



GOVERNMENT OF PUERTO RICO
DEPARTMENT OF PUBLIC SAFETY

Hon. Pedro R. Pierluisi Urrutia
Governor

Alexis Torres
Secretary

DSP-2022-OA-019

DEPARTMENT OF PUBLIC SAFETY

FUSION CENTER SOCIAL MEDIA POLICY

Puerto Rico Fusion Center Analysts



Table of Contents

I. Title3

II. Purpose3

III. Scope.....3

IV. Act No. 20 dated April 10, 2017, as amended (“Act 20”).....4

V. Definitions4

VI. Utilization of Social Media7

VII. Authorization to Access Social Media Websites.....8

VIII. ARTICLE VIII: Source Reliability and Content Validity10

IX. ARTICLE IX: Documentation and Retention11

X. Accountability11

XI. ARTICLE XI: Sanctions **Error! Bookmark not defined.**

XII. ARTICLE XII: Validity12

XIII. ARTICLE XIII: Appendix12



I. Title

- A. This Administrative Order is the Department of Public Safety (“DPS”) Puerto Rico Fusion Center (“PRFC”) Social Media Policy. The term Puerto Rico Fusion Center or PRFC refers to the Security Information Management Office created by virtue of the Section 1.15 of the Act 20-2017, as amended.
- B. This Policy is intended for all analysts working with the Department of Public Safety PRFC being employees of the DPS or not for the proper management and use of information from individuals and/or organizations related to criminal investigations and/or investigations related to domestic or international without violating people’s Privacy, Civil Rights, and Civil Liberties (P/CRCL).
- C. This Policy will be used as a working tool for all analysts assigned to the DPS PRFC, and as a training mechanism for its staff.

II. Purpose

The PRFC recognizes that social media may be a valuable investigative tool to detect and prevent criminal activity. Social media has been used for community outreach events such as providing crime prevention tips, providing crime maps, and soliciting tips about unsolved crimes. Social media may also be used to make time sensitive notifications regarding special events, weather emergencies, service disruptions, missing or endangered persons and/or terrorism activity.

PRFC personnel must adhere to this policy to protect individuals’ privacy, civil rights, and civil liberties and to prevent employee misconduct.

The purpose of this policy to conduct social network-based investigations and research.

III. Scope

- A. The objective of this policy is to become a tool for information gathering in criminal or terrorism related investigation without violating the civil rights and liberties of individuals and groups listed in the United States Constitution, the Puerto Rico Constitution and any related federal or state statutes.
- B. This policy follows the Federal Code (28 CFR Part 23). It is a federal regulation that provides an operational policy for law enforcement personnel and analysts on the use of criminal intelligence systems.



IV. Act No. 20 dated April 10, 2017, as amended (“Act 20”)

- A. Act 20 establishes the Puerto Rico Department of Public Safety for the purposes of creating a new system comprised of all the components that administers the public safety in Puerto Rico and allows for the sharing of personnel and administrative expenses. This law creates the Puerto Rico Police Bureau, the Bureau of the Puerto Rico Firefighters Corps; 9-1-1 Emergency Systems Bureau, the Emergency Management and Disaster Administration Bureau, the Bureau of the Puerto Rico Medical Emergency Corps, and the Puerto Rico Special Investigations Bureau.

Executive Order OE-2011-003, dated February 10, 2011, establishes the Fusion Center in Puerto Rico, in compliance with the Federal Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) *See Appendix*.

The PRFC’s main function is the collection and analysis of information to prevent and adequately respond to threats to public safety, protecting the residents of Puerto Rico and preventing the rest of the United States from being affected. PRFC will also be responsible for carrying out and/or compiling risk and threat assessments of Government of Puerto Rico and municipal buildings. It may also offer this service to non-governmental entities. All agencies must cooperate with the management of PRFC and provide the information and resources necessary for PRFC to carry out its functions, in accordance with the fiscal capacity and mission of each Agency. Agencies will use the management authority and prerogative to direct their employees to provide the necessary support to PRFC to comply with the provisions of this Executive Order.

Executive Order 2017-18, amended EO 2011-003, detailing the purpose and involvement of non-governmental entities in PRFC as (1) to obtain information requested by government agencies for comprehensive data collection; (2) to receive security information based on actual knowledge needs; and (3) to receive public safety and emergency protection training.

V. Definitions

- A. Anonymizer - is a proxy server that makes Internet activity untraceable. An anonymizer protects personally identifying information by hiding private information on the user's behalf.



