| date of the survey. This index will be available to all FBIHQ
| divisions and offices to aid in their search for preexisting data and
| to provide samples of survey questions.

| (6) FINAL APPROVAL: Each survey that meets the terms of
| the above definition will be forwarded to the Deputy Director for
| final approval. The cover communication that transmits the survey
| will contain a specific statement that the survey has been approved by
| the Deputy Director.|

**EffDte: 08/11/1994 MCRT#: 293 Div: D0 Cav: SecCls:

| |11-7 ADMINISTRATIVE USE OF INTERNET/INTERNET ELECTRONIC MAIL (E-MAIL) POLICY AND GUIDELINES

| (1) The Internet is an interconnection of computer networks
| that enables connected machines to communicate directly with one
| another. It connects universities, research labs, and commercial,
| military and government sites around the world. Users of the Internet
| can exchange E-mail as well as send files to one another.

| (2) There has been a surge of interest among FBI employees
| over the past few years to enhance their information and communication
| resources by utilizing the Internet. As the FBI utilizes new forms of
| technology such as the Internet, there is a crucial need for policy
| and guidelines. Set forth are the administrative FBI policy and
| guidelines for Internet E-mail, utilizing the Internet as a research
| tool, and guidelines for providing public information via the
| Internet.

| (3) The following topics are addressed in 11-7.1 through
| 11-7.8:

| (a) GENERAL INFORMATION defines the FBI's
| administrative purpose for using the Internet and user responsibility
| when accessing the Internet.

| (b) INTERNET CONDUCT describes acceptable behavior
| and user expectation when accessing the Internet.

| (c) PRESERVATION OF RECORDS defines a federal
| record, FBI policy for processing and preserving Internet E-mail
| messages, and guidelines for creating E-mail messages.

| (d) INTERNET E-MAIL ACCOUNTS defines an FBI E-mail
| account and provides procedures for obtaining an account.

| (e) SECURITY explains multiuser usage, passwords,
| downloading files to FBI systems and system requirements needed to
| access the Internet.

| (f) PUBLIC INFORMATION explains what type of

| information the FBI can publish on the Internet and Home Pages.

| (g) POINTS OF CONTACT (POC) contains the POC for
| various Internet matters.

| (h) GLOSSARY defines terms used in this document
| which are essential in understanding the administrative Internet
| policy.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

| 11-7.1 General Information

| (1) The FBI will use the Internet to solicit and accept
| Internet E-mail, as a research tool for authorized purposes (See Title
| 5, C.F.R., Section 2635.704(b)(2) and Title 41 C.F.R. Section 128-
| 1.5006-4), and to provide public information on the World Wide Web
| (WWW) (example: press releases, major case information, pamphlets,
| congressional testimonies, job opportunities, Freedom of Information
| and Privacy Act issues and the like).

| (2) Internet policies and guidelines are applicable to all
| FBI employees, federal or state government personnel, contractors, or
| anyone who is granted access to FBI systems.

| (3) Users of FBI systems are individually responsible for
| understanding and respecting Internet policies and guidelines.

| (4) The Security Officer is to ensure compliance with FBIHQ
| security policy for FBI microcomputer systems as contained in the
| MIOG, Part II, 35-9. The points contained in the All SACs Memorandum
| 20-90, dated July 23, 1990, entitled "Security Awareness Training for
| All FBI Employees," must be brought to the attention of all employees
| semiannually. Administrative Internet Policy will be included in this
| briefing (see MIOG, Part I, 261-2).

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

11-7.2 Internet Conduct

(1) Neither the Internet nor the FBI's Internet resources afford individual users any expectation of privacy or confidentiality. Users should understand that the Internet is not a secure medium and all Internet activities and communications are subject to interception/exploitation by unauthorized persons.

(2) The following policy defines the required conduct and expectations of anyone who is granted access to the Internet on FBI systems:

(a) Internet activities involving FBI resources are subject to monitoring (including retrieval and retention) and will be monitored by authorized FBI security, systems, and management personnel (and their authorized Agents). Any use of, or access to FBI resources constitutes consent of such monitoring. (This in no way means that users are free to divulge any information transmitted or received via the Internet. The FBI's requirement that employees must keep all information acquired in their official capacities strictly confidential, applies to Internet communications also, and employees are prohibited from disclosing FBI information to any person or agency not authorized to receive it.) FBI employees are reminded that they should always be mindful of the high standards of behavior expected of them at all times in their personal and official activities (see MAOP, Part 1, Section 1).

(b) Information derived from such FBI monitoring|and any violation of subsections (c) through (f), below, involving the use of Bureau mainframe or laptop computers, may serve|as a basis for administrative, disciplinary, or legal proceedings if evidence illustrates that an employee is involved in illegal or improper activities which violate federal or state laws, regulations, or FBI policies.

(c) Use of the Internet is a privilege, not a right, which may be revoked at any time for inappropriate conduct. The following are examples which will cause the user's access to be revoked: use of the Internet for unlawful or malicious activities; abusive or objectionable language in either public or private messages; browsing|sexually explicit|sites and chat|rooms, or transmitting or forwarding sexually explicit material through Internet or FBI e-mail systems;|misrepresentation of oneself or the FBI; sending chain letters; other activities that could cause congestion and disruption of networks and systems.

