ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-27-2015 BY J75J65T61 NSICG

(b) CREDIT RECORD HEADER INFORMATION - Credit Record Header information provides SKIP/TRACE, ADDRESS UPDATE, Social Security Account Number (SSAN) information, and other personal or business locator information based on name, social security number, or address information.
(c) ASSET INFORMATION - Information concerning personal and corporate assets, property ownership, Federal Aviation Administration (FAA) records by owner's name or by aircraft registration number, judgments, lawsuits, liens, Security and Exchange Commission (SEC) and Uniform Commercial Code (UCC) filings, corporation officers, water vehicle registrations for some states, case law, and news service libraries. Professional licensing information from some states, and deceased SSAN information is also available. Asset information is not available in an automated format for every county in every state.
(d) INFORMATION TO VERIFY SOCIAL SECURITY NUMBERS - Provides information regarding SSANs. A given SSAN can be checked to see if it falls with the range of active account numbers, approximately when it was issued, and from what state.
Information from the Social Security Administration on SSANs that have been reported as deceased, including the name that the SSAN was issued to, the address where the last death benefit was mailed, and the month and year of death.
(e) DUN & BRADSTREET - Provides information on domestic and international corporations, business credit, officers, primary banking relationships, and affiliations with other corporations.
(f) NATIONAL INSURANCE CRIME BUREAU (NICB) - Provides information based on vehicle, fire, property, and casualty insurance claims. Also, information is available on the date and place that a vehicle was manufactured and where the vehicle was first shipped, based on the vehicle identification number. This information is a prerequisite to determine federal jurisdiction for certain offenses such as carjacking. Such information can be obtained in an affidavit form or if necessary, an expert witness from NICB can provide testimony at trial.
(g) NCIC/NLETS/CCH - This is the same service available in all field offices and should still be searched routinely in the field office; however, for offline searches, fugitive investigations, and when specifically requested, the ITCs will have the capability to access this information.
(h) TECS II - Treasury Enforcement Communications System II provides information collected by U.S. Customs Agents, Treasury Agents, and Immigration and Naturalization Service Agents in the course of their investigations. This information can be searched by name and by various identification numbers. Border crossings into the United States may also be searched by individual's name and by vehicle license number or aircraft registration number.
(i) TOXNET - Provides information from the National Institutes of Health on the toxicology of substances, environmental risks of chemical substances, hazardous substances, registry of chemical properties, and Environmental Protection Agency notes on releases of toxic and hazardous chemicals.
(j) SENTRY - Bureau of Prisons on-line information system. Sentry has information on all inmates incarcerated in federal institutions since 1981. Available information includes admissions, transfers, housing, and work histories.
(k) FEDERAL TRADE COMMISSION - TELEMARKETING FRAUD DATABASE - Provides information on complaints received from the National Association of Attorneys General, Telemarketing Fraud Database. This information allows the aggregation and consolidation of complaints nationwide.

10-18 FBI PRINCIPLES AND POLICIES FOR ONLINE CRIMINAL INVESTIGATIONS (See also MIOG, Part 1, 288-5, 288-5.1; Part 2, 10-8.3 through 10-8.4; MAOP, Part 2, 11-7.)

(1) The following Principles address the FBI's use of electronic online services (online services) in criminal investigative and operational activities. Because existing policy can be applied to investigations that involve online communications, these Principles, in general, do not create new policy or rules but act as pointers to existing policy that will also apply to the use of online

services as investigative tools. The FBI's use of online services will not be inhibited by these Principles as long as online services are used with the same caution and sensitivity as other investigative techniques or tools. However, because the use of online services can affect more people than most current investigative tools, the development and implementation of online services as investigative tools should not be undertaken without consulting these Principles and other relevant policy provisions that are referenced herein. In addition, FBI employees should remember that the U.S. Constitution and the rules of criminal procedure are designed to protect U.S. citizens from actions by government actors, and not from the actions of nongovernment actors, and as a result FBI employees may be unable to utilize online services in the exact manner that nongovernment actors can. As with other investigative techniques, Agents must evaluate all risks, such as the risk of violating an individual's privacy, created by using the investigative technique prior to its utilization.
(2) These Principles apply to the FBI's use of online services such as the World Wide Web, electronic mailing lists, news groups, Internet Relay Chat, File Transfer Protocol (FTP), Gopher, Internet electronic mail (e-mail), or other similar online services.
(3) These Principles are also directly derivative of the Department of Justice ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS (DOJ Online Principles). For a more detailed discussion and examples of some of the Principles discussed herein, that document should be consulted.
(4) These Principles are set forth solely for the purpose of internal FBI guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitations on otherwise lawful investigative or litigative prerogatives of the FBI or DOJ.
(5) These Principles also do not limit FBI divisions from developing more restrictive or specific guidelines. In cases involving the investigation of child pornography, for example, there are more restrictive and specific guidelines that should be consulted and followed.
(6) Questions regarding these Principles and the use of online facilities for investigative purposes should be directed to the Investigative Law Unit, Office of the General Counsel (OGC), FBIHQ.
(7) These Principles do not apply to FBI Foreign Counterintelligence (FCI) or International Terrorism (IT) investigations. Questions regarding FCI or IT investigations and the use of online services should be directed to the National Security Law Unit, OGC, FBIHQ, Room 7975, Extension 3951.

10-18.1 Online Communications (See MIOG, Part 1, 288-5, 288-5.1.)

(1) THE FBI'S USE OF ONLINE COMMUNICATION SERVICES
(a) GENERAL PRINCIPLES
1. FBI employees are not prohibited from using online services either for official activities or for personal activities. However, FBI employees who do use online services for official activities must do so in accordance with these Principles and existing FBI policy.
2. Online communications/activities undertaken for any official purpose must be conducted pursuant to these Principles even if the investigative activity is conducted from a non- Bureau facility. As a general rule, all undercover online activity or other covert activity must be conducted using accounts and equipment obtained and authorized pursuant to FBI undercover and other procedures.
(b) LIMITATIONS ON USE
1. FBI policy limits the use of government property to those purposes that are authorized. Therefore, FBI employees must use online services provided by the FBI only for authorized purposes. Authorized purposes are those purposes for which government property is made available or for those purposes authorized in accordance with law or regulation. (Authorized purposes include personal uses that involve only a negligible expense (such as electricity, ink, small amounts of paper, and ordinary wear and tear) and limited personal telephone/fax calls to locations within the office's commuting area, or that are charged to nongovernment accounts.) All government property, including online service facilities, fall within this prohibition. See Manual of

Administrative Operations and Procedures (MAOP), Part 1, 1-3. Also see January 13, 1997, Memorandum for Department of Justice Employees from Stephen R. Colgate, Assistant Attorney General for Administration regarding personal use of the Internet.
2. Because FBI employees are considered to be on-duty when conducting any official activity related to their official duties, any online activity undertaken from a location other than official FBI space to further official objectives must be conducted pursuant to the same rules/policies that would apply if the same activity were conducted from an official FBI space or an FBI facility. In addition, for security reasons, any official investigation should be conducted using only FBI accounts and FBI equipment. In particular, when conducting undercover activity outside of Bureau space, such activity must be conducted using covert FBI equipment with FBI supervisory approval. This policy, however, is not intended to discourage, limit, or otherwise prohibit personal use of the Internet or other available online services. However, when conducting official activity, or when in the course of personal use, employees encounter information that should be investigated or referred to another law enforcement agency, employees should follow all applicable FBI policies and guidelines.
(For a more detailed discussion of the consensual monitoring of electronic communications see Principle #10 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)
(c) USING ONLINE FACILITIES. Where there is no specific policy or guideline that addresses any particular aspect of online communications, FBI employees must follow the same practices and procedures used when communicating over the telephone and when disseminating material through the mail. FBI employees should also be familiar with the following policies that will apply to the use of online communication services:
1. ONLINE IDENTIFICATION. In general, the same policies and procedures apply with respect to when or how an FBI employee identifies himself/herself online. There are specific policy guidelines that address the use of false names or cover identities as well as when FBI SAs are required to show witnesses their credentials. See further discussion below in (3) and 10-18.5.
2. THE DISSEMINATION OF INFORMATION. Online services facilitate the transmission of more information than is capable of being transmitted over the telephone and make it easier to transmit written documents. When communicating online, FBI employees must follow FBI policy regarding the dissemination of information, written and oral. This includes any policy regarding the uploading of graphic images or photographs. A discussion of that policy is found below in 10-18.4. See also MAOP, Part 2, Section 9.
3. THE RETENTION OF INFORMATION. The FBI is required to preserve all federal records in accordance with the General Records and Retention Schedules promulgated by the National Archives and Records Administration. FBI employees must determine whether e-mail messages, attachments, and transmission data are federal records and whether they must be retained. In addition, FBI employees must maintain the same documentation that they would maintain if the information were gathered over the phone. As a general rule, the same policies and practices that would be followed for producing an FD-302, insert, etc., should apply when using online services. A discussion of when information is a federal record and when it must be retained is found below in 10-18.4. See MAOP, Part 2, Section 2. FBI policy on the administrative use of Internet/Internet e-mail was disseminated in an electronic communication (EC) dated December 5, 1997 (see MAOP, Part 2, 11-7). FBI E-mail policy dated March 1998 was provided via a March 12, 1998, EC captioned "ELECTRONIC MAIL (E-MAIL) POLICY," Bufile 66F-HQ-A1144420, Serials 2 and 3.
(d) INTERNET SURFING. "Surfing" the Internet, in this instance, means browsing or otherwise accessing publicly available Internet sites and locations.
1. INTERNET SURFING FOR INVESTIGATIVE PURPOSES. Surfing for investigative purposes means surfing the Internet for the purpose of obtaining information regarding possible criminal activity. FBI employees may surf the Internet for investigative purposes as long as the activity is conducted pursuant to the Attorney General's Guidelines on General Crimes, Racketeering and Terrorism Enterprise Investigations (General Crimes Guidelines). Those Guidelines authorize three types or levels of investigative operations: (1) the "prompt and extremely limited checking out of initial leads"; (2) the "preliminary inquiry"; and (3) the "full investigation." A full investigation

