# Social Media Investigations & LEO Safety

Missouri Information Analysis Center and
Department of Public Safety Office of Homeland Security



## MO DPS/OHS & MIAC Cybersecurity Program

Established in July 2019

Built a Cybersecurity Program with all three Missouri Fusion Centers

Pillars

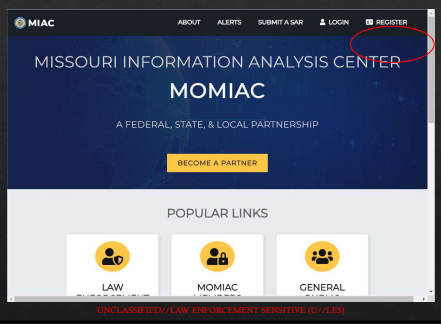
| Intelligence | Coordination | Outreach |
|---|---|---|



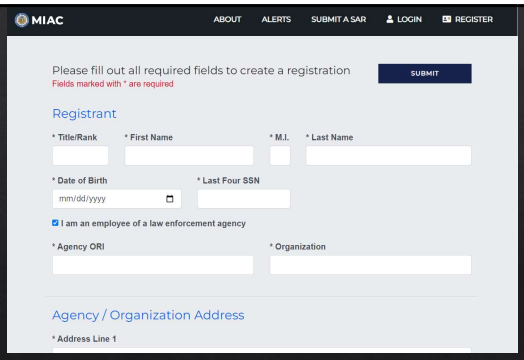
## Program Deliverables & Resources

- Weekly Cybersecurity Oper:Source Intelligence Wrap Up
- Vulnerability notification
- Gathering and processing cyber intelligence
- Intelligence dissemination and logging
- OSINT gathering (including dark web)
- Indicators of Compromise (IOC) research
- Requests for information
- ESF-14 Cybersecurity Planning and working group coordination
- Participation in the National Fusion Center Association Cyber Intelligence Network (CIN)
- ESF-14 Exercises and ESF-14 After Action Reviews
- Conducting Tabletop Exercises for stakeholders
- Conduct Incident Response Workshops for stakeholders
- Cyber Intelligence Partners (CIP) Program
- Cyber Training (local government, schools, etc.)
- Host Missouri Executive Branch Government Cyber Intel bi-monthly call (2x/month)
- Developing and disseminating cyber intelligence products

## MOMIAC

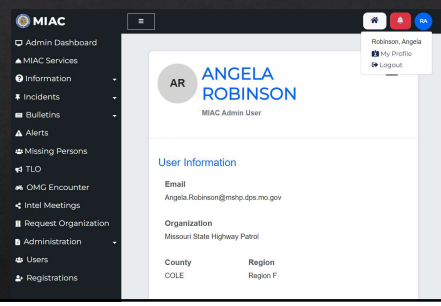




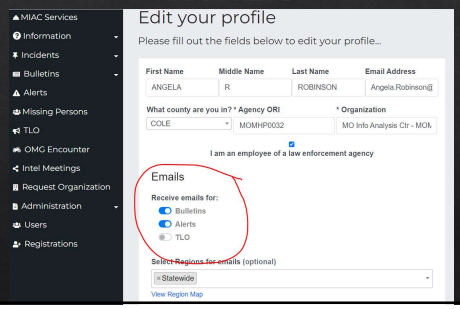






## MOMIAC

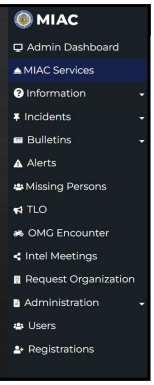


## MOMIAC




## MOMIAC

- Incidents – Single incidents that go into bulletins fed by LE in field
- Bulletins – Incidents in last 24 hours
- Alerts – Missing/Endangered Persons, Blue Alerts, and Life Safety (LEO Safety)
- (Information Library) Pass Throughs – Information from other agencies and/or states
- Cyber Resources
- MIAC Services






## Disclaimers

This presentation is for intelligence gathering purposes.

NEVER use an alias account on your personal devices and NEVER use the alias account or UC computer for any personal use.