(d) Users will not knowingly engage or participate in any activity that causes harm to the FBI (i.e., creating or procreating viruses, loading, downloading unofficial software or shareware, unauthorized access to other systems, or any other unlawful or improper act).

(e) Users will not discuss or transmit sensitive or classified information on the Internet or within Internet E-mail messages.

(f) Users will not create or transmit materials that violate federal or state regulations; or promote discrimination on the basis of race, creed, color, gender, religion, disability, or sexual orientation.

**EffDte: 01/25/2002 MCRT#: 1203 Div: D4 Cav: SecCls:

| 11-7.3 Preservation of Records/Processing Mail

| (1) The FBI is required by law to preserve federal records according to Federal Records Act (FRA) 44 United States Code, Chapters 31 and 33. Federal regulations from the National Archives and Records Administration (NARA), in concert with FBI policy, govern the life cycle of these records which includes storage, preservation, retrieval, and disposition schedules.

| (2) E-mail messages, attachments and essential transmission data are federal records when they meet the criteria defined in the following Federal Records Act.

| WHAT CONSTITUTES A RECORD: Federal records include all books, papers, maps, photographs, machine readable material, or other documentary materials, regardless of physical form or characteristic, 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.

| WHAT CONSTITUTES A NONRECORD: A nonfederal record is information that is not categorized as a federal record and does not require retention beyond its useful life as determined by the originator and/or recipient. Nonrecord information may be purged or destroyed when the information has served the purpose for which it was intended. The following examples, while not all inclusive, illustrate types of nonrecord information: (1) Informal notes and cover notes that are merely informative in nature. (2) Working papers and drafts which have not been approved and are subject to review. (3) Informative notes, communications or documents which an approving official decides should not go to file. (4) Information that is preserved for reference only. (5) 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 included as nonrecords (Title 44, United States Code, Section 3301).

| (3) The following policy and guidelines will be used when processing incoming and outgoing Internet E-mail:

| (a) Internet E-mail, attachments and essential transmission data will be processed like incoming mail from the United States Postal Service (USPS). Once an Internet message is received, it should be (to include but not necessarily inclusive) searched in indices, distributed to correct personnel to determine what classification, file or control file to which the Internet E-mail message should be saved (if a federal record), and follow the current saving and destruction policy (see MAOP, Part II, 2-2.1 through 2-4.3).

| (b) The sender of an outgoing Internet E-mail message

| or attachment that has been deemed a federal record must determine to
| which classification, file or control file the outgoing Internet E-
| mail message should be saved. This is also required of the sender
| when sending a message or attachment that is deemed a federal record
| via the Internet to another Bureau employee.

| (c) Internet E-mail messages and transmission data can
| be easily uploaded into the ECF component of ACS because messages are
| usually in electronic format. If this data is loaded into the ECF
| component of ACS, this information is retrievable by Case ID,
| attributes, serial or full text. Although E-mail messages are usually
| in electronic format, attachments could be in another format such as
| graphics which are not viewable in any component of ACS. Those
| attachments should be printed (if possible), serialized and placed in
| a paper file. Use current FBI policies to determine if these records
| should be loaded into additional FBI applications such as CLEA, [redacted] b7E -1
| [redacted] etc. Note: All files and programs
| that are downloaded to FBI systems from the Internet or from any
| outside sources must be to a standalone computer or to a floppy disk,
| approved by the Computer Specialist or Security Officer and scanned
| for viruses prior to introduction to any other FBI computer (see
| 11-7.5 "Security").

| (d) Check incoming Internet E-mail daily. Internet
| E-mail should be checked more frequently if warranted by the volume of
| mail received.

| (e) Because of the impact on the FBI's reputation and
| credibility, messages that are deemed federal records that the user
| creates and disseminates should be stated in an intelligible, concise
| and professional manner. Obtain necessary approval as required by
| your division before sending a message.

| (f) Some systems have limitations on the number of
| characters in a message. Therefore, keep outgoing Internet E-mail
| messages short and limited to one subject, if possible.

| (g) Because of software and graphic constraints,
| attachments in Internet E-mail messages should be avoided where
| possible. Some systems are not compatible and difficulty could result
| when reviewing messages and files.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4RM Cav: SecCls:

| 11-7.4 Internet E-mail Accounts

| (1) Every FBIHQ division and field office has an FBI
| Internet account. Some FBI employees have an individual FBI Internet
| E-mail account to be used for official FBI business.
| In this document, Internet E-mail accounts are any Internet E-mail
| accounts that are paid for by the FBI (does not include
| investigative, covert, or other specialized investigative accounts).

| For example: Fieldoffice@FBI.GOV; FBIAcademy.EDU;
| AnyUsersName@FBI.GOV; HQDivision@FBI.GOV and so forth.

| (2) The following procedures will be used in obtaining an
| individual Internet E-mail account:

| (a) E-mail accounts will be granted to users that can
| provide a sufficient justification to the SAC or appropriate authority
| in the division or field office. Notify IRD of any existing or new
| accounts granted, for IRD inventory purposes.

| (b) If approval is granted, you must meet system
| requirements and obtain funding for system requirements and/or funding
| for the account if necessary (see EC titled "Internet Account
| Distribution/Guidelines" dated February 28, 1997).

| (c) FBI.GOV Internet E-mail accounts will be
| reevaluated monthly by IRD to determine if users have maintained a
| need for the account. The account will be terminated within 90 days
| for nonuse. Non-FBI.GOV E-mail accounts that are paid for with FBI
| funds should also be reevaluated monthly and terminated within 90 days
| for nonuse.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

| 11-7.5 Security (See MAOP, Part II, 11-7.3.)