may be conducted where "facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed;" a standard that is "substantially lower than probable cause." Where there is insufficient evidence to establish a "reasonable indication" of criminal activity, but where there is a "possibility" of criminal activity, a preliminary inquiry may be initiated. The lowest level of permissible action is where an Agent has even less information, i.e., where "responsible handling requires some further scrutiny beyond the prompt and extremely limited checking out of initial leads." For example, an Agent responding to a complaint, lead, or other information about possible criminal activity could visit relevant sites on the Internet as part of the "prompt and extremely limited checking out of initial leads."

The permissibility of surfing activity by FBI employees depends upon the investigative authority provided in the General Crimes Guidelines and all investigative activity must be commensurate with that authority. As a general rule, the degree of intrusiveness of any investigative technique should increase incrementally according to the specificity of the evidence or allegation. The General Crimes Guidelines are statements of policy, which precisely balance individual interests in First Amendment and other protections with the need for effective law enforcement. Surfing the Internet is not illegal. However, because it is FBI policy to carefully balance the need for investigative activity with, among other things, First Amendment rights, FBI employees should follow the General Crimes Guidelines to ensure that carefully crafted balance is not unnecessarily compromised.

2. While there is no legal bar to the FBI's access to public information on the Internet because the Internet is in the public domain, the FBI's use and access is circumscribed by the Privacy Act which specifically addresses the collection and retention of certain information. (See MIOG, Part 2, 10-18.4.)

3. Although it is legally permissible to access public information via the Internet, the collecting and maintenance of records may be illegal depending upon the purpose for which the records are collected and maintained.

4. INTERNET SURFING FOR NONINVESTIGATIVE PURPOSES. This principle does not limit Internet surfing for training or noninvestigative research and analysis as long as the surfing activity is in support of an authorized law enforcement activity and as long as that activity is accomplished in accordance with applicable FBI policy.

(For a more detailed discussion of the consensual monitoring of electronic communications see Principles #5, #6, #8, and #9 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)

(2) REAL-TIME COMMUNICATIONS/INTERNET RELAY CHAT (IRC).

(a) GENERAL PRINCIPLE. FBI Special Agents (SAs) may participate in or observe real-time electronic communications (IRC or other chat sessions) to which they are a party, when it is pertinent to and within the scope of an authorized law enforcement activity.

(b) LIMITATIONS. FBI SAs should obtain supervisory approval to participate in or observe IRC sessions if being conducted for investigative or case-related purposes or if an Agent plans to access the Web site of an established group. Because of the potential First Amendment issues that may arise when participating in group activities, FBI Supervisors should carefully evaluate FBI SAs' participation in IRC sessions that are conducted by a recognized organization or group, such as a militia group.

(c) FBI POLICY. FBI Policy and the General Crimes Guidelines govern all FBI criminal investigative activity. Although participating in or observing real-time online communications, such as IRC, is not addressed specifically by existing FBI policy or the General Crimes Guidelines, the General Crimes Guidelines do allow the FBI to use any lawful investigative technique as long as the FBI has considered whether the information could be obtained in a timely and effective way by less intrusive means. In addition, the General Crimes Guidelines specifically provide that the choice of a particular technique is a matter of judgment.

Some real-time communications, such as chat-room discussions, are comparable to attending or participating in an anonymous discussion group or attending a public meeting, and participating in these type of electronic communications raises several issues, one of which is the potential

infringement of rights guaranteed by the First Amendment and the effect that undisclosed FBI participation would have on such meetings. As a matter of policy, FBI participation and attendance in public meetings is an investigative technique left to the discretion of FBI supervisors. Similarly, FBI participation in IRC or similar communications should be left to the discretion of FBI supervisors.
When deciding whether this investigative technique should be utilized, FBI employees should consider the type of discussion, the probability that law enforcement participation might be discovered, the effect on other participants' First Amendment rights, the need to obtain the information, and other less intrusive alternatives to obtain the information.
In addition, FBI employees should consult FBI policy regarding the monitoring of electronic communications.
(For a more detailed discussion of the consensual monitoring of electronic communications see Principles #3, #6, #8, and #9 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)
(3) ONLINE IDENTIFICATION
(a) GENERAL PRINCIPLES. FBI employees must disclose their affiliation when conducting interviews online. Interviews conducted over an online communication facility should be approved by the appropriate FBI supervisor.
(b) FBI POLICY. Credentials must be exhibited to all persons interviewed by SAs so there will be no doubt concerning their connection with the FBI. Manual of Investigative Operations and Guidelines (MIOG), Part 2, 7-1. The disclosure of FBI affiliation should be left to the discretion of the SA and should be handled in the same manner that an SA would identify themselves in any other situation. In general, however, SAs should disclose their law enforcement affiliation when necessary to inform the other party that he/she is communicating with a law enforcement official. For example, when an FBI employee is not an active participant in a conversation but is nonetheless present at the conversation, an FBI employee may be required to identify himself/herself depending upon the purpose of the activity. For instance, if the FBI employee were participating in an interview being conducted by another agency, the FBI employee would be required to identify himself/herself. On the other hand, if the FBI employee were present at a conversation taking place in a bar or a restaurant, the FBI employee is most likely not required to identify him/herself. The same rules would apply online. FBI employees who are simply "lurking" in a chat room are not required to identify themselves. But FBI employees who are communicating with someone on a one-on-one basis may be required to identify themselves depending upon the nature of the activity involved.
1. In certain circumstances, the use of a false name or cover identity may require separate approval. See the discussion below in 10-18.5 regarding "Undercover Online Communications."
2. Interviews or investigations conducted through an electronic online communications facility are essentially the same as interviews or investigations conducted over the phone and therefore subject to the same rules. However, because there are less indicia to confirm identity and thus little confidence as to the true identity of the person, an FBI employee considering interviewing a person online should consult with his/her supervisor and if necessary, obtain prior approval. Given the lack of confidence in online identification the FBI's use of online services to conduct an official interview should be limited and circumspect.
3. Online identification can, under most circumstances, be viewed as one of the following, and depending on the purpose of the communication different rules apply.
a. "Official identification." As a general rule, FBI employees should use online communication facilities in accordance with the same practices and procedures they use when communicating by telephone or mail. When communicating online in an official capacity (e.g., with a witness, other agency, or members of the public) FBI employees should identify themselves as FBI/government personnel, unless otherwise authorized. In such circumstances, FBI employees should expressly identify themselves as FBI or federal government employees either by adding a specific reference in the body of the communication or by using an identifying e-mail address such as FBI.GOV.

b. "False identification." Online communications facilities make it much easier to assume a false or fake identification; not using the identification of a real person but creating a false of fake identity. Thus, when adopting a false persona or other cover identity, FBI employees should, if relevant, follow appropriate FBI policy regarding the use of false names and cover identities. See the discussion below in 10-18.5 regarding Undercover Communications and the Attorney General's Guidelines on FBI Undercover Operations (FBI Undercover Guidelines).
c. "Anonymous identification." When authorized and appropriate, nonidentifying communications may also be used. For example, it may be appropriate for FBI employees not to broadcast their identity (e.g., through a user or account name that identifies them as FBI). In such circumstances, it is permissible to obtain and use an Internet account that does not reveal the user's FBI affiliation. For example, an FBI employee can use such an account to access publicly available information on the Internet including visiting Web sites or news groups to conduct research or obtain other information where identity is not an issue.
d. "Pretextual identification." It is also recognized that there are certain circumstances when the use of pretext phone calls may be appropriate. In these circumstances it may be appropriate for FBI employees not to identify themselves as an employee of the FBI. Pretextual contacts such as these are permissible on the Internet to the same extent that they are permitted for telephonic or in-person communications. Such techniques would be permitted when a Web site or other publicly available Internet resource attempts to exclude law enforcement personnel by conditioning access on the user's statement of nonaffiliation with law enforcement.
(For a more detailed discussion of the consensual monitoring of electronic communications see Principle #6 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)

10-18.2 Monitoring Online Communications (See MIOG, Part 1, 288-5, 288-5.1.)

