Office of Intelligence and Analysis
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

DHS I&A Open Source Collection Operations Overview
December 18, 2018

(U//FOUO) Overview: The DHS I&A Current and Emerging Threats Center (CETC), Open Source Collection Operations (OSCO) collects open source publicly available information, and reports information of intelligence value across DHS and its mission partners. ~~Current and Emerging Threats Center (CETC) enables the Chief Intelligence Officer (CINT) to frame threats at the earliest possible opportunity and enable targeted mitigation.~~ (b) (3), (b) (5) [redacted] ~~rovides an intelligence activity that collects open source publicly available information, and reports information of intelligence value across DHS and its mission partners at the lowest possible classification level.~~

(U//FOUO) CETC conducts (b) (3) [redacted] ~~collects information passively~~ using open source methodologies designed to protect the collectors' online presence, providing basic operational security protections for the activity. ~~CETC collects information based on prioritized and validated collection requirements from DHS and its mission partners related to one of three reporting categories:~~

- ~~direct threats to or by US Persons~~
- ~~direct threats to the homeland, or~~
- ~~direct threats to US interests abroad.~~

Formatted: No bullets or numbering

(b) (3), (b) (7)(E), (b) (5) [redacted]

(U//FOUO) ~~To share CETC collected information,~~ CETC produced~~s~~ ~~raw unevaluated information in the form of~~ Open Source Intelligence Reports (OSIRs)~~. These OSIRs~~ are ~~cables~~ recognized across the IC for their value and are used for all facets of intelligence and law enforcement activities.

(U//FOUO) Results: Over the past three years, I&A has seen an increase in the demand for and use of OSIRs in finished intelligence as well as in the tactical use of threat related information with reporting totaling 3,246 OSIRs (FY16-729 OSIRs; FY17- 1251 OSIRs; FY18- 1266 OSIRs). CETC OSIRs ~~have a high~~ evaluation rate is ~~with~~ over 46% ~~of OSIRs receiving evaluations.~~ ~~I~~In contrast ~~to~~ the average evaluation rate for raw intelligence across other IC partners ~~of~~is between

20-30% with many entities below 10%. ~~More~~More than 95% of I&A OSIR evaluations ~~show that~~indicate the information contained in the reporting is of value to the consumer.

(U//FOUO) Examples of OSIR success: CETC has seen OSIRs used across all spectrums of the DHS mission. From direct threats to DHS employees during the conduct of departmental missions, to direct lifesaving during the Houston, TX flooding, to identifying threats of school violence. In the summer of 2017 CETC was asked to provide assistance locating flood victims in need of rescue for the state and local first responders when the city of Houston, TX found their call center being overwhelmed with requests for assistance. Working with the IA Regional Director in the area, CETC was able to provide over 400 tailored requests for rescue from social media platforms directly to the Houston fusion center in a manner which assisted in quick triage and tasking for rescue.

In August 2018, DHS entities found themselves facing direct threats to include bodily harm and in the case of one OSIR, murder. During routine collection based on a (b) (3) [redacted] CETC located a social media post seeking to pay for the murder of an ICE agent. Working with state, local and federal authorities based off information collected by OSCO, the FBI, HSI and local police were able to find and arrest the individual responsible.
In November of 2018, during routine collection (b) (3) [redacted] a CETC collector located a posting where a juvenile outside of Buffalo, NY threatened to conduct an attack on a local middle school. Working with state, local and Federal partners, the originator of the post was identified, with the FBI taking the case for action. ~~DHS OSIRs are used by analysts, investigators, and operators, and have been cited in state and local products, as well as finished intelligence, including in the Presidents Daily Brief. OSIRs are predominantly Unclassified/For Official Use Only, but can be tailored to meet higher classifications needs if necessary. CETC disseminates OSIRs via formal message traffic channels and OSIRs are posted daily on the unclassified, secret, and top secret networks to ensure the broadest possible sharing with other members of the Intelligence Community; the DHS Intelligence Enterprise, Components and state, local, territorial, and tribal partners.~~