| The following policy describes what is required to avoid
| potential abuse of the Internet and to provide accountability when
| accessing the Internet on FBI systems.

| (1) At a minimum, Watchdog software or a similar software
| package will be used to track usage on "multiuser" FBI Internet
| systems. The following illustrates the type of audit trail with the
| minimum information that must be captured to facilitate reconstruction
| of events if compromise or unauthorized activities occur: user name,
| date, time on and off the Internet (see MIOG Part II, 35-9.3.1).

| (a) Watchdog or a similar software requires each user
| be assigned a unique ID and will also require the user to create a
| password, to be used with the ID for authentication. The ID may be
| publicly known, but passwords must be kept secret.

| (b) Contact your Computer Specialist for access to the
| Internet or if you forget your Watchdog (or similar software) password
| and ID.

| (c) Contact your Computer Specialist or Security
| Officer immediately to report security violations or misuse (see
| MIOG, Part II, 35-9.3.1).

| (2) The following system requirements (not necessarily

inclusive) are necessary to access the Internet: standalone computer (486 or higher), 28kbps (or higher modem), Windows 3.1 or Windows 95, 8MB RAM recommended and 6 MB free hard disk space. The hard drive must never have been used for FBINET or sanitized using Norton Utilities Disk Wipe Government Version. For detailed information see EC titled "Internet Account Distribution/Guidelines" dated February 28, 1997.

(3) All files and programs that are downloaded to FBI systems from the Internet or from any outside source must be to a standalone computer or to a floppy disk, approved by the Computer Specialist or Security Officer and must be scanned for viruses prior to introduction to any other FBI computer (see MIOG, Part II, 35-9.4.4).

(4) Users are reminded that the Internet is not a secure medium and all Internet activities and communications are subject to interception/exploitation by unauthorized persons.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

11-7.6 Public Information

(1) In general, per the news media guidelines, FBIHQ provides public information regarding national and international matters. Field offices provide local public information. Field offices are authorized by the Director to make more wide-ranging statements on a case-by-case basis.

(2) In regard to the Internet, the Office of Public and Congressional Affairs (OPCA) oversees the content and appearance of official FBI material on the web. Prior to placement on the FBI Home Page, FBI matters must be reviewed and approved by the National Press Office (NPO) and the OPCA, with concurrence of other appropriate FBIHQ divisions, as needed. This is to ensure consistency with current FBI and DOJ policy and guidelines. (See MAOP, Part II, 5-10.)

(3) FBI field offices may request their own Home Page accessible through the FBIHQ Home Page. Field offices are responsible for submitting their respective Field Office Home Page information and ensuring that information is updated as needed via the NPO and OPCA. OPCA is responsible for placement, removal, and updating of official FBI material on the WWW/FBI Home Page. The sole purpose of this process is to ensure consistency on national issues and compliance with DOJ guidelines.

(4) Submit information for a Field Office Home Page to the NPO and OPCA. Information should be local in nature and avoid repetition of information included on the FBIHQ Home Page. Submit information on a computer disk, in WordPerfect or Freelance programs, ASCII format, with or without formatting instructions, and include a paper copy. For detailed information, see Airtel titled, "Policy For

Publishing FBI Information On The World Wide Web" dated September 22, 1995.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

11-7.7 Internet Points of Contact

Contact the division or unit below on the following Internet issues if you have any questions:

ISSUE	DIVISION AND/OR UNIT
Legal:	Office of General Counsel, Administrative Law Unit
	Chief Division Counsel
Home Page:	Office of Public and Congressional Affairs, Press Office
System Requirements:	Information Resources Division, Investigative Applications Support Unit
Noninvestigative Accounts:	Information Resources Division, Investigative Applications Support Unit
Investigative Accounts:	Criminal Investigative Division, Corruption/Civil Rights Section, Undercover and Sensitive Operations Unit
(Major Cases)	National Security Division, Special Surveillance Group (SSG), FCI/CT Lookout & Undercover Support Unit (NS-5D)

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

11-7.8 Glossary

ACS	Automated Case Support.
Appropriate authority	In this document, appropriate authority refers to FBIHQ or field office management (i.e., Section Chief or higher at FBIHQ; SAC in the field office).
Authorized Purposes	Those purposes for which government property is made available to the public or purposes authorized in accordance with law or regulation

	(see Title 5, C.F.R., Section 2635.704(b)(2)).
CFR	Code of Federal Regulations.
Download	To transmit a file or program from a central computer to a smaller computer or a computer at a remote location.
ECF	Electronic Case File. A component of ACS. ECF serves as the central electronic repository for the FBI's official investigative textual documents. ECF provides the capability to upload word processing documents to the mainframe, where they are then filed and serialized.
Electronic Mail	Also referred to as E-mail, is the most frequently used communications tool on the Internet. E-mail are messages that are sent by computer from one person to another, then saved until the recipient chooses to read them. E-mail arrives immediately and does not require the recipient to be present, nor does it interrupt anything else the recipient may be doing.
FRA	Federal Records Act.
Internet	The Internet is an interconnection of computer networks that enables connected machines to communicate directly with one another. It connects universities, research labs and commercial, military and government sites around the world. Users of the Internet can exchange E-mail as well as send files to one another.
Internet Account	In this document, any Internet account that is paid for by the FBI (does not include accounts used in investigative, covert, or other specialized investigative uses).
Multiuser	When more than one user accesses the same FBI system or account.
NARA	National Archives and Records Administration.
Password	A secret character string that is required to log onto a computer system, thus preventing unauthorized individuals from obtaining access to the computer. Passwords are used to authenticate.
Research	Research, in this document, refers to the collection and maintenance of publicly accessible information for job-related purposes