(1) CONSENSUAL MONITORING
(a) GENERAL PRINCIPLES.
1. Existing technology allows every participant in an IRC or chat session to record the session; thus, the recording of an IRC session can be compared to a public gathering where every participant or attendee is allowed to record the event.
2. All IRC or other chat sessions conducted during or for an investigation must be recorded or logged. In addition, where the communication is, or will be, evidentiary in nature, the communication must be downloaded to a disk and maintained in accordance with all relevant ELSUR policies and guidelines.
(b) FBI POLICY. It is not unlawful to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public. Title 18, USC, Section 2511(2)(g)(i). In addition, all real-time electronic communications can be recorded by all participants, and thus, the recording and logging of those conversations is a matter of routine. However, while online, individuals may, at any time, send a private message directly to another online participant. Because of this ability to send direct private communications while online in a public chat discussion, all real-time electronic communications must be recorded. In these types of discussions, where the IRC session is generally accessible to the general public and any participant can record, SAC approval is not required. However, for evidentiary purposes, other consensual monitoring guidelines/policy should be followed. SAs must still obtain the approval of their immediate supervisor and, if required, approval to use the monitoring equipment; normal ELSUR indexing procedures should be followed and the original recordings should be maintained and treated as ELSUR material.
In nonpublic or non-IRC/chat discussions, where the communication is limited to specific individuals, and is not readily accessible to the general public, monitoring should be conducted in accordance with FBI policy regarding telephonic consensual monitoring. See MIOG, Part 2, 10-10.2. Telephonic consensual monitoring requires SAC approval with Assistant United States Attorney (AUSA) concurrence.

(For a more detailed discussion of the consensual monitoring of electronic communications see Principle 3 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)
(2) NONCONSENSUAL MONITORING
(a) GENERAL PRINCIPLE. FBI employees must follow FBI Guidelines regarding nonconsensual monitoring/interception.
(b) FBI POLICY. Title III generally prohibits the nonconsensual interception of the contents of a wire, oral, or electronic communication through the use of any electronic, mechanical, or other device. Title 18, USC, Section 2511. However, there are statutory exceptions to this provision. Those exceptions allow nonconsensual interception if it is conducted pursuant to a court order, or another statutory exception. Finally, as noted above, a Title III court order is not required if the consent of a party to the communication has been obtained.
FBI employees should also note that the intentional disclosure of the contents of any communication by a person or entity providing an electronic communication service to the public, while in transmission, is specifically prohibited unless the disclosure is accomplished pursuant to a statutory exception. Title 18, USC, Section 2511(3).
It should also be noted that monitoring or collecting information gathered by joining the network such as when an individual joins a chat session, logs on/off, or where the individual is located or connecting from, is not content information but publicly available information that may be collected and maintained in accordance with FBI policy regarding the collection and maintenance of publicly available information. However, SAs should not obtain information such as login records, that under the Electronic Communications Privacy Act (ECPA), Title 18, USC, Sections 2511 et seq., cannot be provided to the government without the appropriate legal process.

10-18.3 Access to Stored Electronic Information (See also MIOG, Part 1, 288-5, 288-5.1; Part 2, 10-8.)

(1) OBTAINING INFORMATION FROM UNRESTRICTED SOURCES
(a) GENERAL PRINCIPLE.
1. FBI employees may OBTAIN information available from publicly accessible online sources and facilities under the same conditions as they may OBTAIN information from other sources generally available to the public. This applies equally to publicly accessible foreign cybersources.
2. Online information is available to the public if it is available to anyone willing to pay a subscription or other user fee in the absence of additional access restrictions.
(b) FBI POLICY. FBI policy limits the collection and maintenance of public source information in two ways.
1. First, the Privacy Act of 1974 limits the collection and maintenance of public source information if it describes how an individual exercises his/her First Amendment rights, unless it is related to an authorized law enforcement activity. This means that any FBI employee who is collecting and maintaining information of this type must be able to show that the information is related to an authorized law enforcement activity.
2. The General Crimes Guidelines outline the parameters of when information is "pertinent to and within the scope of an authorized law enforcement activity." Information may be collected and maintained and placed in the FBI's system of records so long as the General Crimes Guidelines have been followed, even if that information describes how an individual exercises his/her First Amendment rights. In addition, the General Crimes Guidelines do not preclude the collection and maintenance of information that is otherwise collected in conformance with the Privacy Act.
(For a more detailed discussion and examples of obtaining information from electronic sources see Principle 1 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)
(c) ACCESSING PUBLIC ONLINE SOURCES. FBI employees who utilize public online sources should ensure that the source is in fact a public source. Users should keep in mind the type of access that is required to gather the information and whether users are, or should be, aware that their communications are, or will be, widely available. If a particular password or other code, that is not available to the public, is required to access the source, FBI employees are prohibited from accessing the source unless the access is authorized by a federal statute or FBI policy.

(d) SOFTWARE TOOLS. Software tools (e.g., finger or other tools available through the UNIX operating system) that are available to the public are also available to investigating Agents. Software tools cannot be used to defeat the security system of the targeted electronic facility or access areas that are not already publicly viewable by general users of the system or the public absent a search warrant or other legal authorization.
Examples of information that may be obtained using software tools include: identifying information such as a host name (e.g., usdoj.gov); an IP address (e.g., 127.0.0.1); information that indicates whether a site is currently connected to a network; the path over a network between two host computers; the names of host computers on a subnetwork; the name associated with a user name; the time and date of a user's last login; the specific activity of a user who is currently logged into a system; and a user's postal address or telephone number.
Some of the information described above is open to view to system users. Other information will be made available depending upon the practice of the particular service provide. This information is normally controlled by the system administrator. Individual users are also capable of deciding what information to make available about themselves. In any event, it is not appropriate to use available software tools where such use would violate statutory restrictions, such as ECPA, which protects electronic communications, or to provide unauthorized access to records protected by the Right to Financial Privacy Act or the Fair Credit Reporting Act, which protect customer financial records and consumer credit information.
(For a more detailed discussion of obtaining information from unrestricted sources and examples see Principles 1 and 2 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)
(2) OBTAINING INFORMATION FROM RESTRICTED SOURCES
(a) GENERAL PRINCIPLE. FBI employees may not access restricted online sources or facilities unless there is legal authority permitting an entry into private space.
(b) FBI POLICY. FBI intrusion into private areas is governed, in general, by the Fourth Amendment, which protects individual privacy against certain kinds of governmental intrusions. The degree of protection provided to an individual in his/her person, or an area or possession, depends on the reasonable expectation of privacy manifested by the individual. In addition, by its terms, the Fourth Amendment requires that a search for or seizure of evidence must be reasonable. Since the authority of a warrant is the best assurance that a search will be deemed reasonable by the courts, FBI policy requires Agents to obtain a search warrant before searching for evidence. See Legal Handbook for Special Agents (LHBSA), 5-2.1, 5-2.2.19, 5-4.1. This policy, however, as previously noted, is subject to several exceptions, including search by consent. A search to which an individual consents meets Fourth Amendment requirements.
(c) EXAMPLES OF RESTRICTED ONLINE SOURCES include, but are not limited to:
1. Sites or services restricted by password or that limit authorized access to specifically identified individuals.
2. Real-time messages to specific individuals during a real-time chat session.
(d) ACCESSING RESTRICTED ONLINE SOURCES. Restricted online searches are similar to restricted access to other private places. Governmental intrusions into areas that have been designed to be private under circumstances in which the expectation of privacy is reasonable is a search. Thus, before entering into restricted online areas, FBI Agents should evaluate the facts to determine whether the area has been meaningfully restricted such that the restriction or attempt creates a reasonable expectation of privacy. Where there has been a meaningful restriction, FBI Agents should ensure that they obtain the appropriate legal process or otherwise have a valid exception allowing them to search that online facility. If consent is obtained, the scope of an online search, like a search of a physical location, is governed by the scope of the consent given. It is not unlawful, however, to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is accessible to the general public. Title 18, USC, Section 2511(2)(g)(i).
NOTE. A consent may be valid even if the person giving consent does not know the true identity of the person requesting consent. Therefore, an FBI employee acting in an undercover capacity is

not precluded from searching premises even if the employee gained consent using a false name or cover identity.
(e) STATUTORY RESTRICTIONS. Access to STORED electronic communications is governed by statute. A communication is in electronic storage when it is in any temporary intermediate storage incidental to its electronic transmission and when it is stored by an electronic communication service for purposes of backup protection. Title 18, USC, Section 2510(17). For example, e-mail is in electronic storage when it is stored by an electronic communications service, prior to the access of that communication by the ultimate addressee. Unlawful access to stored electronic communications, as well as the disclosure of the content of stored electronic communications, is specifically prohibited. See Title 18, USC, Sections 2701-2709. Governmental access to stored electronic communications is also specifically addressed in the statute and, in most cases, can only be obtained by government personnel by a court order, subpoena, or search warrant. For a more detailed discussion of the ECPA, see May 23, 1996, All SACs Airtel captioned "Electronic Online Services, Applications for Investigative Purposes."
(For a more detailed discussion of accessing restricted sources and examples see Principle 4 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)

10-18.4 Record Retention and Dissemination (See MIOG, Part 1, 288-5, 288-5.1, 288-9; Part 2, 10-18.1.)

