Phone Data and Analysis in FALCON DARTTS

Beginning March 20, 2017, the FALCON DARTTS application will be available to launch as an embedded application inside the FALCON workspace. The web version of DARTTS will also remain available at (b)(7)(E) This guide assumes you have basic familiarity with the DARTTS application, which is covered extensively in the DARTTS User Guide on the FALCON homepage.

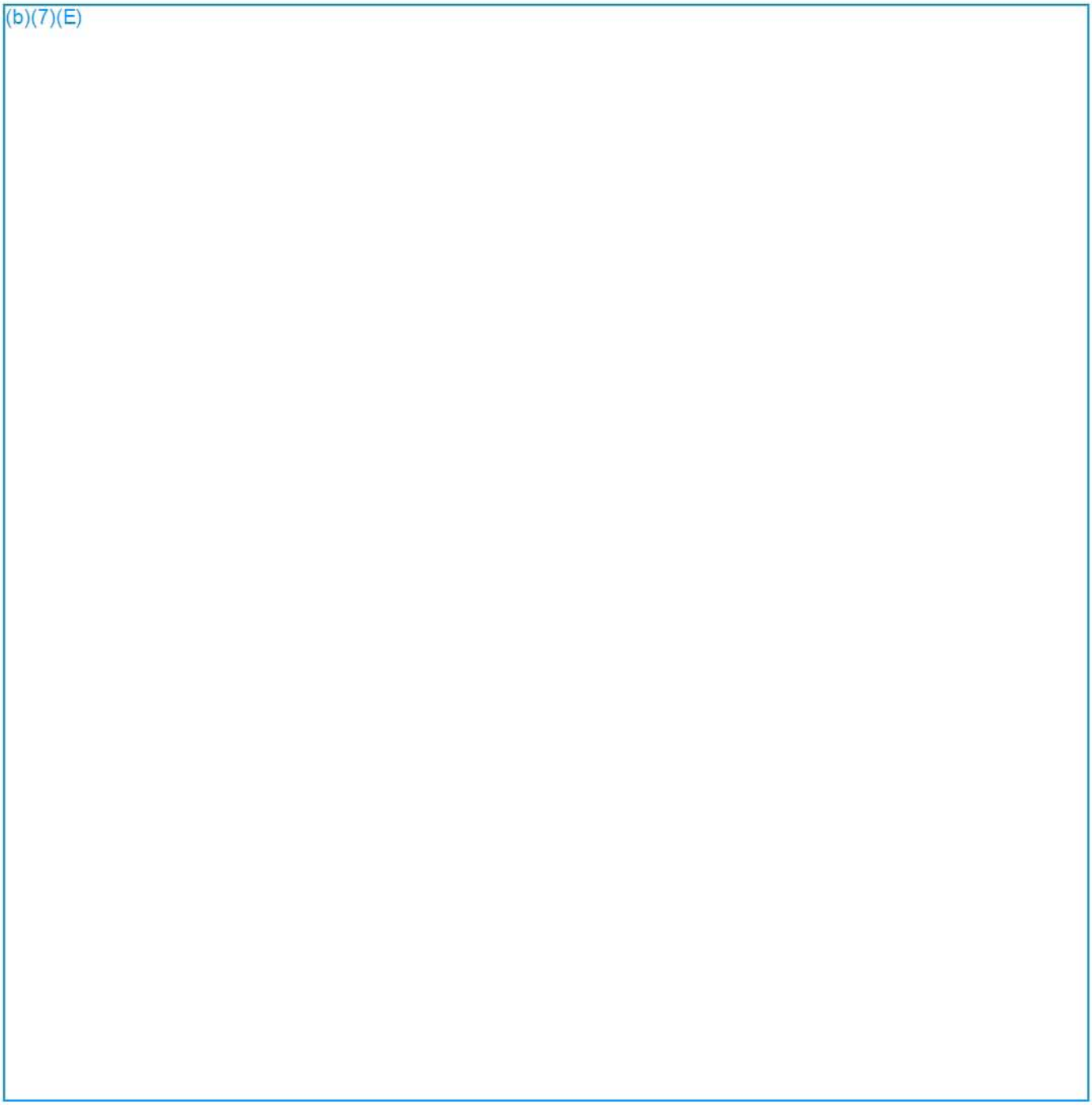
On March 20, 2017, TLS and EDTD call data record data will also be available for analysis in FALCON DARTTS. The previous CDR Application and CDR Helper in the FALCON workspace will no longer be available.

Contents

Launching DARTTS in FALCON workspace

In the Applications Menu in the FALCON workspace, navigate to the "DARTTS" selection and select with your cursor.

(b)(7)(E)



Note: If you are separately logged into a DARTTS session in your web browser outside of the workspace, you will be prompted to end that session prior to logging in via the workspace.

(b)(7)(E)

For full details on DARTTS functionality, please refer to the DARTTS V2 Guide on the FALCON Landing Page.

Phone Data Overview

(b)(7)(E)

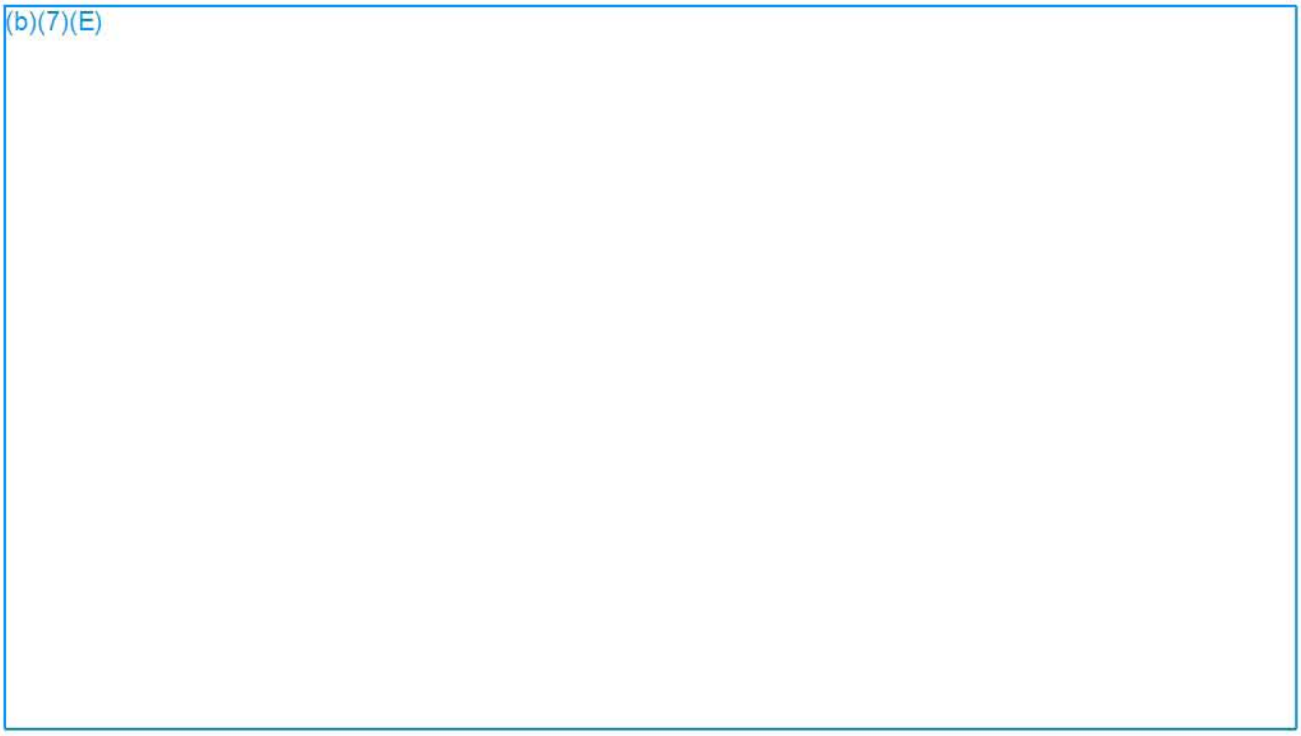
ERO Detention Telephony Data (EDTD) Phone Analysis

The EDTD collection is unique in that all the phone calls are in a single direction. Click on the EDTD Phone Calls collection from the home screen to open.

Finding All Calls from a Specific Detainee

To find all calls from a specific detainee, click the "Add a Filter" button in the Data Sets pane on the left. Choose "Detainee Name (Formatted)", and then type in the name you're interested in. Click Apply to apply the filter.