- B. Blog- a regularly updated website or web page, typically one run by an individual or small group, that is written in an informal or conversational style.
- C. Crime Analysis and Situational Assessment Reports—Analytic activities to enable PRFC identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.
- D. Criminal Intelligence Information—Data which meets criminal intelligence collection criteria, and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.
- E. Criminal Nexus—Established when behavior or circumstances are related to an individual or organization’s involvement or planned involvement in criminal activity or enterprise.
- F. Dark Web- is defined as “the portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser: part of the deep web.”
- G. Deep Web- the portion of the Internet that is hidden from conventional search engines, as by encryption; the aggregate of unindexed websites.”
- H. Electronic Communications—Electronic Communications include, among other things, messages, images, data or any other information used in e-mail, instant messages, voice mail, fax machines, computers, personnel digital assistants (including Blackberry or similar text messaging devices), pagers, telephones, cellular and mobile phones including those with cameras, intranet, Internet, back-up storage, information on a memory or flash key or card, jump or zip drive, any other type of internal or external removable storage drives or any other technology tool. In the remainder of this policy, all these communication devices are collectively referred to as “Systems.”
- I. Internet Service Provider - company that provides Internet connections and services to individuals and organizations. In addition to providing access to the Internet, ISP’s may also provide software packages (such as browsers), e-mail accounts, and a personal Web site or home page.
- J. IP Address- is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.



- K. Media Access Control (MAC Address)- is the unique 6-byte (48-bit) address that is assigned by the manufacturer to a piece of network hardware (like a wireless card or an ethernet card). A MAC address consists of six sets of two characters, each separated by a colon. The first 3 bytes (24 bits) represent the manufacturer of the card, and the last 3 bytes (24 bits) identify the card from that manufacturer. 00:1B:44:11:3A:B7 is an example of a MAC address.
- L. Multimedia Messaging Service (MMS) – is an extension of SMS, that allows users to send multimedia messages to each other. This includes images, videos, and sound files.
- M. Online Alias—An online identity encompassing identifiers, such as name and date of birth, differing from the user’s actual name, date of birth, or other identifiers.
- N. Online Undercover Activity—The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain
- O. Passive Collection - This is the most used type when collecting OSINT intelligence, by default most OSINT gathering methods should use passive collection because the main aim of OSINT gathering is to collect information about the target via publicly available resources.
- P. Public Domain—Any Internet resource that is open and available to anyone.
- Q. Real Time Open Source (R.O.S.A) - is the process conducted by law enforcement and analytic personnel to (1) develop or enhance criminal intelligence (including situational awareness reports), (2) support a criminal investigation, or (3) identify public safety risks either past, present, or anticipated. Law enforcement and analytic personnel gather publicly available information (otherwise known as open source) via social media resources and tools for analysis to determine whether criminal activity is occurring to support a criminal investigation or to assess risks to public safety and security.
- R. Short Message Service (SMS) -is used to send text messages to mobile phones. The messages can typically be up to 160 characters in length, though some services use 5-bit mode, which supports 224 characters. SMS was originally created for phones that use GSM (Global System for Mobile) communication, but now all the major cell phone systems support it.



- S. Social Media Monitoring Tool—A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information.
- T. Social Media Websites—Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation.
- U. URL- Stands for "Uniform Resource Locator." an address that identifies a particular file on the internet, usually consisting of the protocol, as http, followed by the domain name.

VI. Utilization of Social Media

- A. PRFC analyst will use social media for valid law enforcement purposes, which are:
 - 1. Based upon a criminal predicate or threat to public safety; or
 - 2. based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity (criminal intelligence information); or
 - 3. is relevant to the investigation and prosecution of suspected criminal 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 assessment reports for the administration of criminal justice and public safety; or
 - 5. is relevant to pre-employment background investigations.
- B. PRFC analysts will only employ passive collection of Open-Source Intelligence (OSINT)



Real Time Open-Source Analysis

- C. The use of ROSA will be use by PRFC analysts for:
1. Detection of criminal activity, including potentially violent situations or threatening behavior
 2. Assessment of threats to the public or critical infrastructure
 3. Analysis of suspicious activity reports potentially related to terrorism
 4. Acquisition of physical evidence related to a crime, Identification of victims and suspects of a crime
 5. Natural disasters or other emergency management operations
- D. PRFC analysts will not utilize social media to seek or retain information about:
1. Individuals or organizations solely based on their religious, political, social views or activities; or
 2. An individual's participation in a particular non-criminal organization or lawful event; or
 3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual; or
 4. An individual's age other than to determine if someone is a minor.
 5. PRFC will not directly or indirectly receive, seek, accept, or retain information from a source that used prohibited means to gather the information.

VII. Authorization to Access Social Media Websites

- A. No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.
- B. An online alias may only be used to seek or retain information that:



1. Is based upon a criminal predicate or threat to public safety; or
 2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed a criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the US Government, or the Government of Puerto Rico and the information is relevant to the criminal conduct or activity; or
 3. Is relevant to the investigation and prosecution of suspected criminal 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 assessment reports for the administration of criminal justice and public safety.
- C. To submit a request for an online alias, the PRFC analyst must comply with the following:
1. Purpose for the request (i.e., type of investigative activity);
 2. Username;
 3. Identifiers and pedigree to be utilized for the online alias, such as email address, username, and date of birth. Do not include password(s) for online aliases and ensure password(s) are always secured; and
 4. Photograph to be used with online alias, if applicable.