(1) RECORD RETENTION
(a) GENERAL PRINCIPLE. FBI employees must preserve records of their online communications if the communication is a federal record. Such preservation must be consistent with the requirements of the Privacy Act.
(b) FBI POLICY. Other than the EC dated March 12, 1998, regarding E-mail policy, the FBI has no specific policy with respect to the retention and preservation of electronic records. However, to the extent that electronic records meet the definition of federal records, they must be preserved. Federal records include books, papers, maps, photographs, machine readable material, or other documentary material, regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business. The material must be 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. Title 44, USC, Section 3301.
In addition, Title 36 of the Code of Federal Regulations specifically governs the creation, use, preservation, and disposition of electronic records. Electronic records must include transmission data -- name of the sender, the addressee, and the date the message was sent. Information about the receipt of communications should be retained if users consider it necessary for adequate documentation of FBI activities.
All information received or made available to the FBI during the course of an investigation should be evaluated for its pertinence to the investigation and should be retained or preserved in accordance with the applicable FBI policy. An FBI employee who receives an electronic message and determines that the information is pertinent to an FBI investigation and that it is a federal record, should retain the communication, any attachments, and the essential transmission data. (For further guidance, see E-mail policy referenced in EC to all divisions dated March 12, 1998, Bufile 66F-HQ-A1144420 Serials 2 and 3.) This information should be printed and retained in the appropriate file or in a control file. If the electronic communications or attachments are in a form that will allow them to be unloaded into ACS, they must be loaded into the appropriate ACS component.
The Privacy Act provides that the collection, maintenance, use, or dissemination of records describing how an individual exercises his or her First Amendment rights is prohibited unless the information is pertinent to, and within the scope of, an authorized law enforcement activity. Records should not be placed into the FBI's system of records unless there is a predicated case via one of the levels of investigative response authorized by the AG Guidelines. This requirement

may not be avoided merely by placing all collected material into "zero files." As stated in the July 19, 1995, All SACs' airtel, "where no clear nexus to a law enforcement interest can be established, no record may be made of the information." If any material downloaded or printed from the Internet or a BBS is to be retained in Bureau files, it should bear a handwritten notation describing the reason it was collected and maintained. (See July 17, 1989, airtel to All SACs, "Legal Instruction Relating to First Amendment Activities Encountered in the Course of FBI Investigations.")

(c) PRESERVING RECORDS OF ON-LINE COMMUNICATIONS. FBI employees should comply with normal ELSUR indexing procedures and the original recordings should be maintained and treated as ELSUR material.

(2) ONLINE DISSEMINATION OF RECORDS/INFORMATION

(a) GENERAL PRINCIPLE. FBI employees must follow established FBI policy regarding the dissemination of information and should, if appropriate, consult with an appropriate supervisor prior to the dissemination of any FBI information.

(b) FBI POLICY. The dissemination of FBI information is governed by MAOP, Part 2, 9-3. The dissemination of information from FBI files must be accomplished in accordance with the Privacy Act and FBI guidelines.

The dissemination of information to federal judicial and legislative agencies, as well as to state and local agencies, is not prohibited as long as such dissemination does not jeopardize an ongoing FBI investigation or informant, and does not violate the Privacy Act. (See MAOP, Part 2, 9-3 (2).)

The dissemination of FBI information to a legitimate agency of a foreign government may be made where the FBI determines that the information is relevant to the agency's responsibilities, dissemination serves the best interests of the U.S. government, and where the purpose in making the disclosure is compatible with the purpose for which the information was collected and is not prohibited by law. (See MAOP, Part 2, 9-3 (3).)

The dissemination of public source material from FBI files is not prohibited if the information is pertinent and relevant, as long as the public source is fully identified. (See MAOP, Part 2, 9-4.4.2.)

In addition, the uploading of graphic images is also governed by FBI policy. Graphic images that contain pornographic or other suggestive issues should not be uploaded or disseminated via an online service without specific authority from a FBI supervisor. In addition, photographs or other images depicting an identifiable person should not be uploaded and disseminated without the written consent of the person depicted unless the proposed dissemination has been reviewed and approved by the relevant FBIHQ substantive section.

(For a more detailed discussion of online communications -- generally and examples see Principle 5 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)

10-18.5 Undercover Online Communications (See MIOG, Part 1, 288-5, 288-5.1; Part 2, 10-18.1 (1) and (3).)

(1) UNDERCOVER ONLINE COMMUNICATIONS GENERALLY

(a) GENERAL PRINCIPLE. FBI employees may communicate online using a false name or cover identity pursuant to applicable FBI policy.

(b) FBI POLICY. In general, the use of false names and cover identities is governed by the FBI Undercover Guidelines. As provided in those Guidelines, any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another federal, state, or local law enforcement organization working with the FBI is an undercover activity. A series of related undercover activities conducted over a period of time by an undercover employee is an undercover operation (UCO).

b7E -1

(c) DEFINING ONLINE CONTACTS FOR UCOS.

[redacted] b7E -1
[redacted] the current Undercover Guidelines.
In accordance with the current FBI Undercover Guidelines, an online UCO requires approval, as
[redacted]
Field divisions that have questions about whether online communications or exchanges have met this standard should coordinate with the Undercover and Sensitive Operations Unit (USOU) at FBIHQ.
(For a more detailed discussion of undercover communications and examples see Principle 6 and the accompanying commentary in the DOJ ONLINE PRINCIPLES.)
(2) ONLINE UNDERCOVER FACILITIES
(a) GENERAL PRINCIPLE. Technical questions regarding the development or implementation of undercover online facilities should be directed to the National Infrastructure Protection Center (NIPC), Criminal Investigations Unit; the substantive FBIHQ component; or the Engineering Branch, Laboratory Division.
Legal questions regarding the development and implementation of undercover online facilities should be directed to the Chief Division Counsel (CDC) or OGC, Investigative Law Unit (ILU).
(b) DEVELOPING ONLINE UNDERCOVER FACILITIES. The development and implementation of undercover online facilities raise many novel and sensitive legal and policy issues that may not arise in other UCOs. When developing online undercover facilities, FBI employees should keep in mind that most online facilities have the capacity to impact a large number of people. In all UCOs the impact on innocent third parties is a crucial factor that must be evaluated. This is also true in the development and implementation of online facilities that are used in an UCO. As a result, all reasonable steps must be taken to minimize impact on innocent third parties.
Another factor that must be considered in developing and implementing undercover online facilities is the impact on individual privacy. According to the General Criminal Guidelines, the impact on individual privacy must be evaluated in any UCO proposal. This factor is more significant in the utilization of online facilities in UCOs and FBI employees should continue to take reasonable steps to minimize the impact on individual privacy.
DOJ's CCIPS has defined an online undercover facility as including "a service provider, web site, or similar facility that is covertly run or sponsored by law enforcement and is intended to provide services to individuals who do not know they are dealing with law enforcement." Thus, online facilities that provide accounts or information only to individuals who know that the system is operated by law enforcement are not online undercover facilities.
(c) FBI POLICY. Oversight for FBI UCOs was granted to the Director who in his discretion may approve FBI UCOs [redacted] b7E -1
[redacted] Members from the Criminal Division, DOJ, may consult with appropriate FBI personnel, senior DOJ officials, and the United States Attorney as deemed appropriate in reviewing any FBI UCO. Each UCO application must be accompanied by a letter from the appropriate federal prosecutor indicating that he or she has reviewed the proposed operation, including the sensitive circumstances reasonably expected to occur, agrees with the proposal and its legality, and will prosecute any meritorious case that may develop. (Appropriate federal prosecutor means a United States Attorney or Section Chief in the Criminal Division of DOJ.) Pursuant to the FBI Undercover Guidelines, upon initiating and throughout the course of ANY UCO, the SAC or a designated Supervisory Special Agent (SSA) shall consult on a continuing basis with the appropriate federal prosecutor, particularly with respect to the propriety of the operation and the legal sufficiency and quality of evidence that is being produced by the activity.
Further, the DOJ Online Principles specify that agencies and prosecutors who are developing UCOs that are utilizing an online undercover facility, should consult early in the approval process