	but does not include the collection and maintenance of information that is intended to be covert or that which is related to any other specialized investigation that requires authorization from an FBI official.
Sensitive Information	Information that requires protection due to the risk or magnitude of loss or harm that could result from inadvertent or deliberate disclosure, modification and/or destruction of information. Also referred to as Sensitive but Unclassified Information and Limited Official Use Information. (See MIOG, Part II, 35-12.)
Transmission Data	Sometimes referred to as Receipt Data. Can include information such as the date and time message was sent, date and time message was read, acknowledgment by recipient and the identities of senders and recipients. For messages where senders/recipients are identified by "handle" or distribution list, address group, or the like, the means to identify the associated names must also be included.
USPS	United States Postal Service.
WWW	World Wide Web. The entire constellation of resources that can be accessed by Gopher, FTP, HTP, WAIS and other search tools.|

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

********** END OF REPORT **********

RCFP-223

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

| |288-5 INVESTIGATIVE STRATEGY AND TECHNIQUES

| (1) COMPUTER INTRUSION INVESTIGATIVE TECHNIQUES

| Computer Intrusion investigations lend themselves to a number of investigative techniques in order to attribute actions to a subject, collect evidence and discern motive, and determine an investigative course of action. Further detailed examples are contained in the DOJ ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS. Some of the information in the following section was derived from this DOJ policy. (See also MIOG, Part 2, 10-18 through 10-18.6.)

| (a) PUBLICLY ACCESSIBLE INFORMATION

| Law enforcement agents may obtain information from publicly accessible online sources and facilities under the same conditions as they may obtain information from other sources generally available to the public. Obtaining information from online facilities configured for public access is a minimally intrusive law enforcement activity. For Fourth Amendment purposes, an individual does not have a reasonable expectation of privacy in information he or she has made available to the general public (such as a personal "home page" on the web). Similarly, an individual does not have a reasonable expectation of privacy in personal information that is generally made publicly available by others (such as publicly available Internet telephone directories).

| (b) IMPLIED CONSENT AND WARNING BANNERS

| Warning banners or sign-on banners may facilitate prosecution of intruders into computer networks by obtaining consent for keystroke monitoring. Banners can eliminate a reasonable expectation of privacy when included in an employment policy and if the user(s) was on notice as to their legal rights.

| Consent may be expressed or implied. Implied consent exists when circumstances indicate that a party to a communication was "in fact aware" of monitoring, and nevertheless proceeded to use the monitored system. In most cases, the key to establishing implied consent is showing that the consenting party received notice of the monitoring, and used the monitored system despite the notice. Proof of notice to the party generally supports the conclusion that the party knew of the monitoring. Absent proof of notice, the government must "convincingly" show that the party knew about the interception based on surrounding circumstances in order to support a finding of implied consent. Sections 2511(2) (c) and (d) permit any "person" who is a "party to the communication" to consent to

monitoring of that communication.

In computer cases, the implied consent doctrine permits monitoring of a computer network that has been properly "bannered." A banner is a posted notice informing users as they log on to a network that their use may be monitored, and that subsequent use of the system will constitute consent to the monitoring. Every user who sees the banner before logging on to the network has received notice of the monitoring: by using the network in light of the notice, the user impliedly consents to monitoring pursuant to Title 18, USC, Section 2511 (2)(c)-(d).

The scope of consent generated by a banner generally depends on the banner's language: network banners are not "one size fits all." A narrowly worded banner may authorize only some kinds of monitoring; a broadly worded banner may permit monitoring in many circumstances for many reasons. In deciding what kind of banner is right for a given computer network, system providers look at the network's purpose, the system administrator's needs, and the users' culture. For example, a sensitive Department of Defense computer network might require a broad banner, while a state university network used by professors and students could use a narrow one.

(c) COMPUTER SYSTEM LOGS

Computers used to allow or facilitate Internet access often contain stored logs which describe connection information. These logs are often volatile and overwritten frequently. There is no standard policy among computer network administrators on what logs to maintain, or what information is contained therein, but these logs are usually the first piece of evidence which must be analyzed in order to determine the source of an intrusion. System Administrators have the right to perform functions necessary to protect their networks including steps to identify the origin or identity of the violation. Law enforcement can accept log information that has been collected by the victim/System Administrator. However, after law enforcement becomes involved, the System Administrator may become an extension of the government if Agents direct him/her to perform tasks such as obtaining subscriber information from upstream/downstream network administrators or initiating electronic surveillance. These procedures would be in violation of the Title III unless the monitoring meets the four requirements of Title 18, USC, 2511(2)(i), the "Computer Trespasser Exception."