The work unit supervisor must evaluate the request to determine whether an online alias would serve a valid law enforcement purpose. The work unit supervisor must maintain the requests for online alias and their status (approved/denied) for two years from the date of deactivation of the online alias. PRFC analysts with an approved online alias may use their online alias to make false representations in concealment of personal identity to establish social media accounts. The establishment of a social media account with an approved online alias must be documented.

Authorization to Utilize Social Media Monitoring Tools

- D. Prior to utilizing a Real Time Open-Source Tools (ROSA), PRFC's supervisor will submit a request through the chain of command to the Director for investigations for authorization to use the social media



monitoring tool. The social media monitoring tool may be utilized in criminal investigations; criminal intelligence development; and crime analysis and situational assessment reports (e.g., during sporting events, demonstrations or other large gatherings that require a law enforcement presence to ensure the safety of the public). The request must contain the following:

1. A description of the ROSA tool;
 2. Its purpose and intended use;
 3. The social media websites the tool will access;
 4. Whether the tool is accessing information in the public domain or information protected by privacy settings; and
- E. Whether information will be retained by PRFC and if so, the applicable retention period for such information.
- F. The request must be reviewed by the PRFC's Privacy Officer prior to approval.
- G. In exigent circumstances, the PRFC supervisor may obtain verbal authorization to utilize the ROSA tool and provide written documentation as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.
- H. If approved, the ROSA tool may be utilized for a period of thirty (30) days or, in the case of situational assessments such as an event or large gathering, until the conclusion of the law enforcement activity related to the event. After thirty (30) days, the work unit supervisor must submit a summary describing the law enforcement actions that resulted from the use of the ROSA tool. If continued use is needed, the summary may also contain a request to continue using the ROSA tool. The process to approve the request is the same as the original request.

VIII. Source Reliability and Content Validity

- A. Information developed from social media sites should be corroborated using traditional investigative tools including interviews, verification of address, verification of internet protocol address information, or other lawful means.



IX. Documentation and Retention

- A. Other than crime analysis and situational assessment reports, all information obtained from social media websites shall be stored electronically. This includes but not limited to criminal investigations, suspicious activity report, or intelligence report.
- B. Crime analysis and situational assessment reports may be prepared for special events management, including First Amendment protected activities or in the case of Puerto Rico, Article II protected activities. At the conclusion of the situation requiring the report or First Amendment protected and/or Article II, protected activities event where there was no criminal activity related to the information gathered, the information obtained from the ROSA tool will be retained for no more than fourteen (14) days. Information from ROSA tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file in compliance of 28 CFR Part 23 regulations.
- C. Information identified as criminal in nature that is obtained during an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the information via secure digital means. When possible, PRFC analysts will utilize investigative computer systems and software intended to record data from social media sites.

X. Accountability

- A. If any clause, paragraph, article, section, chapter, title, or part of this policy is declared unconstitutional by a competent court, the ruling to that effect shall not affect, prejudice, or invalidate the rest of this policy. The effect of such judgment shall be limited to the clause, paragraph, article, section, chapter, title, or part thereof that has been declared unconstitutional.
 - 1. The PRFC Privacy Officer will review this policy at least annually and direct the updating of the policy and procedures as necessary.

XI. Sanctions

- A. Any personnel that incur in a federal or state violation will be prosecuted accordingly. All PRFC personnel that violates any of the provisions contained in this policy will be referred to the Office of Personal Responsibility of the Department of Public Safety. All personnel that violate any of these provisions and it's not a DPS employee will be immediately

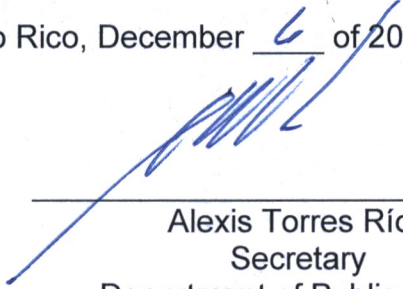


relieved from its functions and reported to its current authority. These personnel will not be able to work again in PRFC.

XII. Validity

This Policy is effective immediately on the day of its signing.

In San Juan, Puerto Rico, December 6 of 2022.



Alexis Torres Ríos
Secretary
Department of Public Safety

XIII. Appendix

- A. Act No. 20, dated April 10, 2017, as amended.
- B. Federal Code of Regulations 28 CFR Part 23.
- C. Executive Order 2017-018, as amended.