with CCIPS or the Computer Telecommunication Coordinator or CTC (each district has designated an AUSA to act as a CTC) in the district in which the operation is based. Therefore, either the SA who is developing an undercover online facility, or the AUSA with whom the Agent is working, is required to consult with the CTC or CCIPS, regarding legal issues that may arise in the use of the undercover online facility.
(For a more detailed discussion of the use of online undercover facilities and examples see Principle 7 and the accompanying commentary of the DOJ ONLINE PRINCIPLES.)
(3) CONSENSUAL APPROPRIATING OF IDENTITY
(a) GENERAL PRINCIPLE. With the consent of the person whose identity will be used, FBI employees may communicate online through the online identity of another person (e.g., user name) if such investigative activity is performed pursuant to the FBI Undercover Guidelines or other applicable policy.
(b) FBI POLICY. There is no specific FBI policy regarding the use of another person's identity. However, the FBI Undercover Guidelines define an undercover employee as an FBI employee whose relationship with the FBI is concealed from third parties in the course of an investigation by the maintenance of a cover or alias identity. Although not specifically contemplated by the FBI Undercover Guidelines, this definition would include the FBI's use of another person's online identity. Thus, the use of another person's online identity, under some circumstances, may implicate the Undercover Guidelines.
Whenever the identity of a CW will be used, the CW should expressly consent, in writing, to the use of his/her identity. This document should explicitly address the scope of that consent. For consent to be valid, consent should be obtained from all parties who are authorized to use the online identity. For example, the subscriber to an online account may provide other users who all may adopt different user names. In that instance, consent should be obtained from the subscriber and the user. Another factor is power to consent. For a consent to be valid, the party consenting must have the authority to consent. For example, in instances where the identity is that of a minor, consent should be obtained from a parent or guardian.
The use of another person's identity that does not fall within the FBI Undercover Guidelines is not prohibited as long as the use is consistent with FBI policy regarding the use of a false name or cover identity. For example, pretext phone calls are often used as an investigative technique. With the consent of the person whose identity will be used, FBI employees may make pretextual electronic communications.
(For a more detailed discussion about the consensual appropriating of identity and examples see Principle 8 and the accompanying commentary in the DOJ ONLINE PRINCIPLES.)
(4) APPROPRIATING ONLINE IDENTITY WITHOUT CONSENT
(a) GENERAL PRINCIPLE. FBI employees may not use another person's online identity without his/her consent unless prior approval has been obtained. Prior to using another person's online identity, FBI employees should obtain approval from USOU, which will consult with OGC before granting such approval.
(b) FBI POLICY. FBI Undercover Guidelines provide guidance concerning the use of another person's identity without their consent. CUORC review and approval is required when untrue representations by persons participating in a UCO concerning the activities or involvement of any third person, without that individual's knowledge or consent, are made. In this instance, such activity is considered a "sensitive circumstance," and requires Group I authority. Circumstances are considered sensitive if the undercover employee makes false or misleading representations about the activities of an innocent third party who is not involved in the activities which are the subject of the investigation, and there is a reasonable possibility that those representations may cause physical or financial harm to the third party or significant harm to his/her reputation. This sensitive circumstance acknowledges that a crucial issue in using another person's true identity is the potential to make affirmative misrepresentations that could negatively affect the individual's reputation or cause others to reasonably rely upon the representations to their detriment. For these reasons, the FBI rarely uses this investigative technique. However, if an FBI employee

desires to "borrow" someone's identity without his/her permission, prior approval from USOU, in consultation with OGC is required.
(c) LIMITATIONS. In instances where there is no UCO, the same analysis and rationale discussed above should apply. Activity that appropriates identity should not be undertaken unless such activity is conducted pursuant to a legitimate authorized activity and the appropriate approval has been obtained. In these instances, if time and circumstances permit, prior approval from USOU is required. In the event of exigent circumstances, the SAC or his/her designee may approve the activity and FBIHQ and CCIPS notified within 48 hours.
(For a more detailed discussion about the nonconsensual appropriating of identity and examples see Principle 9 and the accompanying commentary in the DOJ ONLINE PRINCIPLES.)

10-18.6 International Issues (See MIOG, Part 1, 288-5, 288-5.1.)

(1) ACCESS TO FOREIGN ONLINE FACILITIES
(a) GENERAL PRINCIPLE. FBI employees may obtain information from publicly accessible online sources and facilities that are located in foreign jurisdiction.
(b) FBI POLICY. There is no specific FBI policy regarding access to public information from foreign sources. However, accessing online information from foreign public sources is minimally intrusive and is therefore not prohibited if done in compliance with relevant FBI policy regarding the collection of public information. Persons or organizations who have made information available in this manner may be deemed to have voluntarily disclosed the information. Because information accessible through online sources is most often connected or linked to information from other sources, it is practically impossible to determine, prior to accessing the information, whether the information resides on a foreign or domestic facility. Therefore, FBI employees should follow the same rules when accessing foreign public sources that they would follow to access domestic public sources.
(2) ACCESS TO RESTRICTED FOREIGN ONLINE FACILITIES
(a) GENERAL PRINCIPLE. When FBI employees have information that leads them to reasonably conclude that a witness, subject, or restricted online facility with whom the employee is communicating, is located in a foreign jurisdiction, FBI employees must abide by all relevant FBI policies and procedures that apply to conducting extraterritorial investigations.
(b) FBI POLICY. The Attorney General's Guidelines for FBI Extraterritorial Operations and Criminal Investigations (Extraterritorial Guidelines) govern all extraterritorial criminal investigations conducted by the FBI. Routine extraterritorial FBI operations, i.e., investigations that do not involve one of the sensitive circumstances, can be approved by FBIHQ. However, extraterritorial criminal investigations that involve sensitive circumstances require the approval of the Attorney General.
In general, the level of approval for extraterritorial investigative activity will depend upon the level of intrusiveness of the investigative activity or investigative technique. To minimize the risk that FBI investigative activity utilizing an electronic communications facility will improperly invade the sovereignty of another nation, the intrusiveness of the activity must be minimized, the Extraterritorial Guidelines must be followed, and all applicable prior approvals must be obtained.
(For a more detailed discussion about accessing restricted foreign facilities and examples see Principle 11 and the accompanying commentary in the DOJ ONLINE PRINCIPLES.)

b7E -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-27-2015 BY J75J65T61 NSICG

10-8.3 Access to and Use of Electronic Communications Located on the Internet, E-Mail, and Bulletin Board Systems

This section was superseded by MIOG, Part 2, 10-18.

10-8.3.1 Definitions (See MIOG, Part 1, 139-1.1, and Part 2, 10-8.3.2.)

(1) The "Internet" shall be construed to mean the global network of electronic networks connecting computer users via telephone or other communication lines to information storehouses worldwide. Access to the network requires Internet software, the assistance of an Internet service provider, and the use of a communications link.
(2) "Bulletin Board Systems" (BBS) shall be construed to mean electronic networks of computers which are connected to a central computer, set up and operated by a system operator who has ultimate control over the BBS. The system is accessed by "dial-up" or by modem, and can be accessed by the general public, private persons granted BBS passwords, or both.
(3) "Electronic mail" or "e-mail" is a system that provides for the transmission of messages and files between computers over a communication network. The actual communication itself is addressed to a specific individual or group and requires a password for the communication to be viewed.

10-8.3.2 Interception of Electronic Communications (See MIOG, Part 1, 139-1.2)

(1) Deleted
(2) Pursuant to Title 18, USC, Section 2516, a court order is required for interception of all electronic communications.
(3) An interception occurs where the interception is:
(a) nonconsensual, and
(b) contemporaneous with the transmission.
(4) The definitions for violations of Title 18, USC, Section 2511 regarding the Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited can be found in MIOG, Part 1, 139-1.2.

10-8.3.3 Undercover Use of the Internet

This section was superseded by MIOG, Part 2, 10-18.5.

10-8.4 Monitoring the Internet

This section was superseded by MIOG, Part 2, 10-18.

