department of Defense
DoDD	Department of Defense Directive
DRU	Direct Reporting Unit
DSN	Defense Switched Network
FIPS	Federal Information Processing Standards
FOA	Field Operating Agency
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTP	File Transfer Protocol
GILS	Government Information Locator Service
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAJCOM	Major Command
MAN	Metropolitan Area Network
MWR	Morale, Welfare, and Recreation
NIPRNET	Non-Secure Internet Protocol Router Network
NNTP	Network News Transfer Protocol
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
OPSEC	Operations Security
PA	Public Affairs
PDP	Public Dissemination Products
POC	Point of Contact
RDT&E	Research Development, Test, and Evaluation
rlogin	Remote Login
SAF	Secretary of the Air Force
SMTP	Simple Mail Transfer Protocol

SSL	Secure Sockets Layer
STINFO	Scientific and Technical Information
TCP/IP	Transmission Control Protocol/Internet Protocol
TDY	Temporary Duty
UCMJ	Uniform Code of Military Justice
URL	Uniform Resource Locator
USAF	United States Air Force
WWW	World Wide Web

Terms

Air ForceLINK--The official web information service for the Air Force.

Base Home Page--A public page that is the official base home page for an installation.

Client--A computer or program that requests a service of other computers or programs.

C4 Systems Officer (CSO)--The term CSO identifies the supporting C4 systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base C4 systems responsibilities. At MAJCOM and other activities responsible for large quantities of C4 systems, it is the person designated by the commander as responsible for overall management of C4 systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

DefenseLINK--An official web information service for the Department of Defense.

Designated Approving Authority (DAA)--Official with the authority to formally assume responsibility for operating an automated information system (AIS) or network at an acceptable level of risk.

File Transfer Protocol (FTP)--A protocol for file transfer between computers; transferring files efficiently and reliably among computers and allowing the convenient use of remote file storage capabilities. A transfer protocol used to transfer files from one computer to another.

Firewall--A protection scheme that assists in securing internal systems from external systems.

★**Frames Technology**--The capability to divide a web browser window into multiple window “panes”or display areas, each simultaneously displaying a different document, allowing multiple, independent document viewing within the same browser window.

Gopher--An information transfer protocol based on a menu interface. Gopher is a distributed document search and retrieval system; it combines the best features of browsing through collections of information and fully indexed databases. The protocol and software follow a client-server model, and permits users on a heterogeneous mix of desktop systems to browse, search, and retrieve documents residing on multiple distributed server machines.

Home Page--A starting point or center of an infostructure on the WWW. A typical home page will consist of hypertext links (pointers) to other web documents.

Hypermedia--The extension of hypertext to things other than documents (for example, video and audio clips).

Hyperlink--A way to link access to information of various sources together within a web document. A way to connect two internet resources via a simple word or phase on which a user can click to start the connection.

Hypertext--A method for storing, retrieving, and presenting information based on the processing power of computers. Allows computerized linking and almost instantaneous retrieval of information based on a dynamic index.

Hypertext Markup Language (HTML)--The native language of the WWW. HTML is a subset of the more complex Standard Generalized Markup Language (SGML).

Hypertext Transfer Protocol (HTTP)--It is the primary protocol used to communicate on the WWW.

Infostructure--A group of web documents linked together on one or more servers, usually providing information concerning a certain subject or idea.

Information Protection Office--Formerly C4 Systems Security Office (CSSO).

Information Provider--The person or organization that provides information for posting on the internet.

Internet--An informal collection of government, military, commercial, and educational computer networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit information. The global collection of interconnected local, mid-level, and wide area networks that use IP as the network layer protocol.

Internet Service Provider--A commercial entity providing data connectivity into the internet.

Intranet--A restricted-access network that works like the Web, but isn't on it. Usually owned and managed by an organization, an intranet enables a activity to share its resources with its employees without sensitive information being made available to everyone with internet access. Intranets may allow connection outside of the intranet to the internet through firewall servers and other security devices that have the ability to screen messages in both directions so that the organizations security is maintained.