1. COMPUTER TRESPASSER: MONITORING HACKER ACTIVITY UNDER TITLE 18, USC, SECTION 2511(2)(I)

In network intrusion cases only, the owner or operator of the victim computer may authorize law enforcement to intercept the communications of a "computer trespasser" transmitted to, through, or from a "protected computer." But before monitoring can occur, four requirements must be met:

a. the owner or operator of the protected

computer must authorize the interception of the trespasser's communications;

b. the person who intercepts the communication must be lawfully engaged in an ongoing investigation;

c. the person acting under color of law must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation; and

d. such interception does not acquire communications other than those transmitted to or from the computer trespasser. In other words, investigators are permitted to intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of nonconsenting users authorized to use the computer.

A "computer trespasser" is any person who accesses a protected computer without authorization, and explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." Title 18, USC, Section 2510(21). For example, certain Internet service providers do not allow their customers to send back unsolicited e-mails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers - both because they use authorized users and because they have an existing contractual relationship with the provider.

A "protected computer" is defined in Title 18, USC, Section 1030 as any computer used in interstate or foreign commerce, as well as most computers used by financial institutions or the U.S. government. Thus, almost any computer connected to the Internet qualifies as a "protected computer."

(d) PEN REGISTERS

A pen register, or dialed number recorder, is used to identify telephone, or modem, connections placed from a subject's physical location. Usually obtained through a court order, this is the least intrusive method used to link a subject at a physical location to connections to an Internet Service Provider (ISP). By recording the telephone calls placed from a subject's location, and linking them to the records of an ISP subscriber account, such as America Online, evidence can be collected to be used for probable cause in an affidavit for search warrant of the physical location.

NATIONWIDE EFFECT: A pen register/trap and trace order has nationwide effect. It may be used to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order. For example, the

order would apply to all service providers involved in processing communications to the target. In some circumstances, an Agent may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path in order to convey it to the next carrier in the chain. The Agent would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier. The second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order has been served on the originating carrier who is able to identify the actual source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. Section 3123 therefore requires that, if a service provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

A court may also authorize the installation and use of pen/trap devices outside the jurisdiction of their district. For example, if an investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

REPORTING REQUIREMENT: If a law enforcement agency installs and uses its own pen/trap device on a packet-switched data network of a provider of electronic communication service to the public, the law enforcement agency must report the following information to the court ex parte and under seal within 30 days after termination of the order (including any extensions thereof): (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) the information collected by the device. (Title 18, USC, Section 3123(a)(3))

(e) 2703(F) LETTERS

Title 18, USC, Section 2703(f) provides the vehicle for investigators to preserve records that are under the care, custody, and control of a provider of wire or electronic communication services or a remote computing service. These are formal letters from the agency (FBI) requesting that the recipient make every effort to preserve records (primarily transaction/activity logs) pending the issuance of a court order or subpoena.

(f) 2703(D) COURT ORDERS

Court orders under Title 18, USC, Section 2703(d), are used to obtain contents of a wire or electronic communication, as well as records or other information held by

providers of electronic communication service and remote computing service, which are relevant and material to an ongoing criminal investigation. This includes the contents of, and the transactional and other stored data from, electronic communications (e.g., as preserved by a 2703(f) letter above). This would include logged connections, session activities, opened e-mail, etc. Subscriber information can be obtained through a Federal Grand Jury subpoena, as outlined below, or included in the 2703(d) court order.

A court order under 2703(d) requires specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

NOTICE:

Agents who obtain a court order under 2703(d), must either give prior notice to the subscriber, or else comply with the delayed notice provision of Section 2705.

(g) FEDERAL GRAND JURY SUBPOENAS

Federal Grand Jury subpoenas can be used in criminal computer intrusion investigations to obtain subscriber information, financial records, or mail and telephone records. Federal Rule of Criminal Procedure 6(e) attaches to the evidence collected under this method and only personnel on the Grand Jury 6(e) list, maintained by the United States Attorney's Office, may have access to the 6(e) material. This is usually the fastest method for evidence collection. However, other compulsory process should be considered (e.g., an order under Section 2703(d)) so that the information obtained will not be subject to the 6(e) secrecy rules and may be more readily used for victim notification in circumstances when such notification might prevent further crime or mitigate the effects of past criminal activity (e.g., to notify a victim that their data may have been altered).

(h) SEARCH WARRANTS

Search warrants are the most intrusive, though perhaps the most effective method, of obtaining evidence in 288 matters. Once probable cause has been established to show (1) a crime has been committed and (2) evidence or fruits of that crime are believed to be at a specific (physical) location at a specific time, an application for search warrant can be prepared and presented to a U.S. Magistrate Judge. Search warrants should be used to seize the subject's computer equipment, all storage media, as well as offline documentation, manuals, notes, and memoranda that may be relevant in the investigation. All computer-related search warrants should be executed and coordinated with Computer Analysis and Response Team (CART) members, who specialize in the seizure of computer hardware and electronic evidence.

(i) ONLINE COMMUNICATIONS (See MIOG, Part 2, 10-18.1.)

1. Consensual communications that occur online are not conceptually different from other types of consensual communications, and should be treated the same under agency regulations or procedures. Just as an individual orally discussing a past or future criminal activity assumes the risk that the other party is cooperating with law enforcement and recording the conversation, the individual engaged in an electronic dialogue with a party assumes the same risks.