10-9 ELECTRONIC SURVEILLANCE (ELSUR) PROCEDURES AND REQUIREMENTS

(1) Electronic surveillance is one of the most effective and valuable investigative techniques utilized in both criminal and national security investigative matters. To protect the use of this technique, the administrative and management controls contained in this section will receive the same meticulous oversight as does the informant program. Unless otherwise noted, it will be the responsibility of the case Agent and his/her supervisor to ensure compliance with these instructions. It should be clearly understood that the use of electronic surveillance requires (a) administrative or judicial authorization prior to its use, and (b) contact with the field office ELSUR support employee to coordinate all necessary recordkeeping, and (c) consultation with the Technical Advisor (TA) or a designated Technically Trained Agent (TTA) to determine feasibility, applicable technique, and the appropriate equipment.

10 (U//~~FOUO~~) SENSITIVE INVESTIGATIVE MATTER (SIM) AND SENSITIVE OPERATIONS REVIEW COMMITTEE (SORC)

10.1 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

10.1.1 (U) OVERVIEW

(U) Certain investigative matters should be brought to the attention of FBI management and Department of Justice (DOJ) officials because of the possibility of public notoriety and sensitivity. Accordingly, Assessments and Predicated Investigations involving "sensitive investigative matters" have special approval and reporting requirements.

10.1.2 (U) PURPOSE, SCOPE, AND DEFINITIONS

10.1.2.1 (U) DEFINITION OF SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U/~~FOUO~~) A sensitive investigative matter (SIM) is defined as an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), a religious or domestic political organization or individual prominent in such an organization, or the news media; an investigative matter having an academic nexus; or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of FBI Headquarters (FBIHQ) and other DOJ officials. (Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

(U//~~FOUO~~) The phrase ***"investigative matter involving the activities of"*** is intended to focus on the behaviors and/or activities of the subject, target, or subject matter of the Assessment or Predicated Investigation. The phrase is generally not intended to include a witness or victim in the Assessment or Predicated Investigation. This definition does not, however, prohibit a determination that the status, involvement, or impact on a particular witness or victim would make the Assessment or Predicated Investigation a SIM under subsection 10.1.2.2.7 below.

10.1.2.2 (U) DEFINITIONS/DESCRIPTIONS OF SIM OFFICIALS AND ENTITIES

(U) Descriptions for each of the officials and entities contained in the SIM definition are as follows:

10.1.2.2.1 (U) DOMESTIC PUBLIC OFFICIAL

(U/~~FOUO~~) A domestic public official is an elected official or an appointed official serving in a judicial, legislative, management, or executive-level position in a Federal, state, local, or tribal government entity or political subdivision thereof. A matter involving a domestic public official is a SIM if the Assessment or Predicated Investigation involves corruption or a threat to the national security.

Version Dated:
October 15, 2011

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2011 BY UC 60322 LP/PJ/SZ

RCFP-252

(U//~~FOUO~~) This definition is intended to exclude lower level positions and most line positions, such as a patrol officer or office secretary from the SIM category, but it does include supervisory personnel (e.g., police Sergeant or Lieutenant). The SIM definition also eliminates the "position of trust" language.

10.1.2.2.2 (U) Domestic Political Candidate

(U/~~FOUO~~) A domestic political candidate is an individual who is seeking election to, or nomination for election to, or who has authorized others to explore on his or her behalf the possibility of election to an office in a federal, state, local or tribal governmental entity or political subdivision thereof. As with domestic public officials, a matter involving a political candidate is a SIM if the Assessment or Predicated Investigation involves corruption or a threat to the national security.

10.1.2.2.3 (U) Domestic Political Organization or Individual Prominent in such an Organization

(U/~~FOUO~~)

b7E -1

10.1.2.2.4 (U) Religious Organization or Individual Prominent in such an Organization

(U//~~FOUO~~)

b7E -1

10.1.2.2.5 (U) Member of the News Media or a News Organization

(U/~~FOUO~~)

b7E -1

(U//~~FOUO~~)

(U//~~FOUO~~) Examples of news media entities include television or radio stations broadcasting to the public at large and publishers of newspapers or periodicals that make their products available to the public at large in print form or through an Internet distribution. A freelance journalist may be considered to be a member of the media if the journalist has a contract with the news entity or has a history of publishing content. Publishing a newsletter or operating a website does not by itself qualify an individual as a member of the media. Businesses, law firms, and trade associations offer newsletters or have websites; these are not considered news media. As the term is used in the DIOG, "news media" is not intended to include persons and entities that simply make information available. Instead, it is intended to apply to a person or entity that gathers information of potential interest to a segment of the general public, uses editorial skills to turn raw materials into a distinct work, and distributes that work to an audience, as a journalism professional.

(U//~~FOUO~~) If there is doubt about whether a particular person or entity should be considered part of the "news media," the doubt should be resolved in favor of considering the person or entity to be the "news media."

(U//~~FOUO~~) See the classified provisions in DIOG Appendix G for additional guidance on SIMs.

10.1.2.2.6 (U) ACADEMIC NEXUS

(U//~~FOUO~~)

A) (U//~~FOUO~~)

b7E -1

B) (U//~~FOUO~~)

(U//~~FOUO~~) The sensitivity related to an academic institution arises from the American tradition of "academic freedom" (i.e., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//~~FOUO~~)

b7E -1

10.1.2.2.7 (U) OTHER MATTERS

(U//~~FOUO~~) Any matter that in the judgment of the official authorizing an investigation should be brought to the attention of FBIHQ and other DOJ officials is also a SIM. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

Version Dated
October 15, 2011
RCFP-254

10.1.3 (U) FACTORS TO CONSIDER WHEN OPENING OR APPROVING AN INVESTIGATIVE ACTIVITY INVOLVING A SIM

(U//~~FOUO~~) In addition to the standards for approving investigative activity in Sections 5, 6, 7, 8 and 9, the following factors should be considered by (i) the FBI employee who seeks to open an Assessment or Predicated Investigation involving a SIM, as well as by the (ii) Chief Division Counsel (CDC) or Office of the General Counsel (OGC) when reviewing such matters, and (iii) the approving official when determining whether the Assessment or Predicated Investigation involving a SIM should be authorized:

A) (U//~~FOUO~~) Seriousness/severity of the violation/threat;

B) (U//~~FOUO~~) Significance of the information sought to the violation/threat;

C) (U//~~FOUO~~) Probability that the proposed course of action will be successful;

D) (U//~~FOUO~~) Risk of public exposure, and if there is such a risk, the adverse impact or the perception of the adverse impact on civil liberties and public confidence; and

E) (U//~~FOUO~~) Risk to the national security or the public welfare if the proposed course of action is not approved (i.e., risk of doing nothing).

(U//~~FOUO~~) In the context of a SIM, particular care should be taken when considering whether the planned course of action is the least intrusive method if reasonable based upon the circumstances of the investigation.

10.1.4 (U) OPENING DOCUMENTATION, APPROVAL, NOTICE, AND CHANGE IN SIM STATUS

(U//~~FOUO~~)

b7E -1

(U//~~FOUO~~) The following are required approval and notification levels for investigative activities involving SIMs:

10.1.4.1 (U) REVIEW AND APPROVAL OF SIM ASSESSMENTS BY A FIELD OFFICE

10.1.4.1.1 (U) TYPE 1 & 2 ASSESSMENTS

(U//~~FOUO~~) An FBI employee may open a Type 1 & 2 Assessment, as described in Section 5.6.3.1, without prior supervisory approval. A Type 1 & 2 Assessment involving a SIM must be reviewed by the CDC and approved by the Special Agent-in-Charge (SAC) as soon as practicable, but no later than five (5) business days after the opening to authorize the Assessment to continue.

10.1.4.1.2 (U) TYPE 3 AND 4 ASSESSMENTS

(U//~~FOUO~~) An FBI employee must obtain the following review and approval to open a Type 3 and 4 Assessment as a SIM: CDC review and SAC approval. If a SIM arises after the opening of a Type 3 or 4 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Sections 5.6.3.2.4 and 5.6.3.3.4.)

10.1.4.1.3 (U) TYPE 5 ASSESSMENTS

(U//~~FOUO~~) An FBI employee must obtain the SAC's prior approval to open a Type 5 Assessment on a sensitive potential confidential human source (CHS). If it is determined after the opening of a Type 5 Assessment that the individual is a sensitive potential CHS, the Assessment may continue, but the matter must be approved by the SAC as soon as practicable, but no later than five (5) business days after this determination is made to authorize the Assessment to continue. (See DIOG Section 5.6.3.4.4.1)

10.1.4.1.4 (U) TYPE 6 ASSESSMENTS

(U//~~FOUO~~) An FBI employee must obtain the following review and approval to open a Type 6 Assessment as a SIM: CDC review, SAC approval, and Domain Collection and HUMINT Management Section (DCHMS) Section Chief (SC) approval. If the SIM arises after the opening of a Type 6 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC and DCHMS SC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Section 5.6.3.5.4)

(U//~~FOUO~~) FBIHQ must receive notice and approve all Type 6 Assessments whether or not they involve a SIM.