Group By to Find Top Contacts



Filtering by Phone Number

Searching for a specific phone number can be a little trickier than searching for names, because of the large number of possible variations in phone number format (e.g. with/out country code, with/out area code). To add a filter to search for specific phone number(s), click "Add a Filter" in the "Data Sets" pane,

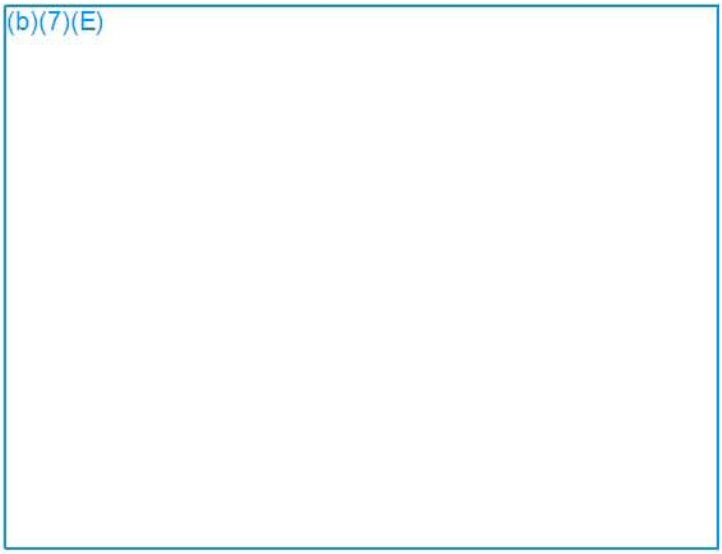
(b)(7)(E)

The above example would filter to phone numbers that start with any number of digits leading to "340887" followed by a single digit. This might be an example of an investigation that only has a partial phone number to search on.

Adding Columns to DARTTS

By default DARTTS only shows a selection of all of the columns, in an effort to keep a clean workspace. If you'd like to view other columns, you can click the "Columns" button at the top of the screen, which brings up the column selector.

(b)(7)(E)



The middle pane holds a list of all possible columns, and the pane on the right holds all of the currently displayed columns. To add a column to the right pane, click the solid green plus sign next to it in the middle pane. To add all possible columns, press the "Select" button on the top of the middle pane. Columns of interest for the EDTD collection include "Facility Name", "Group Name", and "Recording URL". Note that adding a large number of columns can impact performance.

Accessing EDTD Phone Call Recordings

TLS Phone Call Analysis

TLS Phone Calls are organized as a "Target Number", "Contact Number", and a "Direction" column (which contains either "OUTGOING" or "INCOMING" with reference to the Target Number). There is also a "Third Number" column that contains any third parties on the line, and a "Phone Number" column

that is a set of all of these numbers involved in the call. This TLS data model makes analysis somewhat different from EDTD Records in DARTTS.

Filtering TLS by Phone Number

To find all phone calls involving a certain phone, filter on the Phone Number column by clicking "Add a Filter" in the Data Sets pane on the left. By default, you perform a keyword search, which requires grouping the phone number correctly. For example, to return the phone number **+1 234-567-8900** you could search **234-567-8900**, **234 567 8900**, or **567 8900**, but not **2345678900**. If searching for a standard US phone number, searching using either dashes or spaces will work, but using neither will not.

(b)(7)(E)

Group By to Find TLS Top Contacts

Once you've filtered to your group of interest, you can "Group By" on the "Phone Number" field to view top contacts for your number of interest. By definition, your original number will be at the top as it is involved in every call, but all subsequent values will display the most frequent numbers in contact with your number of interest.

(b)(7)(E)

Find All TLS Calls Between Two Parties

To find all calls involving two specific parties, simply add two separate filters, one for each phone number. Note that you must use two filters rather than putting them in the same filter, as that would return all calls involving *at least one of* the parties. Note that this search will also contain any phone calls that contain these two numbers plus a third number.

(b)(7)(E)

TLS Subscriber Analysis

(b)(7)(E)

Exporting

At any point, your dataset can be exported, either to an Excel file or pushed directly to the FALCON workspace. To export to Excel, select the rows you're interested in, or select nothing to export all rows, and then click the Export button in the upper right of the screen. A maximum of 10,000 rows can be exported to Excel at one time.

To export directly to the FALCON workspace, click the "To Falcon" button. A maximum of 1000 rows can be exported to FALCON at one time. More details on Exporting to Falcon can be found in the "Export to Falcon Guide" on the FALCON home page.

Using the Phone Report

The phone report will display differently depending on whether you are looking at EDTD or TLS data, but the basic functionality is the same.

Opening the Phone Report

To use the Phone Report, you will first need to filter down to a set of phone calls smaller than 10k records. You will receive a warning if your set is too big for the report.

To open the Phone Report, click on the Reports tab, and the Phone Report will open by default. If it is not, use the drop down menu to select the Phone Report. Note that this report is only available for TLS Calls and EDTD calls, and not for TLS Subscriber records.

Phone Report Overview

When first opened, the report will show a bar graph of all of the calls over time. While you would normally open the report after filtering to a single person's calls (as is shown here), you can start this process with any data set, such as all calls from a particular case.

Below the chart is a histogram of top callers and top called numbers. At any point, these bins may be clicked on to add another filter to your data set.

To the right, in the Controls pane, you can choose to change the bucketed time interval on the chart to day, week, month, or year. You can also choose specific numbers to focus the report on using the "Focus Numbers" feature.

Focus Numbers in Phone Report

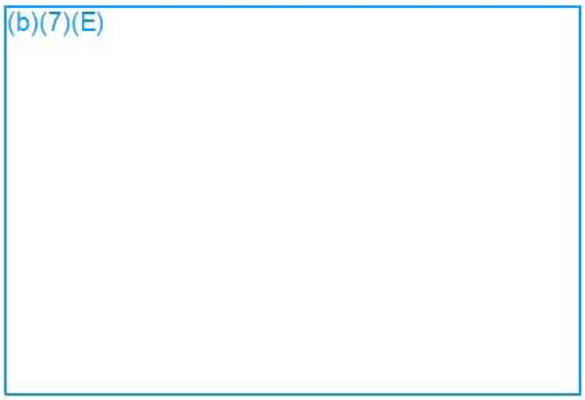
The Focus Numbers feature allows you to visualize inbound and outbound calls on the chart. When clicking in the Focus Numbers box with your cursor, all phone number values present in your data set will be listed, from which you can select one or more. If only one phone number is selected here, the chart will transform to reflect inbound and outbound calls.

You can also select more than one phone number in the Focus Numbers control to show patterns for the selected group of phone numbers.

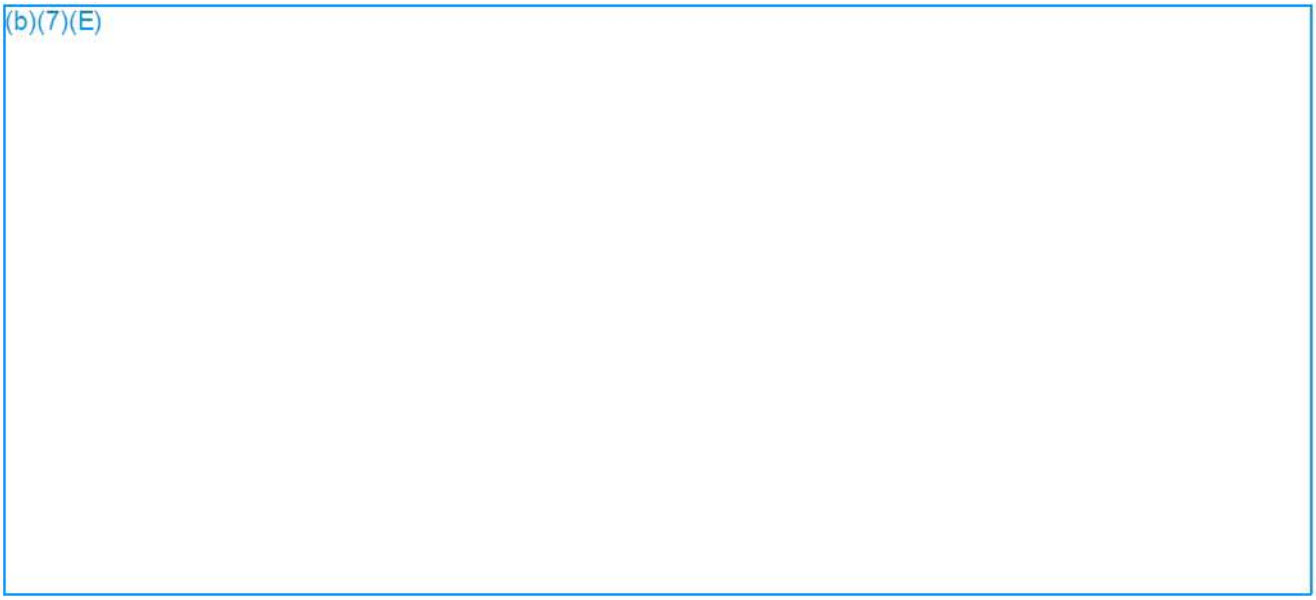
When selecting multiple numbers, the Phone Report will show you inbound calls to the Focus Numbers, calls within the group of Focus Numbers, and outbound calls from the group of Focus Numbers.