~~(U//FOUO) CETC activities further both national and departmental missions simultaneously. They assist executive branch officials performing executive functions, including DHS, other departments and agencies of the Federal Government, State and local government agencies, the private sector, and other entities in identifying protective and support measures regarding threats to homeland security.~~

(U//FOUO) Technology: (b) (3), (b) (7)(E), (b) (5) [redacted]

(b) (3), (b) (7)(E), (b) (5) [redacted]

(U//FOUO) Processing, Exploitation, and Dissemination (PED): CETC/OSCO uses an indigenously built and maintained software system to process, database and disseminate OSIRs. This systems facilitates data access, processing, retrieval, and enables dissemination on all 3 local area networks (C, B, and A-LANs). (b) (3), (b) (5) [redacted]

(U//FOUO) Methodology: The most important capability in CETC are the professionals conducting the collection. (b) (3) [redacted] –The methods for collecting and disseminating raw open source information have been developed through time and experience and are ever changing as the world of social media expands at record pace. (b) (3), (b) (5) [redacted]

(U//FOUO) Training: Because (b) (3) [redacted], there is no single comprehensive training program to certify someone as a DHS open source intelligence collector. In order for CETC to maintain a trained cadre of collectors, CETC leverages IC training ~~for entry level collectors and then applies one to two months of~~in conjunction with on-the-job training and oversight by more experienced collectors. ~~After initial training, advanced open source intelligence training is gained through commercial vendors which often charge high prices for specialized two day advanced courses.~~

~~**(U//FOUO) Results:** Over the past three years, I&A has seen an increase in the demand for and use of OSIRs in finished intelligence as well as in the tactical use of threat related information with reporting totaling 3,246 OSIRs (FY16 729 OSIRs; FY17 1251 OSIRs; FY18 1266 OSIRs). CETC OSIRs have a high evaluation rate with over 46% of OSIRs receiving evaluations, in contrast to the average evaluation rate for raw intelligence across other IC partners of between 20-30% with many entities below 10%. More than 95% of I&A OSIR evaluations show that the information contained in the reporting is of value to the consumer.~~

~~**(U//FOUO) Examples of OSIR success:** CETC has seen OSIRs used across all spectrums of the DHS mission. From direct threats to DHS employees during the conduct of departmental missions, to direct lifesaving during the Houston, TX flooding, to identifying threats of school violence.~~

In the summer of 2017 CETC was asked to provide assistance locating flood victims in need of rescue for the state and local first responders when the city of Houston, TX found their call center being overwhelmed with requests for assistance. Working with the IA Regional Director in the area, CETC was able to provide over 400 tailored requests for rescue from social media platforms directly to the Houston fusion center in a manner which assisted in quick triage and tasking for rescue.

In August 2018, DHS entities found themselves facing direct threats to include bodily harm and in the case of one OSIR, murder. During routine collection based on (b) (3) , CETC located a social media post seeking to pay for the murder of an ICE agent. Working with state, local and federal authorities based off information collected by OSCO, the FBI, HSI and local police were able to find and arrest the individual responsible.
In November of 2018, during routine collection (b) (3) a CETC collector located a posting where a juvenile outside of Buffalo, NY threatened to conduct an attack on a local middle school. Working with state, local and Federal partners, the originator of the post was identified, with the FBI taking the case for action.

Office of Intelligence and Analysis
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

DHS I&A Open Source Collection Operations Overview
December 18, 2018

(U//FOUO) Overview: The DHS I&A Current and Emerging Threats Center (CETC), Open Source Collection Operations (OSCO) collects open source publicly available information, and reports information of intelligence value across DHS and its mission partners.

(U//FOUO) CETC conducts (b) (3) [redacted], using open source methodologies designed to protect the collectors' online presence, providing basic operational security protections for the activity.

(b) (3), (b) (7)(E) [redacted]

(U//FOUO) CETC produced Open Source Intelligence Reports (OSIRs) are recognized across the IC for their value and are used for all facets of intelligence and law enforcement activities.