2. Online Chat Rooms/Internet Relay Chat (IRC)

Public chat rooms, IRC channels, and similar sites are most analogous to public meetings in physical space. Attendance may be unrestricted, and the purpose is to exchange ideas and information. In chat rooms the discussion takes place in real time, and the underlying method of distributing chat room communications does not require storage. These features create an environment that encourages the immediacy and spontaneity typical of an in-person dialogue, even though participants know that they or others can create a transcript of their discussions by turning on their computer's logging function.

Different guidelines exist for passive monitoring of public chat versus active participation in chat discussions. Cooperating Witnesses and Undercover Agents may engage in chat sessions with predicated subjects, which should be covered through execution of a consensual monitoring form (see MIOG, Part 2, 10-10.2). Special Agents should not routinely monitor chat sessions outside of a properly predicated investigation. Rather, passive monitoring of public chat rooms should be considered at the discretion of FBI supervisors under the same circumstances as attending public meetings, with due attention to the types of discussions, the probability that law enforcement participation might be discovered, the potential infringement of rights guaranteed by the First Amendment and the effect that undisclosed FBI participation might have, the need to obtain the information, and investigative options.

(j) UNDERCOVER COMMUNICATIONS (See MIOG, Part 2, 10-18.1 and 10-18.5.)

Special Agents communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when FBI guidelines would require such disclosure if the communication were taking place in person or over the telephone. Special Agents may communicate online under a nonidentifying name or fictitious identity if FBI guidelines and procedures would authorize such communications in the physical world. Agents should review the FBI's Undercover Guide for a detailed discussion relating to communications and the definition of "contacts," as well as the DOJ ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS.

(k) TITLE III

Title III intercepts are usually a last method

| of investigation due to their intrusive nature. This technique has
| been successfully utilized in computer intrusion investigations.
| Data and voice intercepts are highly technical and require a great
| amount of specific justification and oversight.

| Agents considering implementation of a Title III in a computer
| intrusion investigation should notify CIU as soon as possible in
| order to coordinate and facilitate this process.

| (1) USE OF UNDERCOVER AGENTS AND
| INFORMANTS/COOPERATING WITNESSES (CW) IN COVERT OPERATIONS

| An undercover operation (UCO) is defined as any
| investigation wherein an employee of the FBI or other law
| enforcement agency uses a concealed identity in conducting a series
| of related investigative activities over a period of time. In
| addition, a UCO can also incorporate a Cooperating Witness (CW)
| and/or Informant to act alone or in concert with an undercover FBI
| Agent or other law enforcement officer. Online activities for law
| enforcement raises new concerns such as the government's liability
| should it unwittingly become involved or associated with attacks and
| intrusions into foreign computer networks which can raise tremendous
| liability concerns and potentially be construed as an act of war.
| THEREFORE, CIU SHOULD BE INVOLVED AT THE ONSET OF ANY UCO REGARDING
| COMPUTER INTRUSION INVESTIGATIONS.|

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

| 288-5.1 Accessing Computer Records - Summary of Compelled Disclosure under Title 18, USC, Section 2703 (See MIOG, Part 2,|10-10.2,|10-18 through 10-18.6.)

(1) Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. Each mechanism requires a different threshold showing. The five mechanisms, ranking in ascending order of the threshold showing required, are as follows:

(a) Subpoena

(b) Subpoena with prior notice to the subscriber or customer

(c) Section 2703(d) court order

(d) Section 2703(d) court order with prior notice to the subscriber or customer

(e) Search warrant

(2) One feature of the compelled disclosure provisions of

ECPA is that greater process generally includes access to information that can be obtained with lesser process. Thus, a Section 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a Section 2703(d) order can compel (and then some). As a result, Agents generally can opt to pursue a higher threshold instead of a lower one. The additional work required to satisfy a higher threshold will often be justified, both because it can authorize a broader disclosure and because pursuing a higher threshold provides extra insurance that the process complies fully with the statute.

**EffDte: 09/30/2002 MCRT#: 1247 Div: CY Cav: SecCls:

| |288-5.1.1 Subpoena - ECPA Requirements

| Investigators can subpoena basic subscriber information.

| (1) ECPA permits the government to compel two kinds of information using a subpoena. First, the government may compel the disclosure of the basic subscriber information listed including:

| The name, address, local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number of other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for service (including any credit card or bank account number), of a subscriber to or customer of such service.

| (2) Secondly, Agents can also use a subpoena to obtain information that is outside the scope of ECPA such as an e-mail message that is saved on an employer's server wherein the company did not provide "electronic communication service" with respect to that communication because the communication had reached its destination (i.e., been retrieved and subsequently stored) and the company did not provide computer storage or processing services to the public. Accordingly, Section 2703 does not impose any requirements on its disclosure, and investigators can issue a subpoena compelling the company to divulge the communication just as they would if ECPA did not exist. Similarly, information relating or belonging to a person who is neither a "customer" nor a "subscriber" is not protected by ECPA, and may be obtained using a subpoena according to the same rationale.

| (3) NOTICE: A government entity receiving records with a subpoena is not required to provide notice to a subscriber or customer. However, a provider is not precluded from giving its customer notice of the subpoena unless the government requests delayed notification under Section 2705.|

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

| |288-5.1.2 Subpoena with Prior Notice to the Subscriber or Customer

| (1) Investigators can subpoena opened e-mail from a provider if they comply with the notice provisions of Section 2703(b)(1)(B) and Section 2705.

