STANDARD OPERATING PROCEDURE: SOCIAL MEDIA
INDIANA INTELLIGENCE FUSION CENTER

I. PURPOSE

The purpose of the Indiana Intelligence Fusion Center (IIFC) Online Social Media (OSM) Standard Operating Procedure (SOP) is to provide guidance on the use of OSM in crime analysis, threat assessment, situational awareness, public safety, criminal intelligence development, and in support of criminal investigations. The SOP defines guidelines that govern IIFC personnel use of OSM and has been established in accordance with the IIFC Privacy Policy with the purpose of protecting individuals' privacy, civil rights, and civil liberties.

II. DEFINITIONS

Crime Analysis: Analytic activities that help IIFC personnel identify and understand trends, causes, and indicators of criminal activities, including international terrorism and domestic extremism.

Criminal Intelligence: Criminal information with value added resulting from the analytic process that may include conclusions or theory.

Criminal Predicate: The reasonable suspicion that behaviors or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity, including a criminal enterprise as defined under state or federal statute.

Online Alias: An online profile, handle, avatar, or username containing identifiers, such as name and date of birth, differing from the IIFC employee's actual personal identifying information, that is used as a means of covert connectivity to the internet.

Online Social Media (OSM): A category of internet-based resources that integrate user-generated content and user participation. Social Media includes, but is not limited to, social networking sites, micro blogging sites, photo and video-sharing sites, blogs, and other news sites.

Online Social Media Monitoring Tool (OSM Tool): Software used to capture data and monitor non-private social media sites by utilizing automated tools such as web crawlers and work search functions to make predictive analysis, develop trend and time lines, and/or collect information relative to the duties and mission of the IIFC.

Situational Awareness: As it pertains to the use of OSM, the collection of non-private social media postings to facilitate the IIFC in identifying and understanding trends, causes, and indicators of criminal activities, as well as posted intentions to commit crimes, including acts of international terrorism and domestic extremism.

Threat Assessments (Strategic or Tactical): An assessment request to the IIFC by a law enforcement agency or private sector partner for analysis of possible, future criminal/terrorist activity that relates to a specific event, location, and time. Threat Assessments normally require a formal written product as a response.

III. APPLICABILITY

This SOP applies to all personnel who are permanently or temporarily assigned or detailed to the IIFC.

IV. USE OF ONLINE SOCIAL MEDIA

OSM may be utilized by on-duty IIFC personnel for a valid law enforcement/public safety purpose.

a. OSM may be used for crime analysis, threat assessment, situational awareness, public safety, criminal intelligence development, and in support of criminal investigations.

i. All collection of OSM data and metadata by IIFC personnel will be done in compliance and in accordance with the IIFC Privacy Policy.

ii. IIFC personnel may seek and retain social media information that:

1. Is based on a criminal predicate or possible threat to public safety; or
2. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist and domestic extremist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist and domestic extremist) conduct or activity; or
3. Is relevant to the investigation and prosecution of suspected criminal (including terrorist and domestic extremist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
4. Is useful in crime analysis or situational awareness/assessments for the administration of criminal justice and public safety (including topical searches).

IIFC personnel will not seek or retain OSM data or metadata about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations, unless such information is relevant to the individual's criminal conduct/activity or if required to identify the individual for an allowable purpose.

V. AUTHORIZATION TO ACCESS ONLINE SOCIAL MEDIA

a. No supervisory authorization is needed for any use of OSM or OSM tool other than for use that requires an online alias. Once approval is obtained for an online alias, no further supervisory authorization is required.

b. Online Alias.

   i. IIFC personnel may obtain and maintain a non-attributable username and/or password to an online network or site; however, this will only be done with the prior approval of the IIFC Assistant Executive Director, or designee.

   ii. The IIFC Assistant Executive Director, or designee, will maintain a list of authorized non-attributable usernames and passwords used by IIFC personnel.

   iii. IIFC personnel shall not share approved non-attributable usernames; all IIFC personnel must utilize usernames assigned to them from the set of approved aliases maintained by the IIFC Assistant Executive Director, or designee.

c. IIFC personnel will not engage in any two-way communication (act in an undercover capacity) via OSM. Non-attributable usernames may only be used for passive social media searches and may not be used to interact with a subject/group of interest.

VI. PROCEDURE

a. When accessing OSM for IIFC related business, IIFC personnel will make every effort to use a covert computer, unless impractical. Information obtained on the covert computer should be transferred via an IIFC-provided USB drive to the employee's primary IIFC computer.

b. The use of personal or family accounts, equipment, or services for official IIFC business related to social media searches and analysis is prohibited.

c. IIFC personnel shall not access personal or family OSM accounts from IIFC devices or connections.

d. IIFC personnel should make every effort to use multiple sources to determine the reliability and validity of OSM identity, posts, content, data, metadata, and accounts. While formal confidence levels are not required, IIFC personnel should make requesters aware of the degree of confidence in the information (e.g., "information is consistent" or "information cannot be verified"), how the information was found, and conclusions that were reached.

e. The IIFC provides lead information only; therefore, it is imperative that email responses have the standard IIFC disclaimers including informing law enforcement that they must independently verify information provided to them.

VII. DISSEMINATION

Dissemination of social media information will be treated in the same manner as other requests for information/service and will follow all other IIFC guidelines and policies, including, but not limited to, the IIFC Privacy Policy and 28 CFR part 23. The investigating agency will be responsible for maintenance, dissemination, and destruction of the information pursuant to state and federal laws after the IIFC has disseminated OSM information to them.

a. Information obtained from OSM that contains Personally Identifiable Information (PII) must be disseminated to the requester via secure email, telephone, or in person.

b. Any information obtained from OSM that will be included in a bulletin, assessment, or any formal written product must be reviewed by peer editors and by the Privacy Officer, or those trained in the privacy policy, prior to dissemination.

VIII. DOCUMENTATION AND RETENTION

Documentation, storage, and retention of OSM data and metadata will follow all other IIFC guidelines and policies, including, but not limited to, the IIFC Privacy Policy and 28 CFR part 23.

IX. OFF DUTY CONDUCT

a. IIFC personnel will not utilize approved online aliases or OSM tools for personal use.

b. If criminal intelligence or suspicious activity information is inadvertently obtained while off duty, IIFC personnel should send the information to on-duty or supervisory IIFC personnel to be assessed and disseminated as appropriate.