

# Exhibit B

**From:** (b)(6);(b)(7)(C)  
**Sent:** 21 Oct 2016 10:21:17 -0400  
**To:** (b)(6);(b)(7)(C)  
**Cc:**  
**Subject:** Re: Social Locator for OST SOP  
**Attachments:** GOST Brochure.pdf

(b)(6);(b)(7)(C)

Giant Oak is currently finalizing a package of approved "marketing materials" so this is great timing. For the time being, I have attached a brochure for GOST, but keep in mind that the language is tailored for the financial industry, not government. I will get you one tailored to federal law enforcement in the coming weeks.

I can provide some contract language in the meantime:

(b)(5)

On Fri, Oct 21, 2016 at 9:59 AM, (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

wrote:

Hey (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C) and I are working hard to update our entire OST standard operational procedure and training manual(s). We'd like to add quite a bit more about Giant Oak and specifically Social Locator. Do you have any available documents, white papers, or general summaries on Social Locator that we could utilize?

I know there's a couple out there but I can't find them, at least not on my laptop from home.

Thank you,

(b)(6);(b)(7)(C)

# Homeland Security Investigations (HSI)



## Open Source Collection Tools

- Part I – OS Image Guide

(b)(6);(b)(7)(C)

Part II – Arabic

Translation Manual

(b)(6);(b)(7)(C)



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

OS I



U.S. Immigration and Customs Enforcement

# Homeland Security Investigations (HSI)

## OS Image Guide



### What is it?

**-A reference guide created to identify images and symbols commonly associated with terrorist and criminal organizations or other groups of interest**

### Purpose

**-To familiarize analysts with these images and symbols as part of their preparation for open source analysis. This may help to identify derogatory information, or supply further background on a subject**



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## OS Image Guide

### Contents



- The guide currently has entries for 115 organizations from around the world – the primary focus is current and former terrorist organizations, but some criminal, para-military, and groups of interest are also included
- The guide includes the most common known symbols and flags associated with an organization, as well as a description of the group’s background



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## OS Image Guide



- **The OS Image Guide includes images that are considered logos or symbols related to these organizations. For the purposes of this guide, logos and symbols shall primarily refer to pictures, pictograms, banners, or flags. Organizations may also possess common mottos or slogans. These kinds of statements are not extensively covered in the OS Guide at this time, however, analysts note these during OS collection.**



U.S. Immigration  
and Customs  
Enforcement



# Homeland Security Investigations (HSI)

## Terrorists



(b)(7)(E)



**The Guide includes groups currently designated on US terrorist lists**



**U.S. Immigration  
and Customs  
Enforcement**

# Homeland Security Investigations (HSI)

## Terrorists



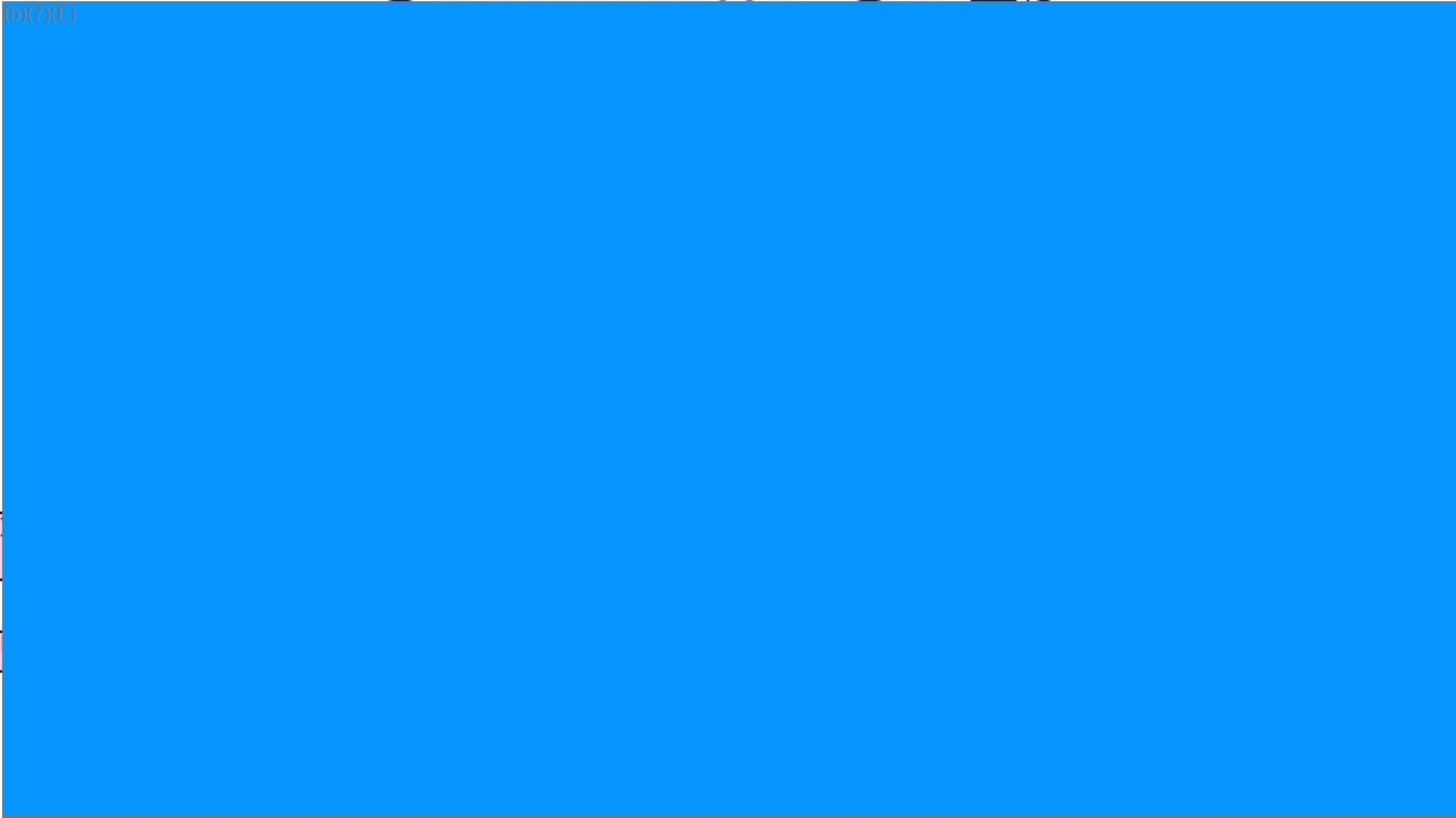
**The Guide also includes some lesser known terrorist groups, and previously designated terrorist groups**



**U.S. Immigration  
and Customs  
Enforcement**

# Homeland Security Investigations (HSI)

## Criminal Orgs



**The Guide includes select criminal groups and other organizations of note**



**U.S. Immigration  
and Customs  
Enforcement**

# Homeland Security Investigations (HSI)

## Example:



(b)(7)(C)