Global Search

The "Global Search" allows you to search across all collections in DARTTS with a single search. To access this feature, click on the "Search" tab in the Analysis screen.



(b)(7)(E)



This search will return results grouped by their collection. Click on a collection name to display the columns in which your search term matched. Click "Save as Data Set" to open that data set with your search terms applied as a filter.

(b)(7)(E)

QUICK GUIDE TO FALCON DARTTS v3

(b)(7)(E)

LAUNCH

- Go to (b)(7)(E)
- Click 'Accept' when the pop-up appears.
- DARTTS guides are located in the 'Help Guides' section on the right-side panel of the FALCON homepage (b)(7)(E)

NAVIGATION BAR

1. **Home:** The DARTTS landing page that where you can create or choose a Workbook (case) and an overview of the available data collections.
2. **Analysis:** (Shown above) The interface for all analytical work in DARTTS
3. **Alerts:** View and manage your DARTTS alerts
4. **Import:** Import structured data (Excel or csv) into DARTTS, such as subpoena returns.
5. **Help:** Creates a help-ticket email to submit issues or questions.
6. **Account Information & Preferences:** View and manage your account and settings.

VIEWS

(b)(7)(E)

27. **Pivots:** Click here to use the pivot functionality of DARTTS.

CREATING AND FILTERING DATA SETS

(b)(7)(E)

CREATING ALERTS

(b)(7)(E)

ANALYZING DATA

(b)(7)(E)


(b)(7)(E)

FALCON Training

Eligibility

FALCON Training is currently available to HSI Special Agents, Analysts, Intelligence personnel, and full time Task Force Officers.

Requirements

The following are required prior to class attendance, account activation and are necessary to maintain access:

HSI Personnel & Contractors

- ICE IRMNET username
- Enabled ICM profile
- HSI Home Office viewable in ICM profile
- Job Title and Series viewable in ICM profile
- Current ICM Privacy Awareness Certification
- Current NCIC Certification
- Background Investigation (BI) Level Clearance of 3 or greater (viewable in ICM)
- Completion of "Introduction to FALCON" CBT in PALMS or 2 Day FALCON Training

Task Force Officers

- ICE IRMNET username
- TECS Profile under HSI Supervisor & SCO
- Active TECS profile
- Current TECS Privacy Awareness Certification
- Current NCIC Certification
- Job Title in TECS profile should be TFO – TASK FORCE OFFICER
- HSI SAC and Home Office viewable in TECS profile
- Background Investigation (BI) Level Clearance of 3 or greater
- Completion of "Introduction to FALCON" CBT in PALMS or 2 Day FALCON Training
- Completion of the "User Privacy Awareness for Investigative Case Management 2017-2018" course
- E-mail approval from HSI Supervisor confirming TFO is full time on HSI led Task Force

FALCON Program Management Office and Training Requests: (b)(7)(E)
FALCON Access, Announcements, and Tutorials: (b)(7)(E)
FALCON Helpdesk: (b)(7)(E)
FALCON Program Code in ICM: (b)(7)(

FALCON Training

FALCON access is granted to full time HSI Task Force members. **A full-time TFO is defined as being co-located with HSI, works directly for an HSI first or second line supervisor, and is significantly contributing to investigations.** TFO's should have their HSI supervisor approve their access and need for FALCON by sending an e-mail to (b)(7)(E) upon completion of the online training course. **Full time TFO accreditation with HSI will be verified prior to account activation.**

FALCON CBT – 1 User

Previously, a request with 5 or more participants was required for access to FALCON. The FALCON Program Management Office (PMO) has modified this process so that access is granted within 24-48 hours of completion of the "Introduction to FALCON" course in the DHS Performance and Learning Management System (PALMS). Follow the steps below to complete the course and receive access:

1) Login to the DHS Performance and Learning Management System (PALMS).
2) Type FALCON into the search engine in the upper right hand corner.
3) Select the magnifying glass to search for the course.
4) On the "Introduction to FALCON" course page select "Open Item".
5) Download the Rules of Behavior and choose "Open" when the pop up appears.
6) Go back to the PALMS training session and click on the button to "Accept" the terms of use on the next page.
7) Ensure that the course marker at the bottom of the page is all the way to the right to receive course credit.
8) A completion certificate will appear on the main course page.
9) Please allow 24-48 hours for the FALCON PMO to grant access.
10) The FALCON PMO will contact you with instructions for accessing FALCON Workspace, Web, (and Mobile for 1811s, 1801s, and 0132s).

2 Day Training – 5 or More Users

Users are required to attend a two day training course to receive Publishing rights in FALCON.

Training will be limited and focused to HSI personnel who are involved in strong agent/analyst working groups and mission critical activities aligning with HSI Strategic goals. HSI will also target FALCON training resources in areas where identified high value projects or operations are either in place or anticipated, and where increased analytical and investigative effectiveness and efficiencies will benefit the overall mission.

FALCON Program Management Office and Training Requests: (b)(7)(E)
FALCON Access, Announcements, and Tutorials: (b)(7)(E)
FALCON Helpdesk: (b)(7)(E)
FALCON Program Code in ICM: (b)(7)(E)

FALCON Training

Requests for classroom training must meet all or most of the following criteria:

- Is mission critical for viable operational or analytical needs
- Promotes Agent and Analyst working groups within the office's area of responsibility or with other HSI offices
- Increases capabilities and efficiency for a specific group or component

To streamline the submission of training requests, the FALCON Program Management Office (PMO) has automated the process. **Paper User Access Request Forms are no longer required or accepted.**
In the event that 5 or more participants in one SAC, AOR, or office would like to receive the two day FALCON training, please have one POC complete a Training Request form. Select "Insert Additional Participant" to add and enter information for all other participants on one electronic form per classroom request. Once the request is received, the FALCON PMO will review the information and contact the POC to coordinate the best possible time for training.

To request training, please follow the steps below:

1. Click on the Request 2 Day *FALCON Training Course -5 or more users* button to open the request form.
2. Complete **ALL** required fields marked with an asterisk*. This information is needed for vetting users.
3. List all HSI personnel requesting training.
   A. The form will expand to accommodate multiple personnel requests.
   B. Click on "Insert Additional Participant" to include additional participants.
4. Under "Reason for Request," please select from the drop down menu.
5. In the additional space include specific advanced workflows that the group would like covered in the training session.
6. If requesting access for Task Force members, please include the Agency and period of time the Task Force Officer will be assigned to the HSI Task Force.
7. Press "Submit" to electronically send the request to the FALCON PMO.
8. The FALCON PMO will review the request and determine if it meets the required criteria and is in the best interest of ICE HSI.
9. The POC will be notified via e-mail that the request is approved. Training coordination will commence within 2 weeks of approval. ***It is the responsibility of the requestor or requesting office to provide an adequate facility for training.***

FALCON Program Management Office and Training Requests: (b)(7)(E)
FALCON Access, Announcements, and Tutorials: (b)(7)(E)
FALCON Helpdesk: (b)(7)(E)
FALCON Program Code in ICM: (b)(7)(E)

FALCON Training

The POC may modify a training submittal by contacting the FALCON PMO for a link to the request. The FALCON PMO staff will immediately be able to view the updated request after changes are made and "Save" is selected.

Consideration will be given to requests of five or more HSI personnel from the same working group, unit, team, or AOR.