## THINGS TO CONSIDER

- Civil Rights & Civil Liberties
- Amendments 1 & 4
- What You Need
- Creating a UC Account
- Tools to Conduct UC Social Media Investigation



## Civil Rights & Civil Liberties

Criminal Predicate

Threat to public safety

Reasonable suspicion that an identifiable organization or individual, has committed an identifiable criminal offense, or is involved in or is planning criminal conduct or activity



## Civil Rights & Civil Liberties

- Justification –
  - There is **no reasonable expectation of privacy on an Internet** site not owned by the subject.
  - The **subject has already released the information to a third party** in the form of the social media or open-source website.
- Law Enforcement – for the purposes of intelligence, SM research should fall under 28 C.F.R. Part 23
  - This is the Federal Regulation for collection and retention of intelligence information. https://www.iir.com/28CFR_Program/28CFR_Resources/Executive_Order/
- Missouri Regulation for the collection & retention of intelligence and criminal history information: https://www.sos.mo.gov/CMSImages/LocalRecords/Prosecutor.pdf

## AMENDMENT 1 - FREE SPEECH & AMENDMENT 4 - UNREASONABLE SEARCHES & SEIZURES

- **Amendment I**

"Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

- **Amendment 4**

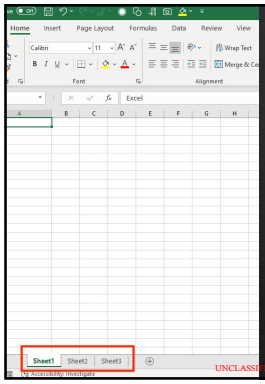
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE (U//LES)

## WHAT YOU NEED

- Clean computer with nothing on it linking it back to the Agency
  - No windows account
  - No Work email
  - No product that your agency pays for

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE (U//LES)




## WHAT YOU NEED

- Spreadsheet
- A. Activation date
- B. Registered email
- C. Type of account (fb,insta, twitter)
- D. User id
- E. Password
- F. Who the account is assigned to
- G. Should an employee with knowledge of account information terminate employment, the intelligence officer will immediately deactivate the account. A record of deactivation will be maintained on the aforementioned spreadsheet including; deactivation date, deactivated accounts, and reason for deactivation. This information will be retained in electronic form indefinitely.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE (U//LES)


## WHAT YOU NEED

- TOOLS TO DOWNLOAD ONTO CLEAN COMPUTER
  - Virtual Private Network (VPN)
  - Tunnel Bear
  - ProtonVPN
  - TOR - also serves as a VPN
  - Use as a VPN
  - Darknet searches
  - Bluestacks - Android Simulator
  - Access apps (Insta, SnapChat, Messanger….)




## WHAT YOU NEED

- ALIAS ACCOUNT SET UP
  - Email
  - Social Media Accounts



## Why OSINT?

- *Ninety percent of intelligence comes from **open source**. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond.*
- Lieutenant General Sam Wilson, USA (Ret)
- former Director, Defense Intelligence Agency

## Before you begin…

| Define a research goal: | Protect yourself accordingly: |
| --- | --- |
| • What am I looking for?<br>• Who or what is my target?<br>• How am I going to conduct my research? | • VPN<br>• Virtual Machine<br>• UC/sock puppet account |



## Search Engines

How to use them, and use them well



## Preservation Requests

- Most companies will take steps to preserve account records in connection with official criminal investigations for 90 days pending receipt of formal legal process.
- Most companies have online access portals to submit these requests. Links available upon request.
  - Use your professional email address, and make sure it doesn't go to your spam folder.
- Data for law enforcement purposes isn't retained unless a preservation request is sent before a user has deleted that content from the site.

## Preservation Requests

- Be specific!
  - The name of the issuing authority and agent, email address from a law-enforcement domain, and direct contact phone number.
  - The email address, phone number (+XXXXXXXXXX), user ID number (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (http://www.facebook.com/username) of the Facebook profile.
- Send on law enforcement letterhead in a non-editable format
- Some companies notify the end user!
  - For purposes of transparency and due process, Twitter's policy is to notify users (e.g., prior to disclosure of account information) of requests for their Twitter or Periscope account information, including a copy of the request, unless we are prohibited from doing so (e.g., an order under 18 U.S.C. §2705(b)).