(U//FOUO) Results: Over the past three years, I&A has seen an increase in the demand for and use of OSIRs in finished intelligence as well as in the tactical use of threat related information with reporting totaling 3,246 OSIRs (FY16-729 OSIRs; FY17- 1251 OSIRs; FY18- 1266 OSIRs). CETC OSIR evaluation rate is over 46%. In contrast the average evaluation rate for raw intelligence across other IC partners is between 20-30% with many entities below 10%. More than 95% of I&A OSIR evaluations indicate the information contained in the reporting is of value to the consumer.

(U//FOUO) Examples of OSIR success: CETC has seen OSIRs used across all spectrums of the DHS mission. From direct threats to DHS employees during the conduct of departmental missions, to direct lifesaving during the Houston, TX flooding, to identifying threats of school violence. In the summer of 2017 CETC was asked to provide assistance locating flood victims in need of rescue for the state and local first responders when the city of Houston, TX found their call center being overwhelmed with requests for assistance. Working with the IA Regional Director in the area, CETC was able to provide over 400 tailored requests for rescue from social media platforms directly to the Houston fusion center in a manner which assisted in quick triage and tasking for rescue.

In August 2018, DHS entities found themselves facing direct threats to include bodily harm and in the case of one OSIR, murder. During routine collection based on (b) (3) [redacted]

(b) (3) , CETC located a social media post seeking to pay for the murder of an ICE agent. Working with state, local and federal authorities based off information collected by OSCO, the FBI, HSI and local police were able to find and arrest the individual responsible.
In November of 2018, during routine collection (b) (3) , a CETC collector located a posting where a juvenile outside of Buffalo, NY threatened to conduct an attack on a local middle school. Working with state, local and Federal partners, the originator of the post was identified, with the FBI taking the case for action.

(U//FOUO) Technology: CETC uses hardware and software that is available to individual members of the public. Such technology includes. (b) (3) which can be tailored to meet the needs of the collector.

(U//FOUO) Processing, Exploitation, and Dissemination (PED): CETC/OSCO uses an indigenously built and maintained software system to process, database and disseminate OSIRs. This systems facilitates data access, processing, retrieval, and enables dissemination on all 3 local area networks (C, B, and A-LANs). Each portion of the PED architecture was built with the idea the CETC process could be expanded to include the DHS Intelligence Enterprise..

(U//FOUO) Methodology: The most important capability in CETC are the professionals conducting the collection. The methods for collecting and disseminating raw open source information have been developed through time and experience and are ever changing as the world of social media expands at record pace.

(U//FOUO) Training: Because (b) (3) , there is no single comprehensive training program to certify someone as a DHS open source intelligence collector. In order for CETC to maintain a trained cadre of collectors, CETC leverages IC training in conjunction with on-the-job training and oversight by more experienced collectors.

(b) (6)

From: (b) (6)
Sent: Saturday, January 25, 2020 8:56 PM
To: (b) (6)
Cc: (b) (6)
Subject: RE: (b) (3) Trial

Follow Up Flag: Follow up
Flag Status: Flagged

(b

I wanted to give you my feedback on (b) (3). I did not find it useful or intuitive for my target set. (b) (5)

For example, I started writing an OSIR earlier this week about the sabotage of the largest freight rail carrier in North America, which carries enough coal at any given time to power roughly 10% of the U.S. (b) (3), (b) (5)

Additionally, (b) (3) eturns results from image boards. While this is helpful, it doesn't return the images, so a majority of the context is lost. (b) (3), (b) (5)

Finally, I reached out to (b) (3) to make sure that I was using the system correctly and asked for their assistance in setting up a search for (b) (3). (b) (3), (b) (5)

For these reasons, I don't think (b) (3) would be an effective tool for (b) (5). I'm more than happy to discuss this in more depth this week.