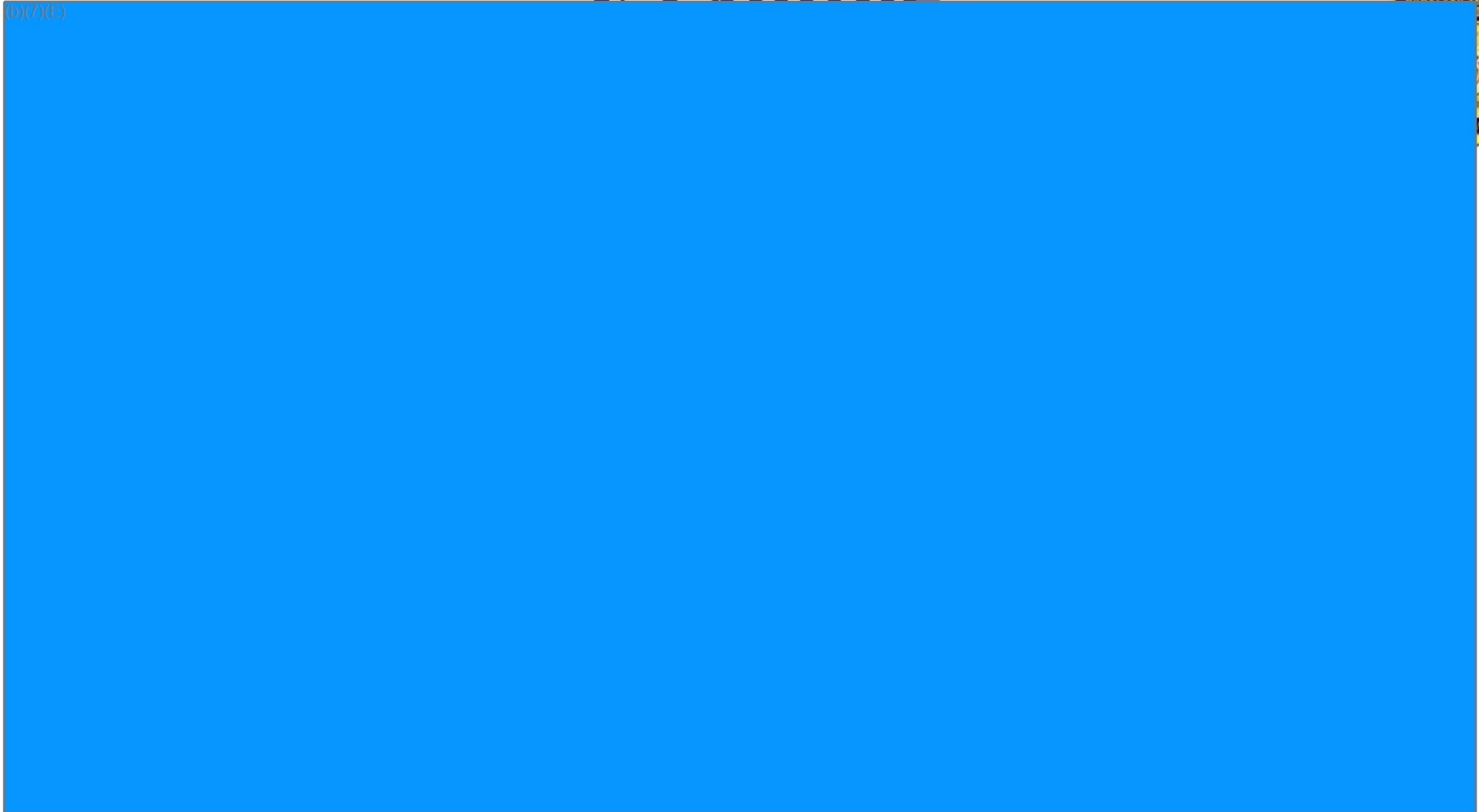


# Homeland Security Investigations (HSI)

## Example:



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

~~Low Enforcement Sensitive~~  
2019-ICLI-00017-441

# Homeland Security Investigations (HSI)

## Reminder



(b)(7)(C)



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## Cautions



- **While the OS Guide is a useful tool, it is not a comprehensive list of all the symbols that might be encountered during OS analysis. When you encounter an image or you can't identify or looks questionable, be a good analyst and conduct further research**



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)



## Arabic Translation Manual



U.S. Immigration  
and Customs  
Enforcement



# Homeland Security Investigations (HSI)



- Understanding the Arabic language and Islamic culture as it pertains to operations of the CTCEUR  
Recognizing the differences between “derogatory” and legitimate uses of Islamic or Arab culture  
Flags and symbols of recognized terrorist organizations  
Using Google to Translate Arabic to English



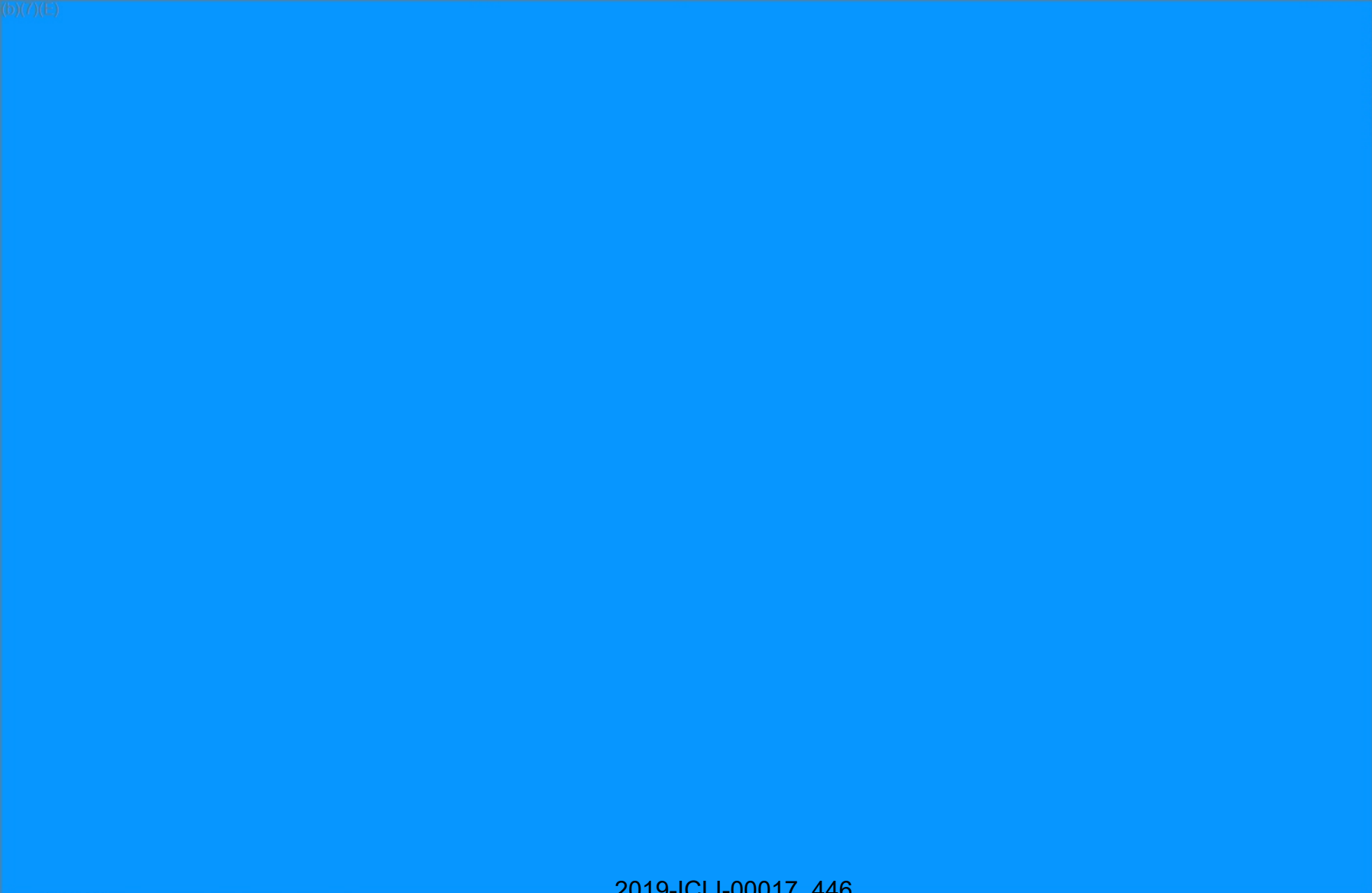
U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