FALCON Training Requests submitted without all required fields filled in **will be considered incomplete**.
Personnel are encouraged to petition individuals who would like to attend a FALCON training session to ensure that all interested users in an AOR are trained concurrently.

Requests with less than 5 participants **will be placed on hold** until more participants from the immediate office or AOR are added to the request.

Training Room Requirements

Training Room requirements are as follows:

- Computers for each user with at least 2GB RAM
- IRMNet connectivity (ideally hardwired, and NOT wireless)
- Overhead or TV hookup for Instructor
- A solid, enterprise grade internet connection (training users on a T1 is not suitable).

If you have any questions relating to FALCON training, please contact the FALCON PMO or Acting National Program Manager, (b)(6);(b)(7)(at (202) 732-(b)(6);(b)(7)(C)

FALCON Program Management Office and Training Requests: (b)(7)(E)
FALCON Access, Announcements, and Tutorials: (b)(7)(E)
FALCON Helpdesk: (b)(7)(E)
FALCON Program Code in ICM: (b)(7)(E)

These are the columns of ATS-4 data that will be mapped automatically when you use the PIM file during the import and the type of objects that will be created. The names of the columns in excel are **bold**, the Falcon properties are not. The color corresponds to the color used in the excel.

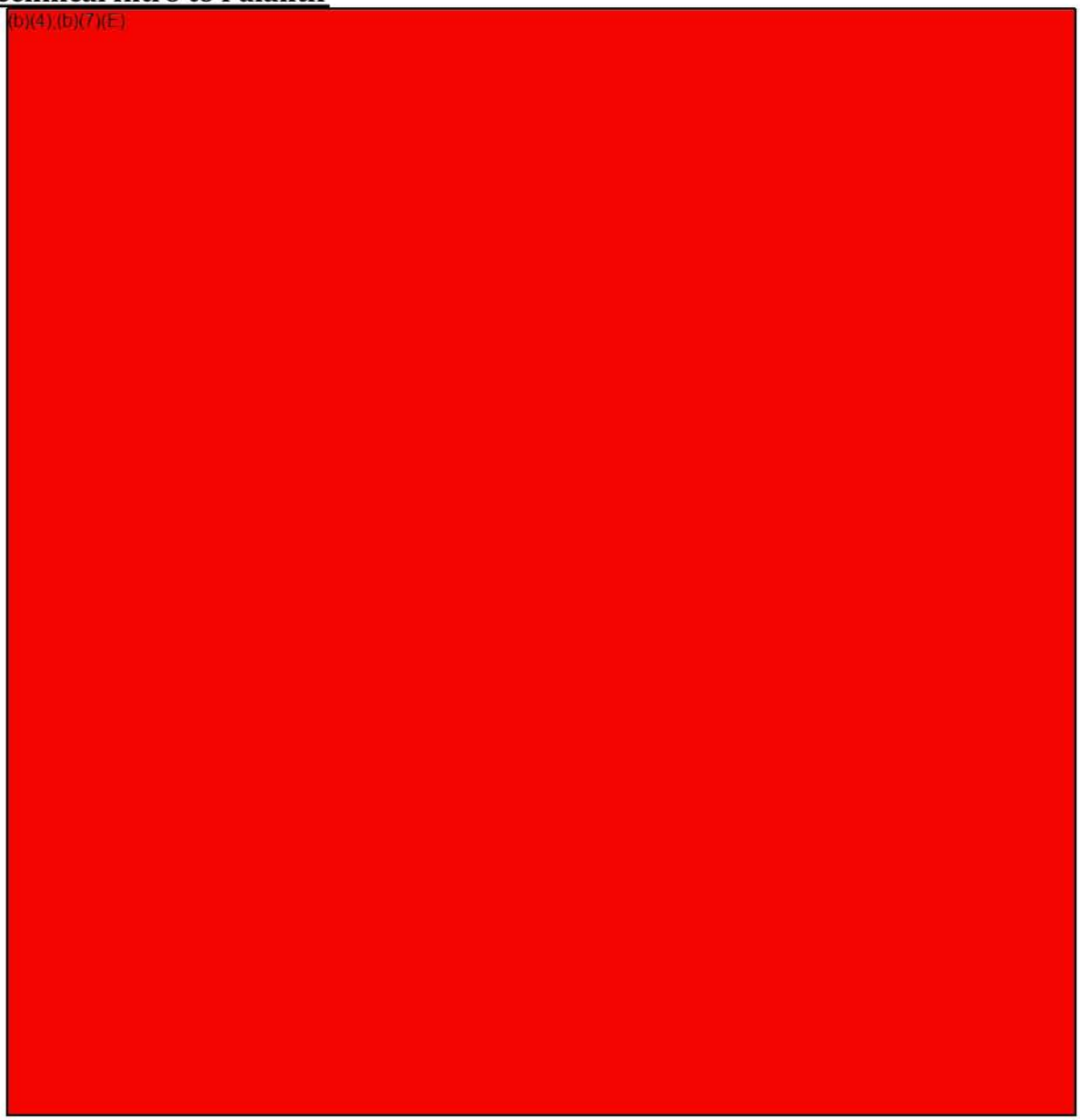
(b)(7)(E)

These are the columns of DIG data that will be mapped automatically when you use the PIM file during the import and the type of objects that will be created. The names of the columns in excel are **bold**, the Falcon properties are not. The color corresponds to the color used in the excel.

(b)(7)(E)

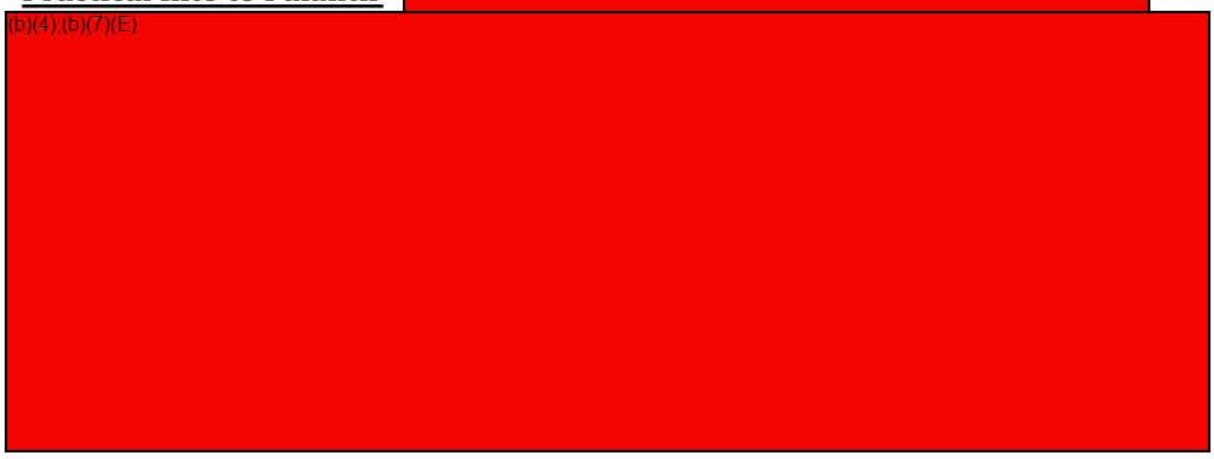
Technical Intro to Palantir

(b)(4),(b)(7)(E)