## Emergency Requests

- In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay
- Note: We will not review or respond to requests submitted by non-law enforcement officials.
- The Electronic Privacy Communications Act authorizes companies to disclose during emergency situations but does NOT require them to do so.



## Questions

## Search Engines

- Google – most popular
- Edge - Microsoft
- Bing – Microsoft-developed
- DuckDuckGo – Privacy-focused
- Yandex – largest search engine in Russia



## People search engines

- People search engines crawled the internet for information on people across the country. People search engines, when supplemented with law enforcement databases, can often provide valuable leads.
- Examples of people search engines include:
  - www.spokeo.com
  - www.pipl.com
  - www.peekyou.com
  - www.zoominfo.com
  - www.classmates.com
  - www.mylife.com
  - www.legacy.com



## Online Communities

Social media, online forums, and more

## Social Media can be used to…

| | |
|---|---|
| Identify | Identify Networks<br>• Who is friends with your target?<br>• Who is your target pictured in photos with? Tagged in posts with?<br>• Who comments on your target's posts? |
| Supply | Supply biographical information<br>• What information is on their profile? Feed?<br>• Where did they go to school? Where do they work? What do they do? What are your target's interest? Hobbies?<br>• Do photos provide any context clues (e.g. excessively lavish lifestyle, illicit activity)? |
| Provide | Provide location information<br>• Does your target have any check-ins anywhere?<br>• Do photos place your target at certain locations at certain times?<br>• Are any posts geo-tagged? |
| Determine | Determine the legitimacy of a business entity<br>• Does your business have a social media presence?<br>• Is content on a business' profile unique or generic (e.g. stock photos, boilerplate language)?<br>• Have people interactive with the business entity's web presence (e.g. liked pages, posted reviews) |



## Helpful Websites

- https://osintframework.com/
- NDCAC - **National Domestic Communications Assistance Center**
  - Cross Talk
  - Chrome Extension
- https://tools.epieos.com/email.php



## LEO Social Media Safety: How to Avoid Becoming the Target

Angie Robinson
Cybersecurity Specialist
Missouri Office of Homeland Security

Do not waste your time in information gathering to recognize technologies, just check companies' recruitment listings. This will give you much better and accurate results within few finger tabs.

OSINT Tactics 086

-Praytush Nema

"Don't say anything online that you wouldn't want plastered on a billboard with your face on it."

– Erin Bury

THE POWER OF OPEN SOURCE IS THE POWER OF THE PEOPLE. THE PEOPLE RULE.

"We don't have a choice on whether we DO social media, the question is how well we DO it."

– Erik Qualman






TECH

**Data breach exposes personal information of thousands of LAPD officers and applicants**

Madeline Purdue USA TODAY

Published 6:31 p.m. ET Jul. 29, 2019 | Updated 7:35 p.m. ET Jul. 29, 2019

Newsweek

U.S.

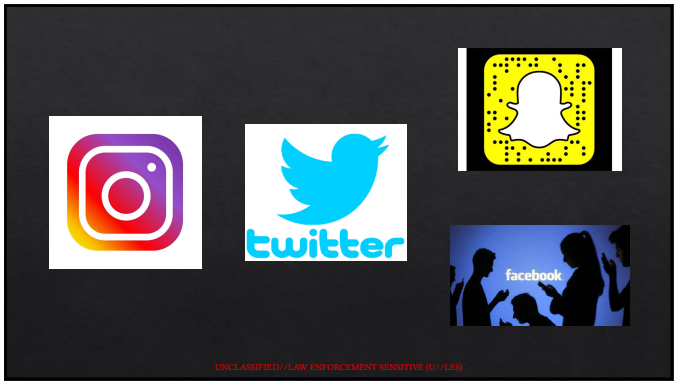
**38 Police Officers Have Been Doxxed During Protests in Portland, DHS Says**