## Islamic symbols, the *Shahada*



(b)(7)(D)



# Homeland Security Investigations (HSI)



(b)(7)(E)



U.S. Immigration  
and Customs  
Enforcement

# Homeland Security Investigations (HSI)

(b)(7)(E)



(b)(6);



U.S. Immigration  
and Customs  
Enforcement

~~Low Enforcement Sensitive~~  
~~2019-ICLI-00017 448~~



U.S. Immigration  
and Customs  
Enforcement

**Procurement Sensitive**

SECRET

Performance Work Statement  
Visa Lifecycle Vetting Initiative



Homeland  
Security

Page 230

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 231

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 232

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 233

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 234

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 235

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 236

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 237

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 238

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 239

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 240

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 241

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 242

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 243

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 244

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 245

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 246

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 247

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 248

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 249

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 250

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 251

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 252

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 253

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 254

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 255

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 256

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 257

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 258

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 259

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 260

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 261

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 262

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 263

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 264

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 265

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 266

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 267

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 268

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 269

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 270

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 271

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 272

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 273

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

LAW ENFORCEMENT SENSITIVE INFORMATION

**ATTACHMENT A  
PERFORMANCE WORK STATEMENT (PWS)  
HSCEMD-17-D-00001**

**Department of Homeland Security (DHS),  
U.S. Immigration and Customs Enforcement (ICE),  
Homeland Security Investigations (HSI)  
National Security Investigations Division (NSID)**

**Performance Work Statement (PWS)  
for  
Open Source/ Social Media Data Analytics**



**August 7, 2017**

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

**Table of Contents**

Part 1 - Overview and Contract Requirements ..... 3  
Part 2 - Privacy & Records Office (PRO) Clauses ..... 17  
**Part 3 - Personnel Security Requirements..... 20**

**ATTACHMENT A  
PERFORMANCE WORK STATEMENT (PWS)  
HSCEMD-17-D-00001**

**Performance Work Statement (PWS)**

**Open Source/ Social Media Data Analytics**

**Part 1 - Overview and Contract Requirements**

**1.0 INTRODUCTION**

The primary mission of the U.S. Department of Homeland Security (DHS) is to lead the unified national effort to secure the country and preserve our freedoms. While the Department was created to secure our country against those who seek to disrupt the American way of life, our charter also includes preparation for and response to all hazards and disasters. U.S. Immigration and Customs Enforcement (ICE) is responsible for the protection of the security of the American people and homeland by vigilantly enforcing the nation's immigration and customs laws.

**1.1 SCOPE**

This Performance Work Statement (PWS) encompasses behavioral based internet search technology, training, social science/program management support and compliance with all IT system and privacy requirements.

Behavioral based internet search technology includes both 1. Electronic batch and/or ad hoc queries received from the Government and 2. Continuous monitoring of individuals and/or entities identified by the Government.

Potential deliveries of services include all 50 US states plus various locations across the globe in which ICE has a presence.

Requests for the use of the behavioral based search technology procured by this contract may originate from any Program Office within DHS upon approval from the CTCEU COR; however only the ICE contracting officer may issue task orders under the resulting contract.

**2.0 BACKGROUND**

The National Security Investigations Division (NSID) was created in 2003 within the U.S. Immigration and Customs Enforcement (ICE) Office of Investigations. It is now a key component of the ICE Homeland Security Investigations (HSI) directorate and plays a critical role in advancing the ICE mission. NSID leads the effort to identify, disrupt and dismantle transnational criminal enterprises and terrorist organizations that threaten the security of the United States.

NSID protects the United States through the following missions:

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

- Enhancing national security through criminal investigations;
- Preventing acts of terrorism by targeting the people, money and materials that support terrorist and criminal activities; and,
- Identifying and eliminating vulnerabilities in the nation's border, economic, transportation, and infrastructure security.

Components within NSID include Counterterrorism and Criminal Exploitation Unit (CTCEU), Visa Security Program (VSP) and Student and Exchange Visitor Program (SEVP).

In 2013, NSID concluded that there was a requirement for an off the shelf, customizable behavior science based internet search technology which could be regularly refined and modified to address different political and operational environments. In 2014, CTCEU was the pioneer as the first to procure and utilize a behavior science based internet search technology that included social media. In 2016, VSP initiated a Social Media pilot program to utilize this technology to much success. In 2017, SEVP and CBP will create pilot programs to test usefulness of utilizing the software.

## **2.1 CTCEU**

The CTCEU is the first and only law enforcement entity entrusted with the enforcement of nonimmigrant visa violations. Today, through the CTCEU, ICE proactively develops cases for investigation from the Student Exchange Visitor Information System (SEVIS) and the Arrival and Departure Information System (ADIS) datasets—which house the records of millions of students, tourists, and temporary workers present in the United States at any given time; to include flight schools and foreign students attending those schools—or those who have overstayed or otherwise violated the terms and conditions of their admission.

Each year, the CTCEU analyzes records of potential status violators, based on data received from SEVIS, ADIS, and other sources. These records are resolved by further establishing potential violations that would warrant field investigations, establishing compliance, or establishing departure dates from the United States. Since the creation of the CTCEU in 2003, analysts have resolved more than 2 million such records using automated and manual review techniques. The CTCEU drew upon various government databases to gather and analyze the identifiable national security leads on foreign students, exchange visitors, and other nonimmigrant visitors.

In order to identify those that pose the greatest threat to national security, the CTCEU employs various targeting and prioritization rules to detect and identify individuals exhibiting specific risk factors based on intelligence reporting, including international travel from specific geographic locations to the U.S., and in-depth criminal research and analysis of dynamic social networks. The targeting and prioritization rules employed by CTCEU are not static and evolve with time, relying on emerging intelligence from inside the Homeland as well as from the intelligence community and theaters overseas. Many of the highest threat leads identified by CTCEU are worked in collaboration with many Federal Agencies.