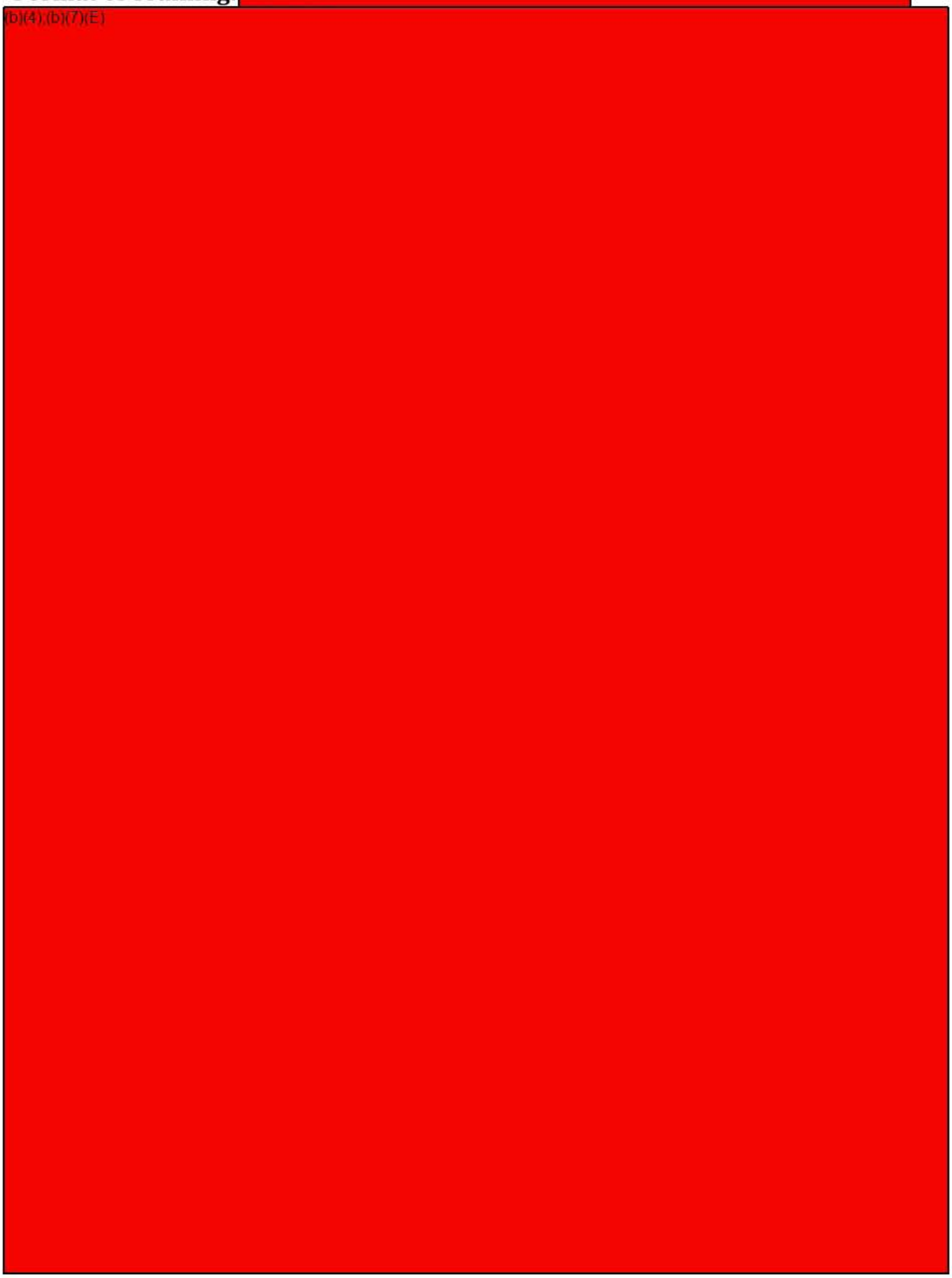


Practical Into to Palantir – (b)(4),(b)(7)(E)

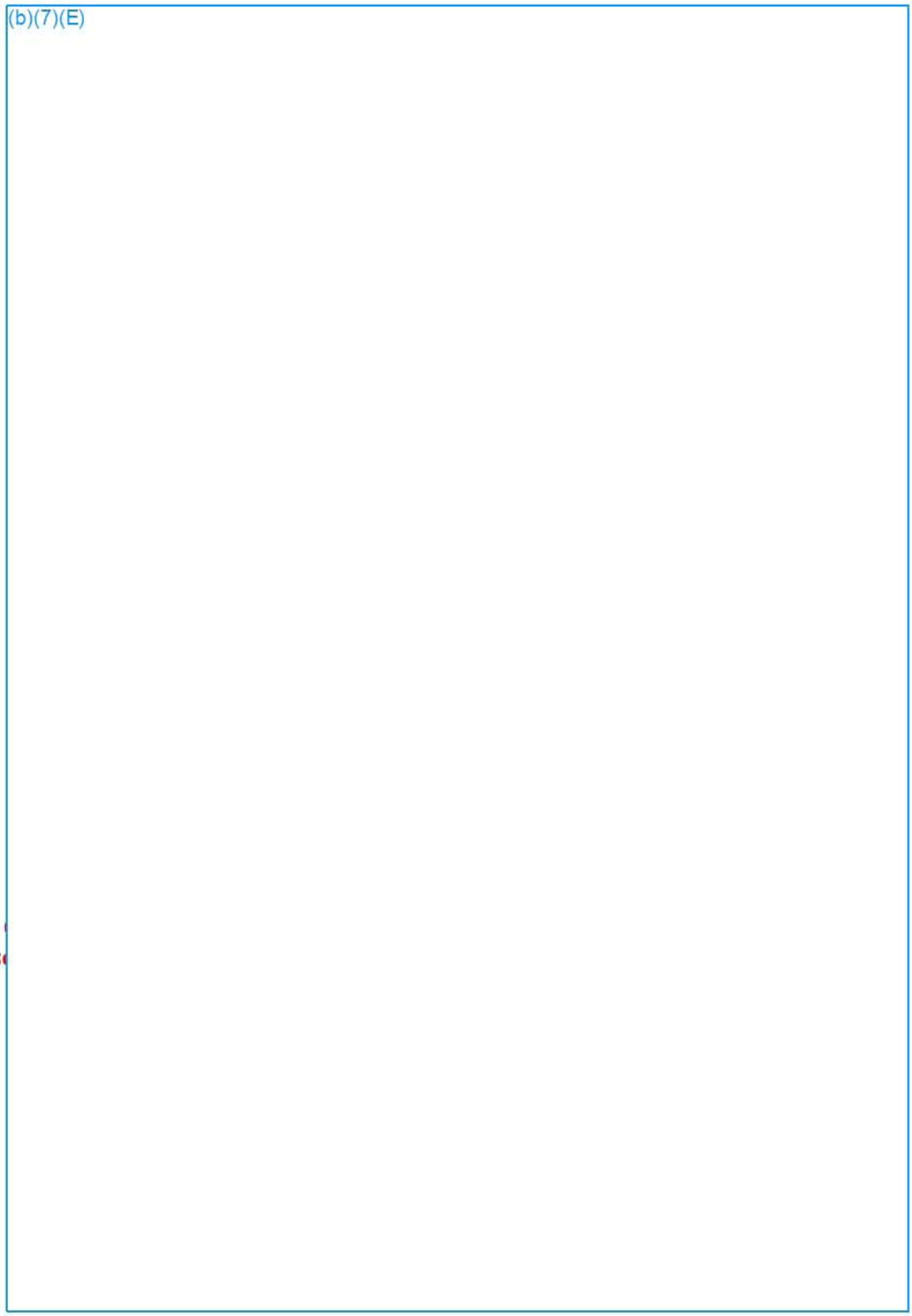
(b)(4),(b)(7)(E)



Format of Training: (b)(4),(b)(7)(E)