BY DANIEL VILLAREAL ON 7/21/20 AT 8:14 PM EDT

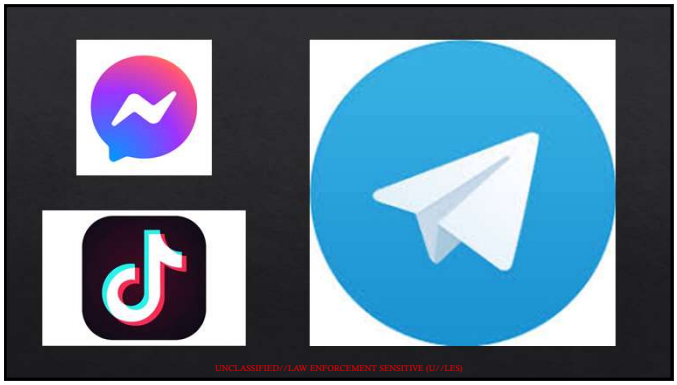
The Intercept_

**HACK OF 251 LAW ENFORCEMENT WEBSITES EXPOSES PERSONAL DATA OF 700,000 COPS**

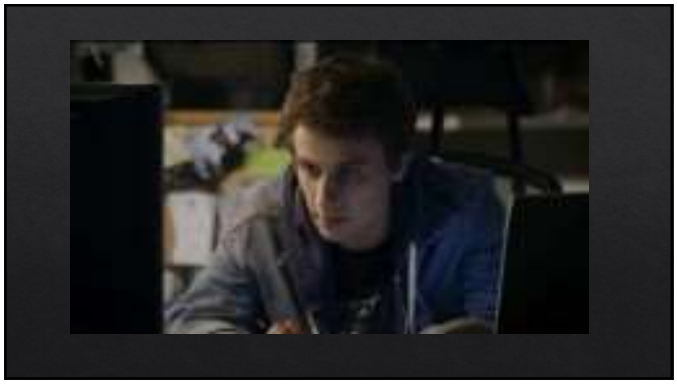
The BlueLeaks archive contains over 16 million rows of data, including emails, descriptions of alleged crimes, and detailed personal information.

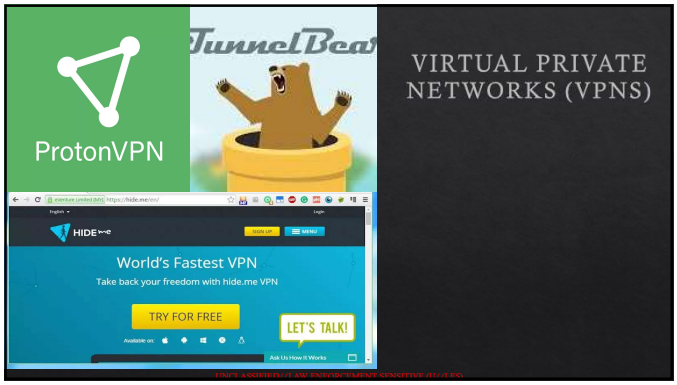


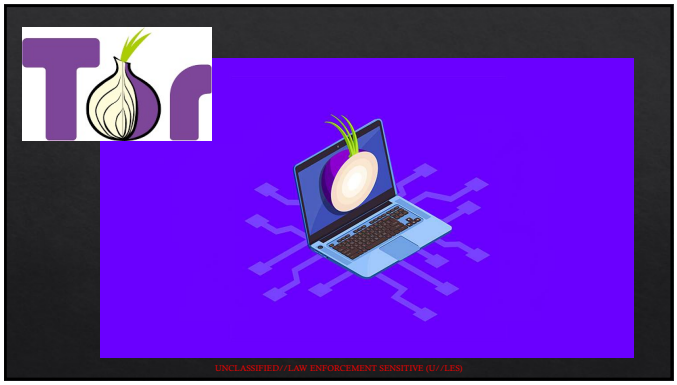







ProtonVPN
TunnelBear
HIDE.ME
World's Fastest VPN
Take back your freedom with hide.me VPN
TRY FOR FREE
LET'S TALK!
VIRTUAL PRIVATE NETWORKS (VPNS)
UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE (U//LES)


Tor
UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE (U//LES)


Handouts
Social Media Privacy and Safety
OHS Cybersecurity Brochure
Digital Exhaust Opt-out Guide for Law Enforcement
UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE (U//LES)

# QUESTIONS


Angie Robinson, CFE, CSMIE & CCIP
Cybersecurity Specialist
Missouri Office of Homeland Security
Missouri Information Analysis Center
Angela.Robinson@mshp.dps.mo.gov
Desk: 573-526-9153
Work Cell: 573-301-2023