V/r,
(b

From: (b) (6)
Sent: Tuesday, January 7, 2020 9:50 AM
To: (
b
Cc: (b) (6)
Subject: RE: (b) (3) Trial

Two weeks, ma'am

(b) (6)

Branch Chief
Open Source Collection Operations|S1 Book Team
Current and Emerging Threats Center
Dept. of Homeland Security
(b) (6) (desk)
(b) (6) (mobile)
(b) (secure)
(b) (6) v
(b) (6)

From: (b) (6)
Sent: Tuesday, January 7, 2020 9:17 AM
To: (b) (6)
Cc: (b) (6)
Subject: RE: (b) (3) Trial

Great. Is it a two week trial or 30 days?

Thank You,

(b) (6)
Open Source Collection Operations (OSCO)
Current & Emerging Threats Center (CETC)
DHS Office of Intelligence and Analysis
Office: (b) (6)

From: (b) (6)
Sent: Tuesday, January 7, 2020 9:16 AM
To: (b) (6)
Cc: (b) (6)
Subject: (b) (3) Trial

Team,

We are actually starting our trial with (b) (3) You names have been submitted as our test users along with previously submitted key words. By the end of the week, if not before you should be receiving instructions on how to log in, the self-tutorial, and sandbox training area. We do have IT support included with the trial so if you run into any issues please let me know.

Most importantly keep good records of what you liked and didn't like about the software. Things that work for us and don't. Your feedback will be used to determine if we will move forward with a contact using (b) (3) as a collection platform.

(b) (6)
Branch Chief
Open Source Collection Operations|S1 Book Team
Current and Emerging Threats Center

Dept. of Homeland Security
(b) (6) (desk)
(b) (6) (mobile)
(b) (secure)
(b) (6)
(b) (6)

(b) (6)

From: (b) (6)
Sent: Monday, January 27, 2020 9:56 PM
To: (b) (6)
Cc: (b) (6)
Subject: (b) (3) Feedback - (b) (6)

Follow Up Flag: Follow up
Flag Status: Flagged

(b

Here is some of my feedback after testing it a bit more.

Pros:

- Wonderfully designed UX.
- Aggregating power and searching for big data.
- (b) (3), (b) (5)

Cons:

- Not easy to operate if you're unfamiliar (recommend users attend a training).
- Cost a ton for a service that may or may not be utilized by collectors.
- (b) (3), (b) (5)

Overall: I have previously used (b) (3) in a previous job, so I've had some on hand experience. Back then, (b) (3), (b) (5) The platform has a wonderful user interface and was crafted with users in mind. (b) (3), (b) (5) From my previous experience, we had a hard time at NOC Media Monitoring getting users to use this since they rather just stick with what they know works for them.

Please let me know if you have any questions or comments,

(b) (6)
Open Source Collection Operations (OSCO)
Current & Emerging Threats Center (CETC)
Office of Intelligence and Analysis
U.S. Department of Homeland Security

From: (
Sent: Tuesday, January 14, 2020 4:04 PM

To: (b) (6)
Subject: (b) (3)

Hi (b)

I talked to (and (b) about you using my (b) (3) username to exploit/test (b) (3) to see if it is worth, is it effective …etc and they were ok with it. So focus your shift on it unless of course there is something urgent that needs your attention.
Few things:
Log in to (b) (3) following the link below on your ALAN
Unfortunately, our names and DHS affiliates is tied to this account so we could not use it (b) (3)
I know this obvious but don't click on any links (b) (3) t provides, it will give you the search results along with links to access the post or blog (b) (3)

Be advised that (b) (3) t can no longer exploit from (b) (3) !! Let me know if you have any questions. Please take notes to provide me with your honest feedback. The link and username is below, password will follow in a different email.

(b) (3)

Thank You,

(b) (6)
Open Source Collection Operations (OSCO)
Current & Emerging Threats Center (CETC)
DHS Office of Intelligence and Analysis
Office: (b) (6)

(b) (3)

PROS

The software search across variety of social media platforms in multiple languages (b) (3), (b) (5)

CONS

-The software does not pull data from two important social media platforms (b) (3), (b) (5)

-Tested the software multiple times on an actual event for example “US Embassy Baghdad Rockets attacks” nothing came back with information on that specific attack. (b) (3), (b) (5)

(b) (3), (b) (5)

I believe all those platforms are not as powerful (regarding time frame) as (b) (3), (b) (5)

-I have problem with the Boxes in the upper Taps. Insides these boxes there should be an icon/symbol, representing the action that will be executed. All the boxes were empty from any Symbol that represent the action. Example supposedly this box has the letter T for translation

For me I was seeing an empty box, I don’t know what the action will be, like this one 

There were many boxes, all were blank, and I have to go through each one of them until I found the action I want. Its time consuming.