| (2) Agents who obtain a subpoena, and either give prior notice to the subscriber or else comply with the delayed notice provisions of Section 2705, may obtain:

| (a) everything that can be obtained using a subpoena without notice;

| (b) "the contents of any electronic communication" held by a provider of remote computing service "on behalf of . . . a customer or subscriber of such remote computing service" (Title 18, USC, Section 2703(b)(1)(B)(i) and Section 2703(b)(2)); and

| (c) "the contents of any electronic communication

| that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." (Title 18, USC, Section 2703(a))

| (d) As a practical matter, this means that Agents can obtain opened e-mail and other stored electronic communications not in electronic storage 180 days or less using a subpoena, so long as they comply with ECPA's notice provisions.|

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

| |288-5.1.3 Section 2703(d) Order

| (1) Agents need a Section 2703(d) court order to obtain account logs and other transactional records.

| (2) Agents who obtain a court order under Title 18, USC, Section 2703(d) may obtain:

| (a) anything that can be obtained using a subpoena without notice; and

| (b) all "record(s) or other information pertaining

| to a subscriber to or customer of such service (not including the
| contents of communications (held by providers of electronic
| communications service and remote computing service))." (Title 18,
| USC, Section 2703(c)(1))

| (3) A court order authorized by Title 18, USC, Section
| 2703(d) may be issued by any federal magistrate, district court or
| equivalent state court judge.

| (a) To obtain such an order, known as an
| "articulable facts" court order or simply a "d" order, the
| governmental entity must offer specific and articulable facts
| showing that there are reasonable grounds to believe that the
| contents of a wire or electronic communication, or the records or
| other information sought, are relevant and material to an ongoing
| criminal investigation.

| This section imposes an intermediate standard to protect on-line
| transactional records. It is a standard higher than a subpoena, but
| not a probable cause warrant. The intent of raising the standard
| for access to transactional data is to guard against "fishing
| expeditions" by law enforcement. Under the intermediate standard,
| the court must find, based on law enforcement's showing of facts,
| that there are specific and articulable grounds to believe that the
| records are relevant and material to an ongoing criminal
| investigation.

| As a practical matter, a one- to three-page factual summary of the
| investigation and the role that the records will serve in advancing
| the investigation usually satisfies this criterion. A more in-depth
| explanation may be necessary in particularly complex cases.

| (4) SCOPE OF THE ORDER

| Section 2703(d) orders are nationwide in scope, much
| like subpoenas. ECPA permits judges to enter Section 2703(d)
| orders compelling providers to disclose information even if the
| judges do not sit in the district in which the information is
| stored.|

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

| |288-5.1.4 Section 2703(d) Order with Prior Notice to the Subscriber or Customer

| (1) Investigators can obtain everything in an account
| except for unopened e-mail or voice mail stored with the Internet
| Service Provider (ISP) for 180 days or less using a Section 2703(d)
| court order that complies with the notice provisions.

| (2) Agents who obtain a court order under Title 18, USC,
| Section 2703(d), and either give prior notice to the subscriber or

| else comply with the delayed notice provisions of Section 2705, may
| obtain:

| (a) everything that can be obtained using a Section
| 2703(d) court order without notice; and

| (b) "the contents of any wire or electronic
| communication" held by a provider of remote computing service "on
| behalf of . . . a subscriber or customer of such remote computing
| service." (Title 18, USC, Section 2703(b)(1)(B), and Section
| 2703(b)(2))

| (3) As a practical matter, this means that the government
| can obtain the full contents of a subscriber's account except
| unopened e-mail or voice mail (which has been in "electronic

| storage" 180 days or less) using a Section 2703(d) court order that
| complies with the prior notice provisions of Section 2703(b)(1)(B).

| (4) Although prior notice serves important constitutional
| values, Agents can obtain an order delaying notice for up to 90 days
| when notice would seriously jeopardize the investigation. Agents
| may also apply for successive renewals of the delayed notice, but
| must apply to the court for extensions. The applicant must satisfy
| the court that "there is reason to believe that notification of the
| existence of the court order may . . . endanger() the life or
| physical safety of an individual; (lead to) flight from prosecution;
| (lead to) destruction of or tampering with evidence; (lead to)
| intimidation of potential witnesses; or . . . otherwise seriously
| jeopardize an investigation or unduly delay a trial." Importantly,
| the applicant must satisfy this standard anew every time the
| applicant seeks an extension of the delayed notice.|

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

| |288-5.1.5 Search Warrant

| (1) Investigators can obtain the full contents of an
| account with a search warrant. ECPA does not require the government
| to notify the customer or subscriber when it obtains information
| from a provider using a search warrant.

| (2) Agents who obtain a search warrant under Rule 41 of
| the Federal Rules of Criminal Procedure or an equivalent state
| warrant may obtain:

| (a) everything that can be obtained using a Section
| 2703(d) court order with notice; and

| (b) "the contents of a wire or an electronic
| communication, that is in electronic storage in an electronic

| communications system for one hundred and eighty days or less."
| (Title 18, USC, Section 2703(a))

| (3) In other words, Agents can obtain every record and
| all of the contents of an account by obtaining a search warrant
| based on probable cause pursuant to Fed. R. Crim. P. Rule 41. The
| search warrant can then be served on the service provider and
| compels the provider to divulge the information described in the
| search warrant to law enforcement. Notably, obtaining a search
| warrant obviates the need to comply with the notice provisions of
| Section 2705. Moreover, because the warrant is issued by a neutral
| magistrate based on probable cause, obtaining a search warrant
| effectively insulates the process from challenge under the Fourth
| Amendment.