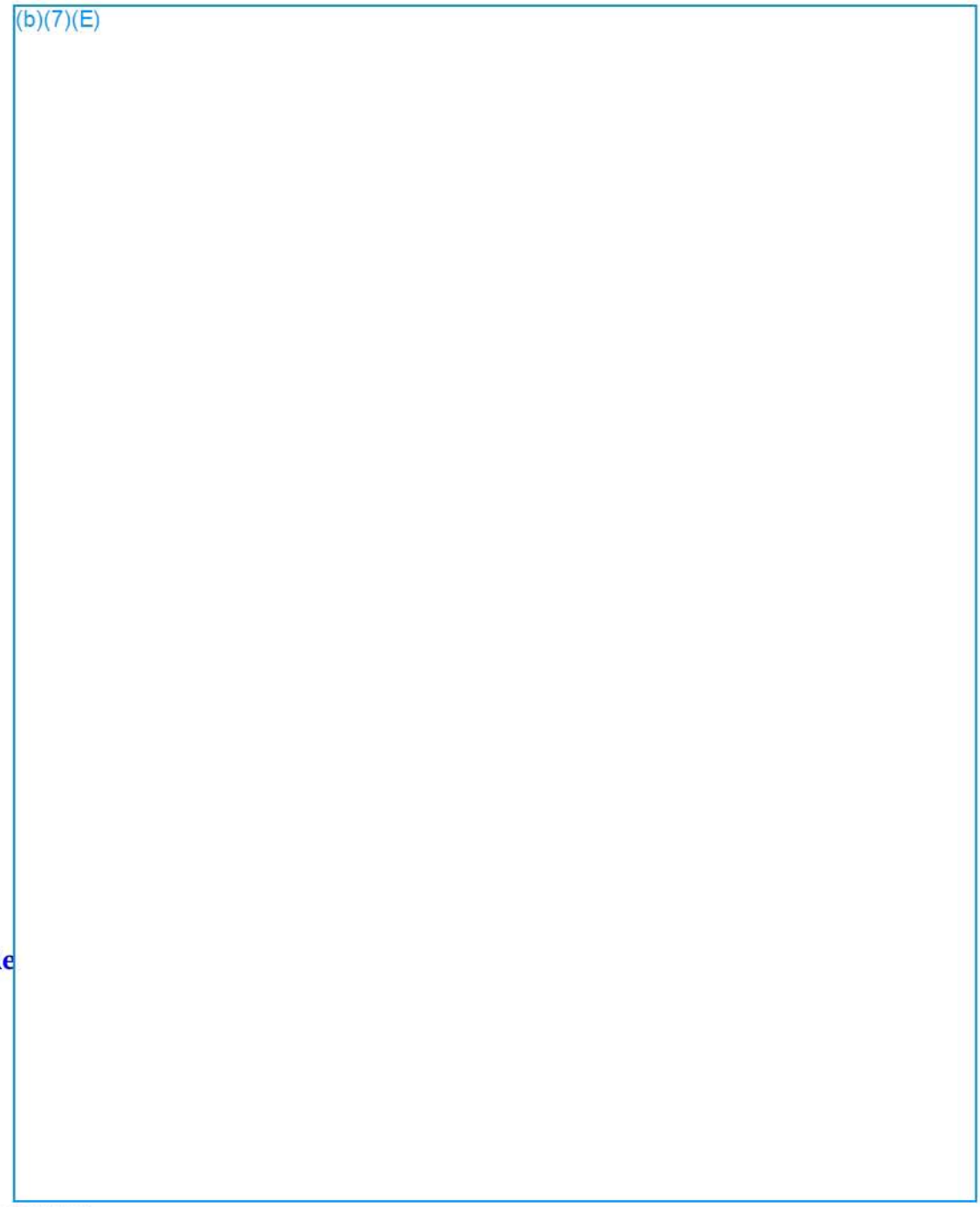
(b)(7)(E)



Brows

Steps (continued)

(b)(7)(E)



Re

(BREAK)

D. Unstructured Import from Douglas Police Department (I)

Explain that previous example was unstructured data already residing within FALCON from the tip line. Unstructured data can be imported from external sources as well – this means local/state law enforcement or other federal agency reports, news articles, etc. Anything you as an agent or analyst believe to be valuable for your investigation. Unstructured import is a power tool to allow you as the

user to bring in external data sources and incorporate into analysis with all of ICE's data.

WHY? You reached out to local law enforcement in Nogales about reports of human smuggling and anything on the Western Union location from the tip – they provided a report on 3 Western Union locations they have received information on.

Steps

(b)(7)(E)

Practical Exercise (You)

(BREAK)

Section 2: Structured Data & Graph Application

(Day 1 Afternoon – approximately 3.5 hours)

A. Structured Import of Western Union Transactions (I)

Explain that a structured import is like unstructured import except that objects, properties and links are assigned to structured data during import rather than in a separate tagging exercise.

WHY? We have been given information from both the tip and local law enforcement that suspicious payments and activities have been reported at a group of Western Union locations. In addition, we know the payment size and cadence for this organization to be $2,000 initially and then $9,000 a week later. Transaction data from these Western Unions would help to paint the picture of the operation and the parties involved.

Steps

(b)(7)(E)

Repeat Steps together (WE)

1. Structured Import

(BREAK)

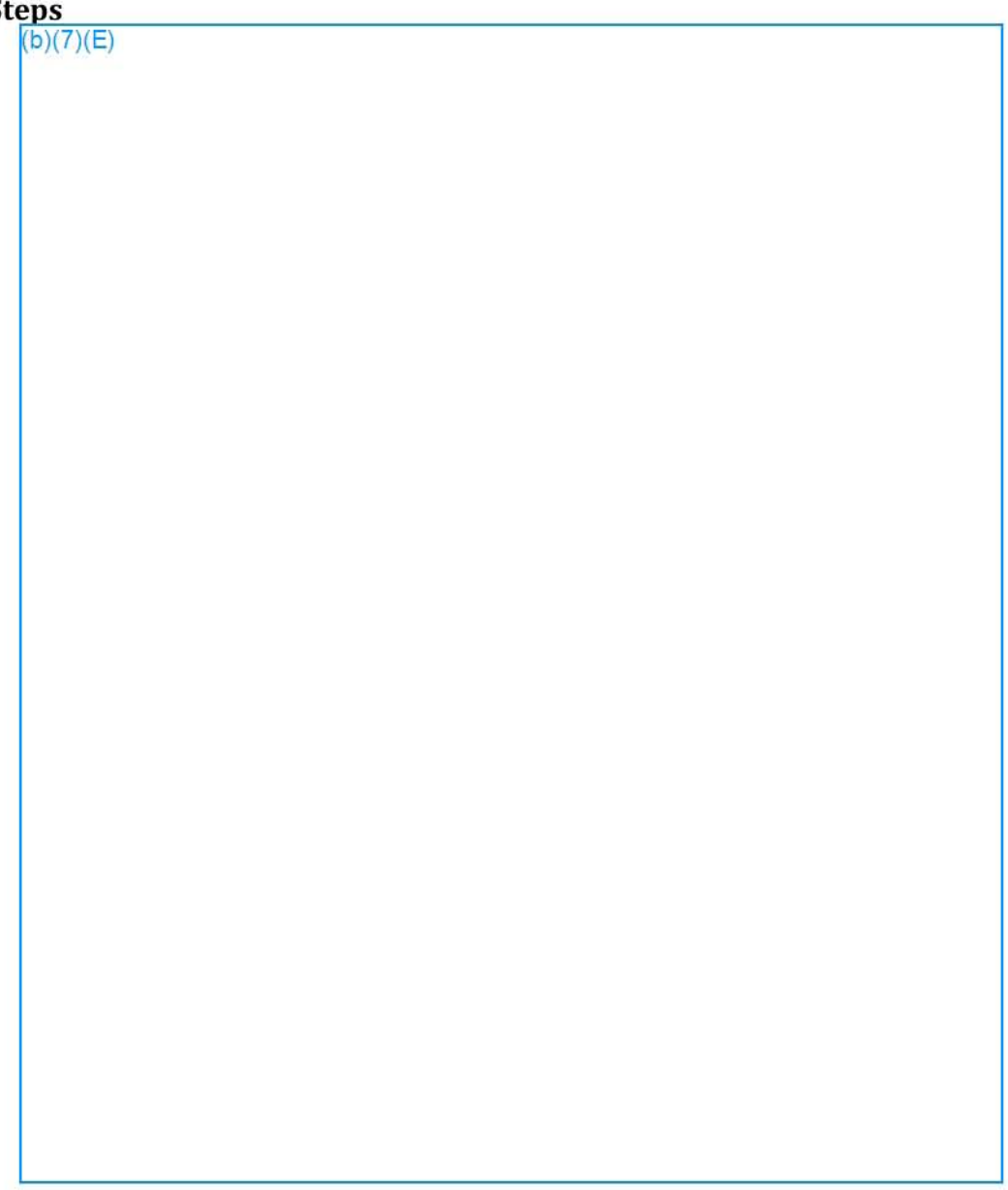
B. Navigate, Organize and Analyze in Graph Application (I)

Explain that the graph application allows users to analyze data in a much more accessible medium than structured or unstructured format. We can analyze and find patterns within these transactions in this format better than in structured or unstructured format.