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

**2.2 VSP**

In an effort to enhance HSI's initiative on safeguarding against terrorism and ensuring the security of the Homeland, CTCEU coordinated its Open Source/Social Media Exploitation capabilities with the NSID Visa Security Program's (VSP) PATRIOT screening and vetting operations and social media exploitation to develop and implement a Social Media pilot program in furtherance of the Overstay Life-Cycle Initiative.

This program aims to more fully leverage social media as a tool to identify the whereabouts and potential derogatory activity of status violators, and provide enhanced knowledge about a non-immigrant visitors' social media postings. The social media tracking will give the U.S. government better visibility should a non-immigrant visitor engage in unlawful activity (e.g. criminality, terrorism, administrative immigration violations) and the program could potentially reveal social media based signs that the individual is becoming radicalized, or is attempting to recruit or radicalize others while present in the U.S.

The Social Media program builds on existing NSID visa security and overstay enforcement efforts, and enhances the ability of HSI to identify potentially derogatory information that is not found in U.S. government holdings. The Social Media Program complements the current VSP PATRIOT operations, and brings a new and important dimension to HSI's visa security and overstay enforcement efforts.

**2.3 SEVP**

Student and Exchange Visitor Program (SEVP) collects, maintains, analyzes and provides information so only legitimate foreign students or exchange visitors gain entry to the United States. The result is an easily accessible information system that provides timely information to Department of State, U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), and U.S. Immigration and Customs Enforcement (ICE), as well as a number of other federal enforcement agencies with "need to know."

The Student and Exchange Visitor Program (SEVP) Analysis and Operations Center (SAOC) provides stakeholders with a single interface for high quality, timely, analytical reports; as well as school compliance and student issue services. SAOC monitors SEVP-certified schools and nonimmigrant students for administrative compliance with applicable federal statutes, and SEVP regulatory record keeping and reporting requirements. SAOC also coordinates with the Counter Terrorism and Criminal Exploitation Unit (CTCEU) and Homeland Security Investigations (HSI) Special Agent in Charge (SAC) offices to lead all administrative investigations related to school and nonimmigrant student compliance.

**2.4 CBP**

U.S. Customs and Border Protection's Electronic System for Travel Authorization (ESTA) allows citizens from 38 select countries to apply to enter the United States without a VISA. CBP

**ATTACHMENT A  
PERFORMANCE WORK STATEMENT (PWS)  
HSCMD-17-D-00001**

is currently looking to test, pilot, and acquire commercial technologies which may aid in incorporating open source and publicly available datasets into its ESTA vetting process.

**3.0 OBJECTIVES**

The purpose of this task order is to obtain mission critical open source search and triage capabilities to include continuous monitoring through custom alert services which will allow DHS to proactively screen travelers and investigate national security leads. In some cases these leads may have incomplete address information and may also include leads that have been returned from field investigations without a resolution. The search capabilities will also be applied to visa waiver travelers, visa applicants, and visa holders.

The contractor shall use a wide range of proprietary, commercially available, open source data to ensure optimal search capability for difficult to find individuals or simply for those individuals whose open source presence is deemed important for screening purposes. Publicly available data searches can include credit bureau information, utilities, real estate, criminal databases and open source publicly available search data such as data from a variety of social media sites including Facebook, LinkedIn, Twitter and others This will enable DHS to leverage data sources in powerful ways to search for persons of interest in both large batches and individual searches. Any proposed solutions to the data analytics and custom alert services requirement must be able to address the following objectives:

- DHS requires data and analytic services that integrate areas of expertise in law enforcement and social science to meet increasing demands for efficiency in accomplishing their unique mission.
- DHS requires that analytics have significant social media and internet searching capabilities.
- DHS requires analytics based upon the application of social and behavioral sciences to multiple data sets to locate these dangerous individuals who pose an eminent threat to the United States.

**4.0 SERVICE PROVIDER – NON PERSONAL SERVICES**

DHS/ICE retains the authority to make all decisions regarding the DHS/ICE mission, and the execution or interpretation of laws of the United States. Contractor services defined are not considered to be inherently Governmental in nature, as defined by Federal Acquisition Regulation (FAR) Subpart 7.5. This is a Non-Personal services contract as defined by FAR Subpart 37.101. Contractor personnel rendering services under this order are not subject to supervision or control by Government personnel.

**5.0 REQUIREMENTS**

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

**a. General Requirements**

The contractor's technology shall track daily address changes and credit activity of individuals (i.e. new aliases, DOB changes, SSNs, etc.), where applicable, to hundreds of thousands of updates from their data sources and compare them to the subjects provided to them on a periodic basis (no more frequent than daily). The contractor shall not search, reference, or use as a source any license plate reader databases. Any relevant changes are then sent out to DHS personnel to review and determine if the information identifies a viable location of the subject, where applicable. The provider must be able to conduct rapid electronic batch searches on entities for information relating to the DHS mission which pose a danger to national security or a risk to public safety. The contractor shall not maintain any data, including the list of individuals provided by ICE and search results provided to ICE, after the government requests the contractor remove the data, nor shall the contractor maintain any data on behalf of ICE after the data is no longer in a state of analysis.

**Return of Information from Non-Open Source and Social Media Sources:**

The contractor shall return to DHS from publicly available or proprietary sources available to the contractor, any information that tracks address changes and changes in identifiers of individuals; i.e. new aliases, date of birth changes, SSN changes, Utility changes, Credit checks, Death Registry, Employment changes, Insurance, where applicable.

**Return of Information from Open Source and Social Media Sources:**

The contractor shall return to DHS any publicly available information that may suggest the presence or existence of derogatory information. The publicly available information may also identify the possible location of an entity, through contact information such as phone numbers, email addresses, or user names; affiliated organizations by which a location can be derived; and employers, where applicable. This initial search and return of information (i.e., tier 1) is limited to information directly connected to the target and may be conducted using open publicly available sources including, but not limited to, Facebook, Google+, LinkedIn, Pinterest, Tumblr, Instagram, VK, Flickr, Myspace, or Twitter. The contractor platform will allow for a launch point to find an open source publicly available collection of any public messages (e.g., Tweets), postings, and media (photos, documents such as resumes, and geocached information) when such messages exist. Search results directly connected to the target that also contain information related to the target's associates shall be included with all tier 1 information returned to ICE.

Upon exhaustion of tier 1 information, ICE may request that the contractor technology conduct a follow-up search and return of information (i.e., tier 2) that includes any publicly available information about the target's associates, such as family members, friends, or co-workers, through which a location of the target may be derived. Tier 2 searches may be conducted using the aforementioned social media sources.

**b. Specific Tasks**



**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

The following items will be provided by the Contractor, when required under a funded task order.

**Task 1:** The contractor shall create a custom domain of the internet, when requested and funded by the Government, that includes communication between the government and the contractor during project launch and periodically throughout software deployment to determine priorities, useful sources, and normal workflow. Part of the domain creation process includes putting greater focus on areas of the open source where government subject matter experts have identified useful data in past work. In addition, part of the domain building process can include the government furnishing the contractor with “ground truth” data which is helpful in modeling human behavior, maturing the custom domain of the internet. Domain refinement will continue throughout the course of the deployment through integration of lessons learned from user clicks. The process of domain creation is an ongoing process that will be revisited periodically to make the software smarter and most efficient. A written report will be provided to the Government upon initial domain definition .