(b) (6)

From: (b) (6)
Sent: Wednesday, September 18, 2019 12:37 PM
To: (b) (6(b) (6)
Peters, Kevin
Subject: FW: Social Media Winter Study revision
Attachments: Enhance Social Media edited.pptx

Please review and get me any input. I will review after you. Heading to a multi hour meeting in 117 if I am needed.

(b) (6)
Director, Current and Emerging Threats Center
Office of Intelligence and Analysis
Department of Homeland Security
(b) (6) (office)
(b) (6) (cell)
(b) (NSTS)

From: (b) (6)
Sent: Wednesday, September 18, 2019 11:58 AM
To: (b) (6)
Cc: (b) (6)
Subject: Social Media Winter Study revision

(b
We are still waiting on a couple more votes, but as I mentioned to (b) earlier this week the winter study for social media exploitation has been getting some positive attention from the DMAG members. We did some editing to the original submission, which if you are ok with this we will update the slide deck that is presented at the DMAG. Let me know what you think.

Best,

(b) (6)
Strategy, Policy, and Plans
Department of Homeland Security
(b) (6) office
(b) (6) cell
(b) (6)

From: DHS I&A (b) (6)
To: DHS I&A (b) (6)
Subject: (b) (3) Quote
Date: Monday, February 3, 2020 4:21:12 PM
Attachments: (b) (3) PRICE QUOTE 200127.pdf

The pricing is on page 12.

From: DHS I&A (b) (6)
To: DHS I&A (b) (6)
Cc: DHS I&A (b) (6)
Subject: RE: ICGE
Date: Thursday, January 30, 2020 4:00:16 PM
Attachments: MITRE FY20 Elections IGCE Draft 2020-01-30.xlsx
HSSEDI ROM Estimate for IA-MOB 1-17-20.docx

DHS I&A (b) (6) —

Here is the current IGCE, but I have to tweak it to reduce the LOE so that there is enough funding to cover ~3 months after this base PoP (9/23/2020).

The datasets cost is in the ODCs. Attached is the MITRE ROM for the datasets.

So as to not cross threads, I'll send you the link to the Cybersecurity Retention Incentive Program docs. But, please note that the CRIP is undergoing changes and so I can't say that the implementation would follow the SOP. However, the certs that qualify haven't changed.

DHS I&A (b) (6)

DHS I&A (b) (6) CISSP, PMP
Deputy CIO for Technology Business Management, I&A
Office of Intelligence and Analysis/CIO
U.S. Department of Homeland Security
NAC DHS I&A (b) (6)
(mobile)

From: DHS I&A (b) (6)
Sent: Thursday, January 30, 2020 3:07 PM
To: DHS I&A (b) (6) @HQ.DHS.GOV>
Cc: DHS I&A (b) (6) @hq.dhs.gov>
Subject: ICGE

Hi DHS I&A (b) (6),

Can you send us the ICGE? We identified another data set that we may want to procure.

On another topic, can you send us the list of cyber trainings that were considered under the cyber pay program?

Thanks

DHS I&A (b) (6)

Branch Chief /Deputy Chief Data Officer
CIO, Mission Operations Branch
Office of Intelligence & Analysis
U.S. Department of Homeland Security

NAC-DHS I&A (b) (6)
[redacted]
[redacted]@dhs.ic.gov

Publicly Available Information Overview

The Office of Intelligence and Analysis (I&A) Intelligence Oversight Guidelines define publicly available information to be:

> Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event open to the public.
>
> Social media sites, Internet sites, chat rooms, bulletin boards, and other electronic and other fora, or portions of the same, belonging to individuals or groups that limit access by use of criteria that cannot generally be satisfied by members of the public are not publicly available sources.