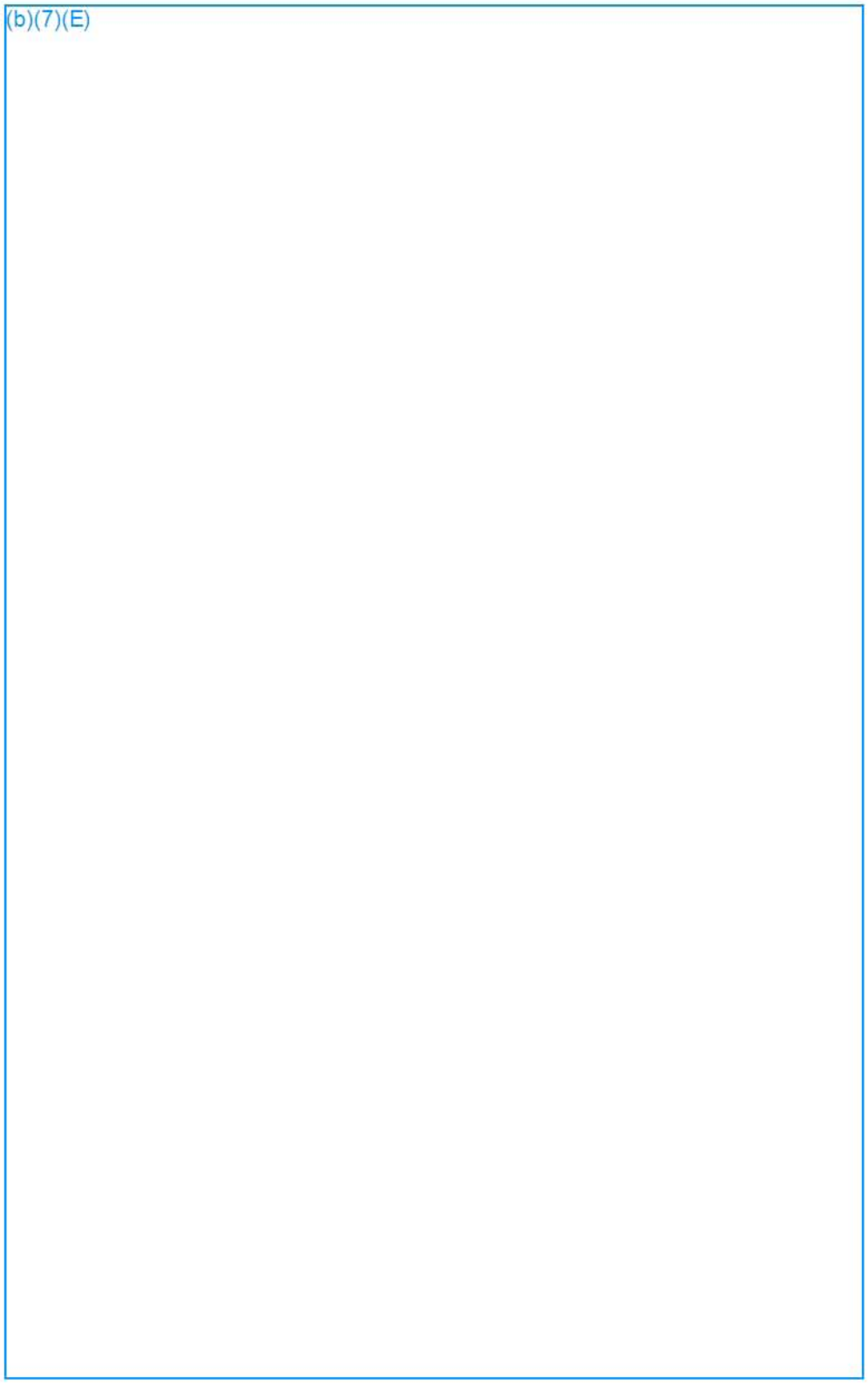
WHY? We know that the human smugglers demanded $2,000 and $9,000 payments so lets look at all payments of this size from the suspicious Western Union locations to look for a pattern.

Steps

(b)(7)(E)



(b)(7)(E)



Repeat Steps together (WE)

1. Navigate, organize and analyze objects on graph application

Practical Exercise (You)

Section 3: CDR Helper & Collaboration Application
(Day 2 Morning – approximately 1 hour)

A. CDR Helper (I)

Explain that the CDR helper is a repository of subpoenaed calls associated with phone numbers of interest (great way to discover possible overlap with other cases). The CDR helper quickly queries and returns results, if any, to be incorporated into analysis.

WHY? We have phone numbers associated with payments and people possibly involved with human smuggling – check to see if there is any existing information on other associations with possible wrongdoer's phones.

Steps

(b)(7)(E)

B. Presentation Features (I)

Explain that presentation features are great for telling the story you have uncovered. Palantir is a tool that not only enables you as an

agent or analyst to perform in depth analysis, but gives you the tools to present the analysis in a way that allows other agents and analysts to full grasp the your investigation.

WHY? We have uncovered a connection between possible illicit Western Union wire transfers and an existing human smuggling case. In order for other agents and analyst to under this connection, we need to use Palantir's presentation features to fully tell the story of our investigation.

Steps

(b)(7)(E)

C. Collaboration Application (I)

Explain Palantir allows for and is most effectively used when users collaborate and share data and analysis while staying within proper security boundaries. The collaboration application is good way to facilitate sharing and combine crucial information about cases across the organization.

WHY? There is an open investigation on the smuggling organization you have identified. The collaboration application allows users build out investigations between multiple users so that the most accurate picture of reality can be realized. Palantir makes it easy to share discoveries and analysis from investigations with other agents and analysts with ICE.

Steps

(b)(7)(E)

Repeat Steps together (WE)

1. CDR helper
2. Presentation features
3. Set object watch feed
4. Use target exporter
5. Export graph HTML
6. Discuss collaboration application

Section 4: Map Application
(Day 2 Morning – approximately 2 hours)

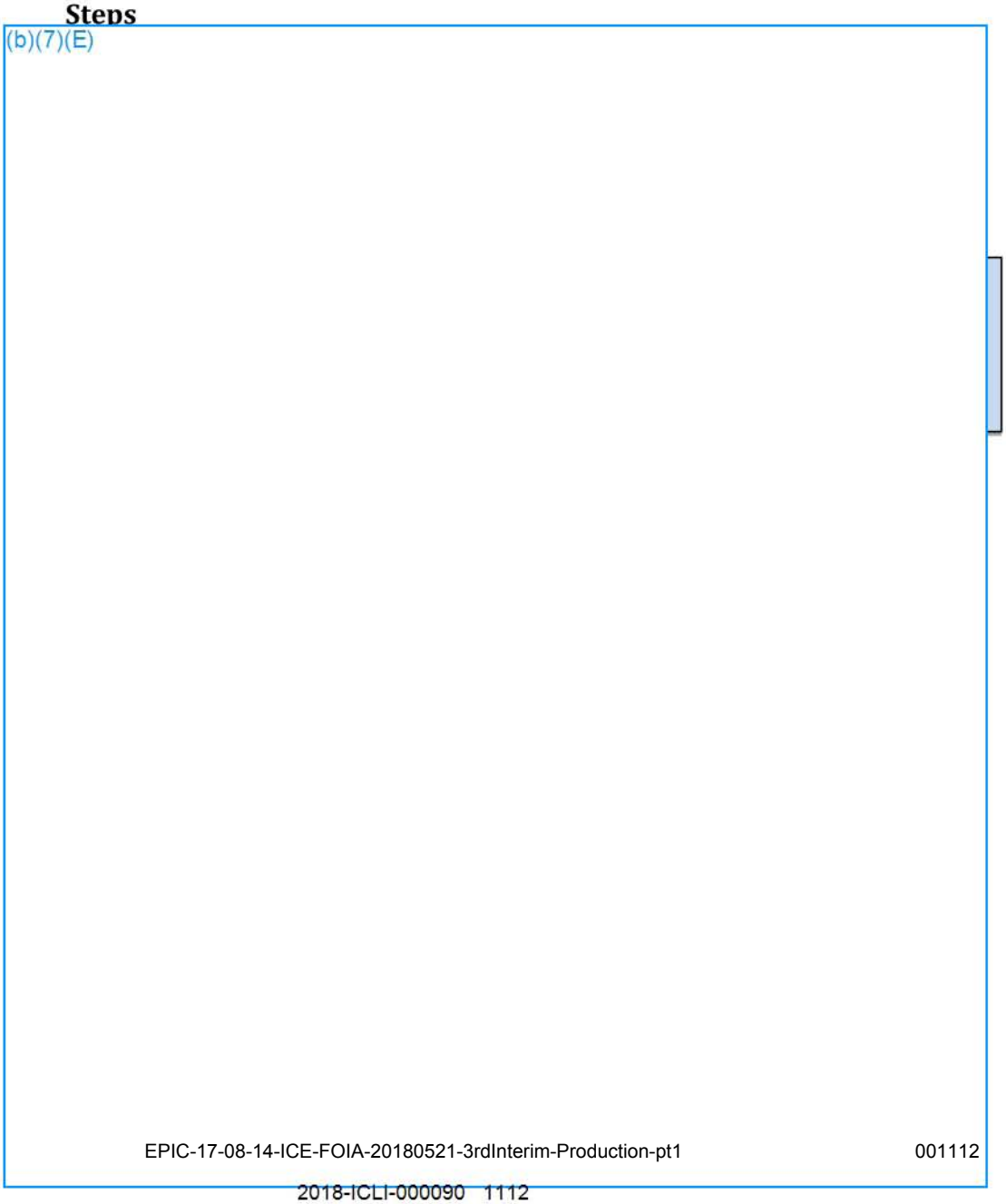
A. Map Application (I)

Explain that the map application is an analytical tool for geospatial data - in this instance, the application is a great place to look at patterns in both space and time.