**Task 2:** The Base Subscription provides monthly unlimited access to contractor’s proprietary data mining software for the purpose of processing, not to exceed 1.2 million ad hoc or batch Entity Queries, of which not to exceed 120,000 entities will be subject to Continuous Monitoring. This subscription is fixed price per month, invoiced monthly.

**Task 3: Queries:** The government shall provide the contractor system with Ad Hoc and Batch searches of up to the funded number of entity queries in each task order. The contractor shall provide continuous monitoring and alert systems up to 10% of funded queries in order to monitor information for new activity. Location information will have mapping capabilities. Alerts will be pushed directly to the software on a frequency to be determined by the component office (no more frequently than daily).

**Task 4:** The contractor shall provide On-Site Internet Domain Support Services at either a full time or part time basis.

**Task 5:** The contractor shall provide onsite or virtual training (to be mutually agreed by the government and contractor) that will include annual certification in the use of the Software Tool. Training will include all resources required to obtain certification.

**Task 6:** ATO and Ongoing security scans and remediation in accordance with HSAR Deviation 15-01.

**Task 7:** Travel, as deemed necessary by the government.

**5.1 COLLECTION OF SOCIAL MEDIA INFORMATION**

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

The contractor and contractor personnel must adhere to the following requirements when obtaining information from social media sources in fulfillment of their duties under the contract:

1. **Obtaining Information from Unrestricted Sources.** When conducting social media searches, the contractor may obtain information from publicly-accessible online sources and facilities under the same conditions they may obtain information from other sources generally open to the public. This principle applies to publicly-accessible sources located in foreign jurisdictions as well as those in the United States.
2. **Accessing Restricted Sources.** When conducting social media searches, the contractor may not access restricted online sources or facilities.
3. **Obtaining Identifying Information about Users or Networks.** The contractor may not use software tools, even those generally available as standard operating system software, to circumvent restrictions placed on system users.
4. **Public Interaction.** The contractor may access publicly-available information only by reviewing posted information and may not interact with the individuals who posted the information.
5. **Appropriating Online Identity.** "Appropriating online identity" occurs when an entity electronically communicates with others by deliberately assuming the known online identity (such as the username) of a real person, without obtaining that person's consent. The contractor may not use this technique to access information about individuals.
6. **PII Safeguards.** The contractor will protect personally identifiable information (PII) as required by the Privacy Act and DHS privacy policy.
7. **International Issues.** Unless gathering information from online facilities configured for public access, law enforcement personnel conducting investigations should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever an item or person is located abroad, law enforcement personnel follow ICE's policies and procedures for international investigations.

**6.0 POSITION(S) DESCRIPTION(S)**

The Contractor is to provide monitoring data and custom alert technologies. The following position(s) may need access to Classified Information.

**6.1 SOCIAL SCIENTIST**

**Position Description:** The Social Scientist assists NSID analysts in analyzing the trails of data left by people in social media, public records, and other data sources resulting

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

from human behaviors and decisions. The Social Scientist tweaks the algorithms behind the Search Technology and works with NSID analysts and the software development team to identify and integrate new sources of data in the system. The Social Scientist also improves the transliteration and name matching tools built into software to be further specialized for certain ethnic groups, non-roman languages and alphabets, or countries of origin. To be truly proficient and knowledgeable, the Social Scientist will, on occasion, require access to classified facilities in order to engage in meaningful conversations related to homeland security missions, and obtain awareness of emerging relevant technologies in the Intelligence and Law Enforcement communities, for the benefit of the software's continued useful deployment within NSID.

**Classification Level:** This position requires access to classified information at the TS/SCI level

**PROGRAM MANAGER/DATA SCIENTIST**

**Position Description:** In order to implement a successful deployment of the behavioral based internet search technology within NSID, it is required that the vendor provide a person with program management and data science expertise. The program management responsibilities will include contract oversight, including programmatic and financial functions. The Data Scientist function is highly important to the software's success within NSID, as this role is responsible for executing experiments pertaining to major components of the system (i.e. data comparisons, reliability and relevance scoring, algorithm accuracy, etc.) and subsequently assessing the statistical significance of all experiment outcomes. To be truly proficient and knowledgeable, the Program Manager/Data Scientist will, on occasion, require access to classified facilities in order to engage in meaningful conversations related to homeland security missions, and obtain awareness of emerging relevant technologies in the Intelligence and Law Enforcement communities, for the benefit of the software's continued useful deployment within the NSID.

**Classification Level:** This position requires access to classified information at the TS/SCI level

**7.0 GENERAL REQUIREMENTS**

**7.1 PERIOD OF PERFORMANCE**

The total potential Period of Performance is five years.

**7.2 PLACE OF PERFORMANCE**

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

The locations in which the internet search technology will be predominately be utilized are listed below however, the Government may utilize the software from alternative work sites such as teleworking and international locations.

CTCEU  
HSI Division 1  
1525 Wilson Blvd suite #425  
Arlington, VA 22209

VSP  
HSI Division 1 VSCC  
1953 Gallows Road  
VIENNA, VA 22182

SEVP  
2451 Crystal Drive  
Arlington, VA 22202.

CBP  
22330 Glenn Drive  
Sterling, VA 20164

**7.3 CONTRACT TYPE**

This contract will be a single award Indefinite Delivery, Indefinite Quantity contract (IDIQ).

**7.4 CONTRACT PROGRESS – MEETINGS AND TELECONFERENCES**

The Contracting Officer (CO) , Contracting Officer Representative (COR) and Government Program Manager as appropriate will meet periodically or participate in teleconferences with the Contractor to review contract performance, progress, and resolve technical issues. Minutes of the meetings/teleconferences, with action items identified, shall be documented by the Contractor and provided to the COR no later than 72 hours after meeting.

**7.5 RELEASE OF INFORMATION**

Contractor access to proprietary and Privacy Act-protected information (covered by DHS/ICE-009 External Investigations System of Records Notice (SORN)) is required under the PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the Privacy Act of 1974, and the *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*. Contractor and subcontractors shall not hold any discussions or release any information relating to this contract to anyone not having a direct interest in performance of this contract, without written consent of the CO. This

~~LAW ENFORCEMENT SENSITIVE INFORMATION~~

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

restriction applies to all news releases of information to the public, industry or Government agencies, except as follows: Information for actual or potential subcontractors or other individuals necessary for Contractor's performance of this contract. Contractor and subcontractors shall not issue advertisements about projects performed under this task without government review and approval. For the purposes of this paragraph, advertisement is considered to be Contractor-funded promotional brochures, posters, tradeshow handouts, world-wide-web pages, magazines, or any other similar type promotions.

**7.6 NON-DISCLOSURE STATEMENTS**

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of these tasks and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of these tasks. Contractor personnel are required to sign Non-Disclosure statements (DHS Form 11000-6).