10.1.4.2 (U) NOTICE FOR SIM ASSESSMENTS BY A FIELD OFFICE

(U//~~FOUO~~) Notice for SIM Assessments—There is no requirement to notify FBIHQ, DOJ, or the United States Attorney (USA) of the opening of an Assessment involving a SIM. (AGG-Dom, Part II.B.5.a)

10.1.4.3 (U) REVIEW AND APPROVAL OF SIM PREDICATED INVESTIGATIONS BY A FIELD OFFICE

10.1.4.3.1 (U) PREDICATED INVESTIGATIONS INVOLVING A SIM

(U//~~FOUO~~) CDC review and SAC approval. (See Sections 6.10 and 7.10)

10.1.4.3.2 (U) ENTERPRISE INVESTIGATIONS INVOLVING A SIM

(U//~~FOUO~~) CDC review, SAC approval, and SC approval. (See Section 8.6)

Version Dated:
October 15, 2011
RCFP-256

10.1.4.3.3 (U) POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS INVOLVING A SIM

(U//~~FOUO~~) CDC review, SAC approval, and DCHMS SC approval. (See DIOG Sections 9.6 and 9.10)

10.1.4.4 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS BY A FIELD OFFICE

10.1.4.4.1 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS

(U//~~FOUO~~) The field office must provide written notification (EC and a disseminable LHM) to the responsible FBIHQ unit and section within 15 calendar days after the opening of a SIM Predicated Investigation. The field office also must notify the appropriate United States Attorney's Office (USAO), in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the Unites States Attorney (USA), or the matter is a counterintelligence or espionage investigation. (See the CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ section must notify, in writing, the appropriate DOJ Criminal Division official or NSD official. The notification must be made as soon as practicable but no later than 30 calendar days after the opening of the investigation. [redacted] See the classified provisions in DIOG Appendix G for [redacted] b7E -1

(U//~~FOUO~~) [redacted] b7E -1

10.1.4.4.2 (U) NOTICE FOR SIM ENTERPRISE INVESTIGATIONS

(U//~~FOUO~~) See DIOG Section 8.6 for notice requirements.

10.1.4.4.3 (U) NOTICE FOR SIM POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS

(U//~~FOUO~~) See DIOG Section 9.9 for notice requirements.

10.1.4.5 (U) REVIEW AND APPROVAL OF SIM ASSESSMENTS OPENED BY FBIHQ

10.1.4.5.1 (U) TYPE 1 & 2 ASSESSMENTS

(U//~~FOUO~~) An FBI employee may open a Type 1 & 2 Assessment, as described in Section 5.6.3.1, without prior supervisory approval. An Assessment involving a SIM must be reviewed by the OGC and approved by the SC as soon as practicable, but no later than five (5) business days after the opening to continue the Assessment. [redacted] b7E -1

b7E -1

[redacted]

10.1.4.5.2 (U) TYPE 3 AND 4 ASSESSMENTS

(U//~~FOUO~~) An FBI employee must obtain the following reviews and prior approvals to open a Type 3 or 4 SIM Assessment: OGC review and SC approval [redacted] b7E -1

[redacted]

10.1.4.5.3 (U) TYPE 5 ASSESSMENTS

(U//~~FOUO~~) An FBI employee must obtain his/her SC's approval to open a Type 5 Assessment on a sensitive potential CHS [redacted] b7E -1

[redacted]

10.1.4.5.4 (U) TYPE 6 ASSESSMENTS

(U//~~FOUO~~)An FBI employee must obtain the following reviews and approvals to open a Type 6 Assessment as a SIM: OGC review and SC approval. [redacted] b7E -1

[redacted]

10.1.4.6 (U) NOTICE REQUIREMENTS FOR SIM ASSESSMENTS BY FBIHQ

(U//~~FOUO~~) There is no requirement to notify DOJ or the United States Attorney of the opening of an Assessment involving a SIM (including opening a sensitive potential CHS). (AGG-Dom, Part II.B.5.a)

10.1.4.6.1 (U) REVIEW AND APPROVAL OF SIM PREDICATED INVESTIGATIONS BY FBIHQ

10.1.4.6.2 (U) PREDICATED INVESTIGATIONS INVOLVING A SIM

(U//~~FOUO~~) OGC review and SC approval. (See DIOG Sections 6.7 , 6.10; 7.7 and 7.10)

10.1.4.6.3 (U) ENTERPRISE INVESTIGATIONS INVOLVING A SIM

(U//~~FOUO~~) OGC review and SC approval. (See DIOG Sections 8.6)

10.1.4.6.4 (U) POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS INVOLVING A SIM

(U//~~FOUO~~) OGC review and SC approval. (See DIOG Section 9.9)

Version Dated
October 15, 2011
RCFP-258

10.1.4.7 (U) Notice for SIM Predicated Investigations by FBIHQ

10.1.4.7.1 (U) Notice for SIM Predicated Investigations

(U//~~FOUO~~) The responsible FBIHQ section must provide written notification (EC and a disseminable LHM) to any appropriate field office within 15 calendar days after the opening of a SIM Predicated Investigation; the USAO, unless such notification is inappropriate under the circumstances, or the matter is a counterintelligence or espionage investigation (See the CD PG for details concerning notice in counterintelligence and espionage investigations.); and the appropriate DOJ Criminal Division official or NSD official, as soon as practicable, but no later than 30 calendar days after the opening of the investigation. If notice is not provided to the USAO under the circumstances described above, FBIHQ must explain those circumstances in the written notice to the field office(s) and DOJ. [redacted] known SIMs involved in the investigation. See the classified provisions in DIOG Appendix G for [redacted] b7E -1

(U//~~FOUO~~) [redacted]

10.1.4.7.2 (U) Notice for SIM Enterprise Investigations

(U//~~FOUO~~) See DIOG Section 8.6 for notice requirements.

10.1.4.7.3 (U) Notice for SIM Full Positive Foreign Intelligence Investigations

(U//~~FOUO~~) See DIOG Section 9.9 for notice requirements.

10.1.4.8 (U) Change in SIM Status

(U//~~FOUO~~) [redacted] b7E -1

10.1.4.8.1 (U) Documentation

(U//~~FOUO~~) The FBI employee must:

A) (U//~~FOUO~~) ***In Type 1 & 2 Assessments:*** Submit an updated FD-71 or Guardian [redacted] The FD-71 or Guardian must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required. b7E -1

B) (U//~~FOUO~~) ***In Type 3 through 6 Assessments:***

1) (U//~~FOUO~~) Opened by a Field Office - Submit an EC (for Type 5 Assessments, an EC or a successor form in [redacted] that must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required. b7E -1

2) (U//~~FOUO~~) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.

C) (U//~~FOUO~~) ***Predicated Investigations:***

1) (U//~~FOUO~~) Opened by a Field Office - Submit an EC that must be approved by the supervisor responsible for the investigation, reviewed by the CDC, and approved by the SAC. For Predicated Investigations, notification must be provided to the same FBIHQ entities (appropriate Unit and Section) that received notice of the SIM.

2) (U//~~FOUO~~) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.

D) (U//~~FOUO~~) ***Enterprise Investigations:***

1) (U//~~FOUO~~) Opened by a Field Office - Submit an EC that must be approved by the supervisor responsible for the investigation, reviewed by the CDC, and approved by the SAC and the appropriate SC.

2) (U//~~FOUO~~) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.

E) (U//~~FOUO~~) ***Positive Foreign Intelligence Full Investigations:***

1) (U//~~FOUO~~) Opened by a Field Office - Submit an EC that must be approved by the appropriate supervisor, reviewed by the CDC, approved by the SAC and the appropriate DI UC.

2) (U//~~FOUO~~) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the DI SC.

10.1.4.9 (U) CLOSING SIM INVESTIGATIONS

10.1.4.9.1 (U) SIM ASSESSMENTS CLOSED BY A FIELD OFFICE

A) (U//~~FOUO~~) ***Type 1 & 2 Assessments*** - These SIM Assessments must be closed on the FD-71 or FD-71a (Guardian) with approval of the supervisor responsible for the investigation and the SAC. (See DIOG Section 5.6.3.1)

B) (U//~~FOUO~~) ***Type 3, 4, and 5 Assessments*** - The closing EC (or successor form in [redacted] for Type 5 Assessments) must be approved by the supervisor responsible for the investigation and the SAC. (See DIOG Section 5.6.3.2, 3, and 4) b7E -1

C) (U//~~FOUO~~) ***Type 6 Assessments*** - The closing EC must be approved by the supervisor responsible for the investigation, SAC and the DI SC. (See DIOG Section 5.6.3.5)

10.1.4.9.2 (U) SIM PREDICATED INVESTIGATIONS CLOSED BY A FIELD OFFICE

(U//~~FOUO~~) The closing standards, approvals and notice requirements for SIM Predicated Investigations, including Enterprise Investigations and foreign intelligence Full Investigations, are specified in DIOG Sections 6.12; 7.12; 8.9; and 9.12 above.