Internet Protocol (IP) Spoofing--The use of software to change the address of a data packet to make it appear to come from another machine. Many network routers use these IP addresses to identify which machines have valid access rights to the network. Spoofing allows a hacker to "change his identity" and appear as a valid machine within the network. This type of attack can be foiled by the filtering router which drops "outside" packets with an "inside" source address.

Limited Access--Limited access of internet information applies to information that has been approved for limited access. This information has added safeguards that limit the access to a specific group or groups. According to AFI 35-205, the Office of Public Affairs (PA) will provide security and policy review for internet information at the OPR's request. The OPR must determine the appropriate security and access controls required to safeguard the information.

Limited Access by Domain--Limiting access by using the domain name (for example, .mil, .gov, .edu, and so forth) to restrict access of an area to a specific group or subgroup. Domains are established by the Internet Engineering Task Force (IETF) and assigned based on function or geography.

Limited Pages--Web pages intended for viewing by a limited audience.

Military Controlled Access Paths--Nonclassified networks or "links" that are leased, configured, managed, and secured by a government agency. This includes the unclassified but sensitive Internet Protocol Router Network (NIPRNET-AF, previously AFIN [Air Force Internet]) as well as dedicated links that have a node on the base network.

Network News Transfer Protocol (NNTP)--Also known as Usenet, specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the internet community. NNTP is designed so that news articles are stored in a central database, allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided.

Page Maintainer--The creator and, or focal point for specific material posted on the organization's home page.

Proxy Server--A server connected to the internet through which all incoming and outgoing requests go through; used to enhance security and increase performance/efficiency.

Public Access--Public access of internet information applies to information approved for unlimited public release. Public access information has no access or security controls to limit access to the information. This review determines degree of releasability only; actual release of the material is the decision of the originator (OPR).

Public Dissemination Products (PDP)--Information products produced by the Air Force specifically for the public.

Public Pages--Web pages intended for viewing by the general public. Information on these pages should be of interest to the general public.

Scientific and Technical Information (STINFO)--STINFO includes all technical publications and documents generated by all Air Force-funded research development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports, that DoD could decide to disseminate to the public domain. It also encompasses engineering drawings, standards, specifications, technical manuals, blueprints, plans, instructions, computer software and documentation, photograph, technical orders, databases, and any other information that which is usable or adaptable design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment. It applies to recordings. It does not apply to cryptographic and communications security documents, communications and electronic intelligence, and other categories that the Director, National Security Agency, or the Chief, Central Intelligence Agency designates.

Secure Sockets Layer (SSL)--A security protocol that provides privacy over the internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated.

Server--Software residing on an appropriate hardware platform (computer) that provides a service to other computers or programs, by satisfying client requests.

Simple Mail Transfer Protocol (SMTP)--The protocol used to send electronic mail on the internet.

TELNET--Also known as rlogin, TELNET starts a remote session by specifying a computer to connect to. The command and program used to log in from one internet site to another. The TELNET command/program gets you to the "login:" prompt of another computer or computer system. From that time until you finish the session, anything you type is sent to the other computer.

Transmission Control Protocol/Internet Protocol (TCP/IP)--The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams.

Trojan Horse--A malicious program designed to break security or damage a system that is disguised as something else benign, such as a directory list, archive, a game, or a program to find and destroy viruses.

Uniform Resource Locators (URL)--An internet "address" of a resource. URLs can refer to web servers, FTP sites, Gopher resources, News Groups, etc.

Web Browser--Software that acts as a client, allowing a person to retrieve information from various sources on the WWW.

Web Document--A physical or logical piece of information on the WWW.

Web Page--A single document that includes the text of the document, its structure, any links to other documents, images, and other media.

Web Server--A software/hardware combination that provides information resources to the WWW.

Web Server Administrator--The system administration for the web server, usually referred to as the "Webmaster."

World Wide Web (WWW)--Uses the internet as its transport media and is a collection of protocols and standards that allow the user to find information available on the internet by using hypertext and/or hypermedia documents.