WHY? The other agent/analyst on the investigation published new data on the new phone phones associated with the Western Union payments. The agent subpoenaed the new phone records and identified the "Handler' as possibly important to the human smuggling operator. To better understand movements and activities, he/she placed GPS pings on the phone – the GPS data lends itself to the map application to analyze the activities of the suspect in both space and time.

Steps

(b)(7)(E)



Repeat Steps together (WE)

1. See shared graph from Lewis Card and add to graph
2. Add pings to map (Don't do heatmap together)
3. Explore pings in the timewheel
4. Perform radius search around Sierra Vista Motel.

Practical Exercise (You)

These are the columns of Western Union data that will be mapped automatically when you use the PIM file during the import and the type of objects that will be created. The names of the columns in excel are **bold**, the Falcon properties are not. The color corresponds to the color used in the excel.

(b)(7)(E)

These are the columns of Western Union data that will be mapped automatically when you use the PIM file during the import and the type of objects that will be created. The names of the columns in excel are **bold**, the Falcon properties are not. The color corresponds to the color used in the excel.

(b)(7)(E)

(b)(4)

FALCON Mobile Overview
NCIC Search Capability

New NCIC Search Feature

(b)(4)

(b)(7)(E);(b)(4)

NCIC Workflow Example

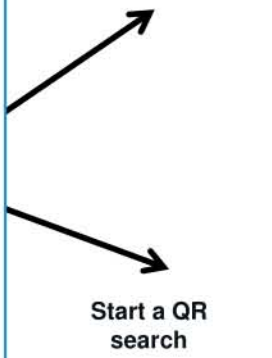
(b)(4)

QH Search

QH Result

Follow-on Searches

(b)(7)(E);(b)(4)



(b)(7)(E);(b)(4)

FALCON Resources

(b)(4)

FALCON Help

Please direct any systems related questions or concerns regarding FALCON to the FALCON Help Desk at: (b)(7)(E)

FALCON Web Resources

For announcements, video tutorials, and how-to guides, visit the FALCON Home page: (b)(7)(E)

FALCON Training

If you or your team are interested in additional training or have questions, comments, or requests concerning the FALCON program, please reach out to your local Field Service Representative or (b)(7)(E)

MOBILE FEEDS

Quick Reference Guide

With a few clicks and some keywords, FALCON can be set-up to automatically send alerts to your mobile app when new data matching your criteria is added to the system. There are 3 types of feeds; Filter Feeds, Object Watch Feeds, and Document Search Feeds.

To set up and receive mobile feed results you will need a Falcon account and the Falcon mobile app. If you do not have a Falcon account please visit this link to learn more: FALCON Account. If you already have a FALCON account, then check out the FALCON Mobile tab in the right panel of the FALCON homepage (b)(7)(E) for instructions on how to create your own custom feeds.

Feed Types

1) *Object Watch Feeds – sends alerts when changes are made to a specific object. For example: an object watch feed for a case or a person would send alerts when those objects are changed or updated. New links, properties or media are examples of changes that would result in an alert.*

2) *Document Search Feed – uses keywords to identify documents and send alerts. The feed can be focused on specific document types. Examples: 1) alerts are sent whenever an HSI Tipline report is created with the keywords "Baltimore" and "MS-13" 2) alerts are sent whenever an ROI is written that contains the words "Bitcoin" and "narcotics proceeds".*

3) *Filter Feeds – This is the most versatile type of feed. You can choose any object type (person, SEACATS seizure incident, etc.) and add specific properties of interest for that object and the feed will send alerts when it finds matches. Examples: 1) get alerts every time there is a SEACATS seizure of a mail parcel containing synthetic marijuana that was destined for an address in a particular state, city or zip code 2) set alerts for any HSI Tipline report for a specific SAC/RAC area AND a specific category (narcotics, human trafficking, financial, etc.)*

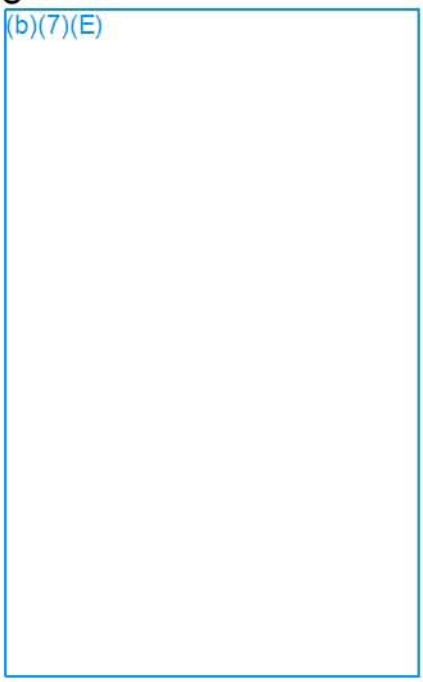
MOBILE FEEDS
Quick Reference Guide

Viewing Feeds Using Mobile App

(b)(7)(E);(b)(4)

MOBILE FEEDS
Quick Reference Guide

(b)(7)(E)

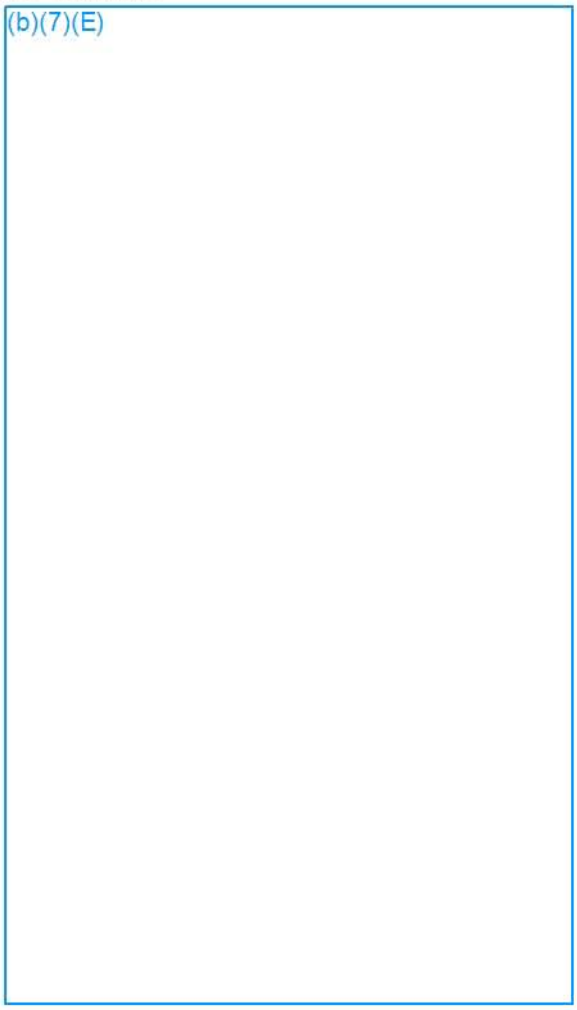


3) Unread feed results have **blue** text but will revert back to black after they are read. There is a 'Mark all read' button which will also eliminate the red alert notification on the feed.

MOBILE FEEDS

Quick Reference Guide

(b)(7)(E)



Conclusion: *Mobile feeds are a great way to get notifications without having to log onto a computer and run the search yourself. If you have any questions, concerns, or ideas for future enhancements to this feature, please don't hesitate to send them to the Falcon Help Desk* (b)(7)(E)