Version Dated:
October 15, 2011
RCFP-260

10.1.4.9.3 (U) SIM ASSESSMENTS CLOSED BY FBIHQ

A) (U//~~FOUO~~) ***Type 1 & 2 Assessments*** - May be closed on the FD-71 or FD-71a (Guardian) with the approval of the UC responsible for the investigation and his/her SC.

B) (U//~~FOUO~~) ***Type 3, 4, and 5 Assessments*** - The closing EC (or successor form in [redacted] for Type 5 Assessments) must be approved by the UC responsible for the investigation and his/her SC. b7E -1

C) (U//~~FOUO~~) ***Type 6 Assessments*** - The closing EC must be approved by the DI UC responsible for the investigation and his/her DI SC.

10.1.4.9.4 (U) SIM PREDICATED INVESTIGATIONS CLOSED BY FBIHQ

(U//~~FOUO~~) The closing standards, approvals and notice requirements for SIM Predicated Investigations, including Enterprise Investigations and Full foreign intelligence investigations, are specified in DIOG Sections 6.12; 7.12; 8.9; and 9.12 above.

10.1.5 (U) DISTINCTION BETWEEN SIM AND SENSITIVE CIRCUMSTANCE IN UNDERCOVER OPERATIONS

(U//~~FOUO~~) The term "sensitive investigative matter," as used in the DIOG, should not be confused with the term "sensitive circumstance," as that term is used in undercover operations. "Sensitive circumstance" relates to an undercover operation requiring FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the Attorney General's Guidelines on FBI Undercover Operations and in Section 18 of the DIOG. The Criminal Undercover Operations Review Committee (CUORC) and the [redacted] must review and approve undercover operations that involve sensitive circumstances. The policy for undercover operations is described in DIOG Section 18.6.13, the Field Guide for Undercover and Sensitive Operations (FGUSO), National Security Undercover Operations Policy Implementation Guide (NSUCOPG), and the FBIHQ operational division program implementation guides. b7E -1

10.1.6 (U) DISTINCTION BETWEEN SIM AND SENSITIVE UNDISCLOSED PARTICIPATION

(U//~~FOUO~~) The term "sensitive investigative matter," as used in the DIOG, should not be confused with "sensitive UDP (undisclosed participation)." The rules regarding "sensitive investigative matter" and "sensitive UDP" (see DIOG Section 16.2.3.5), while similar, must be applied independently. The SIM designation applies to the overall investigation of which FBI and DOJ officials should be aware due to potential public notoriety and sensitivity. Sensitive UDP, on the other hand, applies to participation by employees or CHSs in lawful organizations that are designated as sensitive. Sensitive UDP can occur in either SIM or non-SIM designated investigations because sensitive UDP focuses on the activity (UDP) - not on the type of investigation in which it is taking place. Certain investigative or intelligence activity, particularly in situations involving academic institutions or student groups, may be covered by one or both these rules. The following scenarios demonstrate how these policies are to be applied:

10.1.6.1 (U) SCENARIOS

(U//~~FOUO~~) [redacted] b7E -1

(U//~~FOUO~~) [redacted] b7E -1

(U//~~FOUO~~) [redacted] b7E -1

(U//~~FOUO~~) [redacted] b7E -1

(U//~~FOUO~~) [redacted] b7E -1

(U//~~FOUO~~) [redacted] b7E -1

10.2 (U//~~FOUO~~) SENSITIVE OPERATIONS REVIEW COMMITTEE

(U//~~FOUO~~) At the request of the Director, a new joint DOJ/ FBI oversight committee, the Sensitive Operations Review Committee (SORC), has been established to review and monitor certain aspects of FBI investigative activities that are not within the purview of other oversight committees, particularly with regard to Assessments. The SORC is described as follows:

10.2.1 (U) MEMBERSHIP AND STAFFING

A) (U//~~FOUO~~) **Chair:** [redacted] b7E -1

B) (U) **Members:**

Version Dated:
October 15, 2011
RCFP-262

1) (U//~~FOUO~~) **FBI:** Assistant Directors or designated Deputy Assistant Directors for the [redacted] b7E -1 and any other appropriate representative, given the issue presented to the SORC.

2) (U//~~FOUO~~) **DOJ:** Assistant Attorneys General of the [redacted] and any other appropriate representative, given the issue being considered by the SORC.

C) (U//~~FOUO~~) **Advisors:** The Unit Chief or a designee of the FBI's Corporate Policy Office (CPO) will serve as a policy advisor to the SORC. In addition, DOJ's Chief Privacy and Civil Liberties Officer or a designee will also serve as an advisor to the SORC.

D) (U//~~FOUO~~) **Staff:** The staff of the SORC shall be from the executive staffs of the Executive Assistant Directors of the NSB and the CCSB. Proposals from the NSB shall be handled by its executive staff; proposals from CCSB shall be handled by its executive staff. The staffs will be collectively referred to here as "SORC Staff." The SORC Staff is responsible for ensuring that FBI and DOJ members of the SORC have the information required to perform their SORC duties and are kept fully informed of process developments in matters reviewed by the SORC.

10.2.2 (U) FUNCTION

(U//~~FOUO~~) The SORC will review and provide recommendations to the Director on matters submitted, as described below.

10.2.3 (U) REVIEW AND RECOMMENDATION

(U//~~FOUO~~) The SORC shall review sensitive activities in the categories described below and provide recommendations to the Director, who shall be the approval authority:

A) (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) [redacted] b7E -1

B) (U//~~FOUO~~) [redacted]

C) (U//~~FOUO~~) [redacted]

D) (U//~~FOUO~~)

E) (U//~~FOUO~~)

b7E -1

10.2.3.1 (U) Factors to Consider for Review and Recommendation

(U//~~FOUO~~) In addition to factors unique to the proposal being considered, the SORC will consider the following in determining whether to recommend that a proposed activity be approved:

A) (U//~~FOUO~~)
B) (U//~~FOUO~~)
C) (U//~~FOUO~~)
D) (U//~~FOUO~~)
E) (U//~~FOUO~~)
F) (U//~~FOUO~~)
G) (U//~~FOUO~~)
H) (U//~~FOUO~~)
I) (U//~~FOUO~~)

b7E -1

10.2.3.2 (U) Process for Review and Recommendation

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E -1

Declassified
October 15, 2013
RCFP-264

A) (U//~~FOUO~~) The applicable FBIHQ operational

b7E -1

B) (U//~~FOUO~~) Upon receipt of the EC and the proposal, the

C) (U//~~FOUO~~) prior to a scheduled SORC meeting, the SORC Staff must

b7E -1

D) (U//~~FOUO~~) SORC meetings are to be conducted with the expectation that

E) (U//~~FOUO~~) If there is no consensus among the SORC members

F) (U//~~FOUO~~) Once the SORC has made its recommendation, the SORC Staff

b7E -1

G) (U//~~FOUO~~) For each proposal, at the next SORC meeting the SORC Staff

10.2.4 (U) EMERGENCY AUTHORIZATION

(U//~~FOUO~~) When necessary to [redacted] SORC [redacted] b7E -1

10.2.4.1 (U) NOTICE/OVERSIGHT FUNCTION OF SORC

(U//~~FOUO~~) To facilitate its ability to [redacted]

A) (U//~~FOUO~~) In a [redacted] any approval to task a [redacted]

B) (U//~~FOUO~~) In a [redacted] any [redacted] b7E -1

C) (U//~~FOUO~~) In a [redacted]

D) (U//~~FOUO~~) In an [redacted] any [redacted]

E) (U//~~FOUO~~) In an [redacted] to obtain [redacted]

(U//~~FOUO~~) *Note*: [redacted] falling into any of the above-listed categories must be [redacted] b7E -1

F) (U//~~FOUO~~) The SORC may [redacted] to provide it:

1) (U//~~FOUO~~) [redacted]

2) (U//~~FOUO~~) [redacted]

3) (U//~~FOUO~~) [redacted]

Version Dated
October 15, 2011
RCFP-266

G) (U//~~FOUO~~) The SORC must [redacted]

[redacted]

b7E -1

H) (U//~~FOUO~~) [redacted] to the SORC as [redacted]

10.2.5 (U) LOGISTICS

(U//FOUO) The Executive Assistant Director for the NSB is responsible for all logistical support required for the proper functioning of the SORC (i.e., schedule meetings, provide place for meetings, draft agendas, record keeping and retention functions, all necessary communications, etc.). The CPO and the OGC will assist in establishing the logistical support required for the SORC.

RCFP-267