| (4) SERVING THE WARRANT: As a practical matter, Section
| 2703(a) search warrants are obtained just like Rule 41 search
| warrants. As with a typical Rule 41 warrant, investigators must
| draft an affidavit and a proposed warrant that complies with Rule
| 41. Once a magistrate judge signs the warrant, however,
| investigators ordinarily do not themselves search through the
| provider's computers in search of the materials described in the
| warrant. Instead, investigators bring the warrant to the provider,
| and the provider produces the material described in the warrant.
| Before adopting this approach, however, consult the Chief Division
| Counsel (CDC) and applicable AUSA to discuss the process for serving
| the warrant prior to obtaining the warrant. It is recommended that
| you consider the following: 1) Speak with the legal compliance unit
| of the target ISP regarding their exact procedure for complying with
| 2703 search warrants; 2) Explain the ISP's compliance procedure in
| the search warrant application, and ask permission from the Court to
| execute the search warrant by fax or other desired means and obtain
| permission to utilize the assistance of the ISP legal compliance
| staff; 3) make sure the grant of that permission is explicitly added
| to the search warrant order itself, and 4) forward your contact
| information with the search warrant together with written
| instructions that they are to contact you if there is any ambiguity
| over what material in their possession falls within the ambit of the
| search warrant. Preserve all documents and written instructions and
| document all contacts with the ISP for later possible use in a
| suppression hearing to demonstrate the reasonableness of the search
| warrant's execution as executed with the assistance of the ISP
| staff.|

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

| |288-5.1.6 Voluntary Disclosure

| The voluntary disclosure provisions of ECPA appear in
| Title 18, USC, Section 2702. This statute governs when a provider
| can disclose contents and other information voluntarily, both to the

government and nongovernment entities. If the provider may disclose the information to the government and is willing to do so voluntarily, law enforcement ordinarily does not need to obtain a legal order to compel the disclosure. If the provider either may not or will not disclose the information, Agents must comply with the compelled disclosure provisions under Section 2703 and obtain the appropriate legal orders.

(1) Contents

(a) Providers of services not available "to the public" may freely disclose the contents of stored communications. Providers of services to the public may disclose the contents of stored communications only in certain situations.

(b) When considering whether a provider of remote computing service (RCS) or electronic communication service (ECS) can disclose contents, the first question Agents must ask is whether the services offered by the provider are available "to the public." If the provider does not provide services "to the public," then ECPA does not place any restrictions on the voluntary disclosure of contents.

(c) If the services offered by the provider are available to the public, then ECPA forbids the disclosure of contents unless:

1. the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service" (Section 2702(b)(5));

2. the disclosure is made "to a law enforcement agency . . . if the contents . . . were inadvertently obtained by the service provider . . .(and) appear to pertain to the commission of a crime" (Section 2702(b)(6)(A));

3. the Child Protection and Sexual Predator Punishment Act of 1998, Title 42, USC, Section 13032, mandates the disclosure (Title 18, USC, Section 2702(b)(6)(B));

4. the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay (Title 18, USC, Section 2702(b)(6)(c)); or

5. the disclosure is made to the intended recipient of the communication, with the consent of the intended recipient, to a forwarding address, or pursuant to a court order. (Title 18, USC, Section 2702 (b) (1)-(4)) (See Title 18, USC, Section 2702.)

In general, these exceptions permit disclosure by a provider to the public when the needs of public safety and service providers outweigh privacy concerns of customers, or else when disclosure is unlikely to pose a serious threat to privacy interests.

(2) Records Other than Contents

Whether a provider can disclose noncontent records depends first on who will receive the disclosure. ECPA permits providers to disclose "record(s) or other information pertaining to a subscriber to or customer of such service" voluntarily to anyone outside of the government for any reason. The rules permitting the disclosure of noncontent records to a government entity are considerably more narrow, however. For this reason, Agents should be extremely careful when communicating with network service providers in an undercover capacity so as not to violate ECPA. Likewise, when they are not in an undercover capacity, Agents should clearly identify themselves as law enforcement agents.

A provider may disclose noncontent records to a government entity:

(a) as may be necessarily incident to the condition of the service or to the protection of the rights or property of the provider (Section 2702(c)(3));

(b) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure (Section 2702(c)(4));

(c) with the lawful consent of the customer or subscriber (Section 2702(c)(2)); or

(d) as otherwise authorized by Section 2703.

**EffDte: 08/12/2002 MCRT#: 1206 Div: CY Cav: SecCls:

288-6 CYBER ACTION TEAM (CAT)

(1) CYBER INCIDENT RESPONSE CONCEPT

The cyber incident response concept involves a coordinated response to incidents by FBI field office NIPCIP Squads and a Cyber Action Team (CAT) located at FBIHQ. The cyber incident response concept will assist in a rapid, coordinated, effective investigative response to significant cyber incidents, whether criminal or counterintelligence related, involving multiple field offices. In addition to the coordination of investigative information, the CAT will be able to provide investigative, analytical, technical, and legal support and resources to field office NIPCIP squads conducting investigations related to a specific cyber incident.

A CAT is used in order to establish a procedure for the initial response and investigation of a computer intrusion, virus proliferation, denial of service, or other related significant cyber incidents involving widespread outages or the targeting of