**7.7 TRAVEL**

The Contractor shall coordinate specific travel arrangements with the COR to obtain advance, written approval for the travel to be conducted. The Contractor's request for travel shall be in writing and contain the names of individuals traveling, dates, destination, purpose, and estimated costs of the travel. The Government will not reimburse for local travel. Local travel is defined as travel within a 50-mile radius of the Contractor personnel's specific place of performance.

No travel at government expense is authorized unless fully funded on the contract in advance of travel.

The Contractor shall, to the maximum extent practicable, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase. Charges associated with itinerary changes and cancellations under nonrefundable airline tickets may be reimbursable as long as the changes are driven by the work requirement. Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e., designated work Site) shall not be reimbursed. Costs associated with Contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs and Federal Travel Regulations, prescribed by the General Services Administration, for travel in the contiguous United States.

**8.0 DELIVERABLES**

The Contractor shall provide the following deliverables:

The list below reflects the deliverables. The Government will establish a Quality Assurance Surveillance plan that is not part of this task order in order to monitor performance requirements summary items described in the list below.

~~LAW ENFORCEMENT SENSITIVE INFORMATION~~

**ATTACHMENT A  
PERFORMANCE WORK STATEMENT (PWS)  
HSCMD-17-D-00001**

**DELIVERABLES SCHEDULE:**

<b>Deliverable</b>	<b>Reference</b>	<b>Type of Report</b>	<b>Frequency</b>	<b>Due Date</b>
Post Award Conference (Kick-off Meeting) Minutes	Para 10.0	Draft – Word; Final – PDF	Once	Draft due within 7 calendar days after meeting. Final version due within 5 calendar days of government’s review of Draft.
Invoice Courtesy Copy	Para 8.2	Electronic	Monthly	No later than the 10 <sup>th</sup> calendar day of the month
Monthly Meeting Notes	Para 7.4	Meeting Notes; electronic Delivery	Monthly	Draft due within 7 calendar days after meeting. Final version due within 5 calendar days of government’s review of Draft.
Ad Hoc Reports	Para 8.1	Electronic	As required	Due within 5 working days of request

<b>Deliverable</b>	<b>Reference</b>	<b>Type of Report</b>	<b>Frequency</b>	<b>Due Date</b>
Post Award Conference (Kick-off Meeting) Minutes	Para 10.0	Draft – Word, Final - PDF	Once	Draft due within 7 calendar days after meeting. Final version due within 5 calendar days of government’s review of Draft.
Invoice Courtesy Copy	Para 8.2	Electronic	Monthly	No later than the 10 <sup>th</sup> calendar day of the month
Querie Results	Para 5.0	Electronic Record	As required	Within 24-48 hours

**ATTACHMENT A  
 PERFORMANCE WORK STATEMENT (PWS)  
 HSCEMD-17-D-00001**

Training Certification	Para 5.0	PDF	As required	Upon course completion
Written report of the initial domain definition	Para 5.0	PDF	Once	Upon completion of initial setup
Monthly Meeting Notes	Para 7.4	Meeting Notes; electronic Delivery	Monthly	Draft due within 7 calendar days after meeting. Final version due within 5 calendar days of government's review of Draft.
Ad Hoc Reports	Para 8.1	Electronic	As required	Due within 5 working days of request

**8.1 AD HOC REPORTS**

The government may request a variety of ad hoc reports. The Contractor shall create and run routine and non-routine ad hoc reports, as requested.

**8.2 INVOICE COURTESY COPY**

The contractor shall provide a courtesy copy of the monthly invoice to the CO and COR.

**9.0 GOVERNMENT ACCEPTANCE PERIOD:**

The Task Order COR will review the deliverables prior to acceptance and provide the Contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the Task Order COR will send an e-mail to the Contractor as notification that the deliverable has been accepted. A lack of response by the Government within 20 **calendar** days can be construed as acceptance. In this event a final version, if applicable must be submitted by the vendor within the allocated number of days

In the event of a rejected deliverable, the Contractor will be notified in writing by the Task Order COR of the specific reasons for rejection. The Contractor shall have an opportunity to correct the rejected deliverable and return it per delivery instructions.

**10.0 POST AWARD ORIENTATION CONFERENCE:**

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

The contractor shall participate in a post-award conference for the purposes of making introductions, coordinating security requirements, discussing schedules, prioritizing SOW requirements.

The contractor shall commence work on the first day of the period of performance. The Post Award Orientation Conference shall be coordinated with the Contracting Officer and held no later than 10 days after award.

**11.0 PRIVACY ACT:**

Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

**12.0 REPORTING SUSPECTED LOSS OF SENSITIVE PII**

Contractors must report the suspected loss or compromise of Sensitive PII (as defined in the *Guide to Safeguarding Sensitive PII at DHS*) to ICE in a timely manner and cooperate with ICE's Inquiry into the incident and efforts to remediate any harm to potential victims.

1. Contractor must report the suspected loss or compromise of Sensitive PII by its employees or sub-Contractors to the ICE Contracting Officer's Representative (COR) or Contracting Officer within one (1) hour of the initial discovery.
2. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and sub-Contractors are trained to identify and report potential loss or compromise of Sensitive PII.
3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of Sensitive PII containing the following information:
  - a. Narrative, detailed description of the events surrounding the suspected loss/compromise.
  - b. Date, time, and location of the incident.
  - c. Type of information lost or compromised.
  - d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
  - e. Names of person(s) involved, including victim, Contractor employee/sub-Contractor and any witnesses.
  - f. Cause of the incident and whether the company's security plan was followed or not, and which specific provisions were not followed.
  - g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.



**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

- h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.
4. The Contractor must cooperate with ICE or other government agency inquiries into the suspected loss or compromise of Sensitive PII.
5. At the government's discretion, Contractor employees or sub-Contractor employees may be identified as no longer eligible to access Sensitive PII or to work on that contract based on their actions related to the loss or compromise of Sensitive PII.

ATTACHMENT A  
PERFORMANCE WORK STATEMENT (PWS)  
HSCMD-17-D-00001

## Part 2 - Privacy & Records Office (PRO) Clauses

**PRIV 1.4: Separation Checklist for Contractor Employees:** Contractors shall enact a protocol to use a separation checklist before its employees, Subcontractor employees, or independent Contractors terminate working on the contract. The separation checklist must cover areas such as: (1) return of any Government-furnished equipment; (2) return or proper disposal of Sensitive PII (paper or electronic) in the custody of the Contractor/Subcontractor employee or independent Contractor, including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to Sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee, Subcontractor employee, or independent Contractor, the Contractor shall notify the Contract Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.  
(End of clause)

**PRIV 1.7: Privacy Act Information:** In accordance with FAR 52.224-1, PRIVACY ACT NOTIFICATION (APR 1984), and FAR 52.224-2, PRIVACY ACT (APR 1984), this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974. The Agency advises that the relevant system of records notices (SORNs) applicable to this Privacy Act information are but not limited to:

- DHS/ICE 001- Student and Exchange Visitor Information System
- DHS/ICE 007-Alien Criminal Response Information Records (ACRIME)
- DHS/ICE 009 - External Investigations
- DHS/ICE 011 - Criminal Records, Arrest Records, and Immigration Enforcement Records (CARIER)
- DHS/ICE 015 – LeadTrac System
- DHS/CBP 006 – Automated Targeting System
- DHS/CBP 017 – Analytical Framework for Intelligence System