Though there are some variations between Intelligence Community elements, this definition is consistent with those in the Executive Order 12333 Attorney General Guidelines for the Department of Defense, Central Intelligence Agency, National Counterterrorism Center, and others.

Overall, information available on the open web, which is indexed and available to any member of the public, is considered publicly available information. Information available on the deep web may be publicly available information but is not always such. In determining whether information online is publicly available information, I&A may consider the following factors:

Steps Necessary for Access.

- Account creation/registration: Information is still publicly available if the only barrier to access is the creation of an account where any member of the public may create an account. This includes where the account holder needs to provide a valid email address, phone number, or other contact method in order to establish the account.
    - Ex: The New York Times requires users provide an email address to create an account, but any person with an email address may do so. Some content is only available to users with accounts. This content is still publicly available information.
- Fees: Information made available to any member of the public willing to pay a fee is still publicly available information.
    - Ex: To access full content of The Wall Street Journal, users may pay for a subscription. Any person may subscribe. The content of the subscription is publicly available information.
- Password: Where a password is required to access information (beyond the password a user may create as a necessary step of account creation), that information is only publicly available information if the password is available to any member of the public upon request.
    - Ex: A blog has a password protected chat forum. If the password is given out to any user who contacts the blog owner, this chat forum is publicly available information. If the blog owner uses their discretion to provide the password or otherwise sets qualifications that cannot be met by the general public, this is not publicly available information.
- Obfuscation: When accessing this information online, I&A's use of virtual private networks, fake accounts, or other tradecraft to obfuscate I&A's identity does not change whether information is publicly available.

- Ex: Logging into a Facebook account may require dual-factor authentication. I&A may use a fake email account and burner phone to obfuscate affiliation with the government. I&A may use a VPN to access the website. These tradecraft steps do not change the nature of whether the content being accessed is publicly available.

Position or Status of Recipient.

- Membership or Association: Information is not publicly available information if made available or distributed based on a specific membership or association not open to the general public. For example, posts in a Facebook or LinkedIn group made for those affiliated with a specific employer or university would not be publicly available information.
  - Ex: LinkedIn group for DHS employees would not be publicly available. Meanwhile, a LinkedIn group completely open (no approvals required) to anyone who loves dogs is publicly available.
  - Ex: Messages in a Nextdoor neighborhood limited to members with a certain address would not be publicly available information
- Intended government recipient: Some private companies make social media information available to government agencies. Where the data offerings made available to a government agency are the same as those made available to any member of the public, this would still be publicly available information. If only made available because of government status, this may not be deemed publicly available information.
  - Ex: A private company sells data to U.S. government agencies, but not private individuals. This data is not publicly available information
  - Ex: A company aggregates social media posts from a variety of different social media platforms and makes these available to any government or non-government customer. This data is publicly available information.

Engagement.

- Connections: Some social media users only make their information available to users who connect with them by joining a group or through direct connection (e.g. add a friend, follow a user, etc.). Where any member of the general public may request and automatically be granted access, this would likely be publicly available information. Where there are indications of moderation or other discretionary approvals for allowing access to information, this is likely not publicly available information.
  - Ex: Oprah's Twitter feed may be viewed by any user. It is publicly available. Justice Kagan's Twitter feed may only be viewed by users whose follow requests she has approved. Even if she approves your follow request, it is not publicly available.
- Participation: Participating in an online forum, to include membership and more active engagement, may implicate other legal and policy considerations, such as compliance with undisclosed participation requirements and the rules of behavior governing I&A tools.

Even where the information is all publicly available, I&A may not collect publicly available information for the sole purpose of monitoring activities protected by the First Amendment (such as speech, press, assembly, and religious exercise). Online speech, to include social media, protected by the First Amendment, collection and analysis of this content may give rise to First Amendment concerns. Given these implications and the difficulty of discerning when certain information constitutes publicly available information, I&A is encouraged to consult with the Office of the General Counsel/Intelligence Law Division when engaging in these collections.