These SORNs may be updated at any time. The most current DHS versions are publicly available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy). SORNs of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System of the Government Publishing Office, available at <http://www.gpo.gov/fdsys/>.  
(End of clause)

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

**REC: 1.1: Required DHS Basic Records Management Training:** The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to Sensitive PII as well as the creation, use, dissemination and/or destruction of Sensitive PII at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site. The Agency may also make the training available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance. The Contractor must submit an annual e-mail notification to the Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.  
(End of clause)

**REC 1.2: Deliverables are the Property of the U.S. Government:** The Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable without the expressed permission of the Contracting Officer or Contracting Officer's Representative. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract. The Agency owns the rights to all data/records produced as part of this contract.  
(End of clause)

**REC 1.3: Contractor Shall Not Create or Maintain Unauthorized Records:** The Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records. The Contractor shall not create or maintain any records containing any Government Agency data that are not specifically tied to or authorized by the contract.  
(End of clause)

**REC 1.4: Agency Owns Rights to Electronic Information:** The Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation created as part of this contract. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the Agency to use the data.  
(End of clause)

***CLARIFICATION FROM GIANT OAK: Rec 1.2 and Rec 1.4 relate to the delivered data resulting from Giant Oak's technologies and not the Giant Oak owned software used to prepare deliverables and reports. Since Giant Oak is not contracted to develop nor deliver such software, all Giant Oak owned software, including but not limited to its Social Locator tool, shall remain the exclusive property of Giant Oak and the Government has no ownership***

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

***interest nor licensed rights in such software.***

**REC 1.5: Comply With All Records Management Policies:** The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(End of clause)

**REC 1.6: No Disposition of Documents without Prior Written Consent:** No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

(End of clause)

**REC 1.7: Contractor Must Obtain Approval Prior to Engaging Subcontractors:** The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(End of clause)

~~LAW ENFORCEMENT SENSITIVE INFORMATION~~

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

**Part 3 - Personnel Security Requirements**

**SECURITY REQUIREMENTS**

**GENERAL**

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the task as described in **HSCEMD-17-D-00001** requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) may access classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the *National Industrial Security Program Operating Manual (NISPOM)* for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at an ICE or other Government Facility, it will abide by the requirements set by the agency.

In conjunction with acquisition **HSCEMD-17-D-00001** the contractor shall ensure all investigative, reinvestigate, and adjudicative requirements are met in accordance with *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 2-1.

No person shall be allowed to begin work on contract **HSCEMD-17-D-00001** and/or access sensitive information related to the contract without ICE receiving clearance verification from the Facility Security Officer (FSO). ICE further retains the right to deem an applicant as ineligible due to an insufficient background investigation or when derogatory information is received and evaluated under a Continuous Evaluation Program. Any action taken by ICE does not relieve the Contractor from required reporting of derogatory information as outlined under the NISPOM.

The FSO will submit a Visitors Authorization Letter (VAL) through the Contracting Officer's Representative (COR) to (b)(6);(b)(7)(C) for processing personnel onto the contract. The clearance verification process will be provided to the COR during Post-Award. Note: *Interim TS is not accepted by DHS for access to Top Secret information. The contract employee will only have access to SECRET level information until DoD CAF has granted a full TS.*

For processing any personnel on a classified contract who will not require access to classified information see BACKGROUND INVESTIGATIONS (Process for personnel do not require access to classified information).

**ATTACHMENT A  
PERFORMANCE WORK STATEMENT (PWS)  
HSCEMD-17-D-00001**

**PRELIMINARY DETERMINATION**

ICE shall have and exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation.

ICE may, as it deems appropriate, authorize and make a favorable preliminary fitness to support decision based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment fitness determination or a full employment fitness determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment fitness determination or final fitness determination by the OPR-PSU.

**BACKGROUND INVESTIGATIONS (Process for personnel not requiring access to classified information):**

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the OPR-PSU. Prospective Contractor employees without adequate security clearances issued by DoD CAF whether a replacement, addition, subcontractor employee, or vendor employee, shall submit the following security vetting documentation to OPR-PSU, in coordination with the Contracting Officer Representative (COR), within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1. Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by applicant in their OPM e-QIP account.
2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by applicant in their OPM e-QIP account.
3. Two (2) SF 87 (Rev. March 2013) Fingerprint Cards. **(Two Original Cards sent via COR to OPR-PSU)**

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

4. Foreign National Relatives or Associates Statement. **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant’s OPM e-QIP account prior to electronic “Release” of data via on-line account)**
5. DHS 11000-9, “Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act” **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant’s OPM e-QIP account prior to electronic “Release” of data via on-line account)**
6. Optional Form 306 Declaration for Federal Employment **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant’s OPM e-QIP account prior to electronic “Release” of data via on-line account)**
7. Two additional documents may be applicable if applicant was born abroad and/or if work is in a Detention Environment. If applicable, additional form(s) and instructions will be provided to applicant.

If the contract authorizes positions which do not require access to classified information: In those instances where a Prospective Contractor employee will not require access to classified information, areas or classified systems the Vendor will add to and the COR will insure the following statement is added to the eQip Worksheet prior to submitting it to OPR PSU: “Employee will not require NSI Access to Classified Information or Classified Systems at any level”.

Required information for submission of security packet will be provided by OPR-PSU at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU as notified via the COR.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, ICE retains the right to deem an applicant as ineligible due to insufficient background information.

**EMPLOYMENT ELIGIBILITY**

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

The contractor will agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represent the best means currently available for employers to verify the work authorization of their employees.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

**CONTINUED ELIGIBILITY**

If a prospective employee is found to be ineligible for access to Government facilities or information, the COR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU will conduct reinvestigations every 5 years, or when derogatory information is received, to evaluate continued eligibility.

ICE reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

**REQUIRED REPORTS:**

The contractor/COR will notify OPR-PSU of all terminations / resignations, etc., within five days of occurrence. The Contractor will return any expired ICE issued identification cards/ credentials and building passes, or those of terminated employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR, referencing the pass or card number, name of individual to whom issued, the last



**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCEMD-17-D-00001

known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU through the COR as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation) . The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

The contractor is required to report certain events that have an impact on the status of the facility clearance (FCL) and/ or the status of the contract employee's personnel security clearance as outlined by *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 1-3, Reporting Requirements. Contractors shall establish internal procedures as are necessary to ensure that cleared personnel are aware of their responsibilities for reporting pertinent information to the FSO and other federal authorities as required.

CORs will submit reports to [psu-industrial-security@ice.dhs.gov](mailto:psu-industrial-security@ice.dhs.gov)

**SECURITY MANAGEMENT**

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

Contractors shall provide all employees supporting contract **HSCEMD-17-D-00001** proper initial and annual refresher security training and briefings commensurate with their clearance level, to include security awareness, defensive security briefings. (*National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 3-1. The contractor shall forward a roster of the completed training to the COR on a quarterly bases.

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

**INFORMATION TECHNOLOGY**

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data

**ATTACHMENT A**  
**PERFORMANCE WORK STATEMENT (PWS)**  
HSCMD-17-D-00001

as outlined in *DHS MD 140-01 - Information Technology Systems Security and DHS MD 4300 Sensitive Systems Policy*. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

**INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT**

In accordance with Chief Information Office requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractors, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

**From:** (b)(6);(b)(7)(C)  
**Sent:** 21 Feb 2018 14:06:10 +0000  
**To:** (b)(6);(b)(7)(C)  
**Subject:** VLVI language

- The Visa Lifecycle Initiative, which began as a pilot program in August 2016, tracks nonimmigrant visitors from the time they file a visa application to the time they depart from the United States, or until such time as they become an overstay or otherwise fail to comply with their terms of admission (i.e., become “out-of-status”). This initiative aims to allow ICE to continuously monitor, vet, and identify any derogatory information on foreign visitors that may arise during their period of admission into the United States, or until such person violates his/her visa status. In instances that any violators are identified, appropriate enforcement actions will be initiated. The initiative focuses on nonimmigrants seeking business/tourist (i.e., B1/B2) or student (i.e., F, J, and M) visas from Department of State (DOS) visa issuing posts (b)(7)(E). (b)(7)(E) CTCEU submits all subjects who have been issued a visa from selected issuing posts to the NCTC to conduct an automated vetting process.

(b)(6);(b)(7)(C)  
Section Chief  
Visa Security Coordination Center  
National Security Investigations Division  
Homeland Security Investigations  
Cell (b)(6);(b)(7)(C)  
Office (b)(6);(b)(7)(C)  
(b)(6);(b)(7)(C)

**From:** (b)(6);(b)(7)(C)  
**Sent:** 27 Mar 2018 17:43:29 +0000  
**To:** (b)(6);(b)(7)(C)  
**Subject:** RE: due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

Gracias.

(b)(6);(b)(7)(C)  
Section Chief  
Visa Security Coordination Center  
National Security Investigations Division  
Homeland Security Investigations  
Cell (b)(6);(b)(7)(C)  
Office (b)(6);(b)(7)(C)  
(b)(6);(b)(7)(C)

---

**From:** (b)(6);(b)(7)(C)  
**Sent:** Tuesday, March 27, 2018 1:28 PM  
**To:** (b)(6);(b)(7)(C)  
**Subject:** RE: due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

I attached a document done when GOST was first coming into the picture of Social Media vetting. The document is extensive but provides all the information on the basics of the GOST system. I think (b)(6);(b)(7)(C) sent the dossier on Social media vetting which probably combines the GOST tool along with the analytical side of vetting in a more informative and easy to read format.

(b)(6);(b)(7)(C), Program Manager  
Homeland Security Investigations  
Visa Security Coordination Center (VSCC)  
National Security Investigations Division  
(b)(6);(b)(7)(C)  
Office: (b)(6);(b)(7)(C)  
Cell: (b)(6);(b)(7)(C)

---

**From:** (b)(6);(b)(7)(C)  
**Sent:** Tuesday, March 27, 2018 12:57 PM  
**To:** (b)(6);(b)(7)(C)  
**Subject:** FW: due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

Gents, I'm putting together a reply to the tasking below and need some info asap please.

(b)(6);(b)(7)(C) – Do you have any talking points on what GOST is and how it works? Something that succinctly explains that (b)(5)  
(b)(5)

(b)(6);(b)(7)(C) – Can you send me the most current version of the social media dossier that you’ve been working on?

Thanks,

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Section Chief  
Visa Security Coordination Center  
National Security Investigations Division  
Homeland Security Investigations  
Cell (b)(6);(b)(7)(C)  
Office (b)(6);(b)(7)(C)  
(b)(6);(b)(7)(C)

**From:** NSID Tasking

**Sent:** Tuesday, March 27, 2018 12:46 PM

**To:** (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

**Cc:** (b)(6);(b)(7)(C)

**Subject:** due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

Afternoon everyone,

**Request:** DD is interested in accurate information on how both ERO and HSI use Facebook data. **Please describe your unit’s current use of Facebook, and/or provide any context on current use/parameters or other clarifying factors.** (full background below)

Please send your responses to Tom and I by **4:00PM today**. **\*Negative responses required\***

Thank you,

(b)(6);(b)(7)(C) | *Program Manager/SADAD*

DHS – ICE | Homeland Security Investigations | NSID

(b)(6);(b)(7)(C) (HSDN/SIPR) CIWells@dhs.ic.gov (C-LAN/JWICS)

(b)(6);(b)(7)(C) | (b)(6);(b)(7)(C)



**Homeland Security**

**From:** (b)(6);(b)(7)(C)

**Sent:** Tuesday, March 27, 2018 11:49 AM

**To:** NSID Tasking; (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Cc: (b)(6);(b)(7)(C)

**Subject:** TASKING REQUEST - HSI NSID USE OF FACEBOOK

Good morning Taskings/Units:

**Request:** DD is interested to get accurate information on how both ERO and HSI use Facebook data. **Please describe your unit's current use of facebook, and/or provide any context on current use/parameters or other clarifying factors.**

Background:

- HSI is pulling together a briefing paper to describe how we utilize facebook data.: Input can be sent in brief paragraphs as this will be consolidated in short briefing paper with other HSI input (C2 and D23).
- Please review the article below for context. For instance, the story talks about use of backend data from facebook; it also mentions use of facebook page picture), and a request for proposal for a private contractor.

**Due:** If possible, please provide by **COB today**, or advise if an extension until tomorrow is needed.

*Please coordinate final submissions through the taskings team at Tysons.*

Thank you

(b)(6);(b)(7)(C)

**From:** Blank, Thomas <[Thomas.Blank@ice.dhs.gov](mailto:Thomas.Blank@ice.dhs.gov)>

**Date:** Tuesday, Mar 27, 2018, 8:38 AM

**To:** (b)(6);(b)(7)(C)

**Cc:** (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

**Subject:** Facebook

(b)(6);(b)(7)(C)

DD is interested to get accurate information on how both ERO and HSI use Facebook data. See the story below and we expect this could stay in the news given what is going on with Facebook right now.

Thanks,

(b)(6);(b)(7)(C)

**ICE USES FACEBOOK DATA IN TRACKING DOWN IMMIGRANTS.** According to a [report](#) (3/26, 100K) from The Intercept, ICE "uses Facebook data to aid in tracking down immigrants, including finding their cell phone numbers, ahead of its roundups," [Axios](#) (3/26, Kight, 1.31M) reports.

Citing the same Intercept piece, the [San Jose \(CA\) Mercury News](#) (3/26, Sanchez, 514K) reports ICE “used backend Facebook data to track down undocumented immigrants targeted for deportation,” adding that “documents and emails obtained by the publication through a public records request provided a rare glimpse into one of the tactics ICE used to monitor undocumented immigrants before rounding them up.” A spokesperson for Facebook said, “Facebook does not provide ICE or any other law enforcement agency with any special data access to assist with the enforcement of immigration law. We have strict processes in place to handle these government requests. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague demands for information.”

Thomas Blank  
Chief of Staff  
US Immigration and Customs Enforcement  
US Department of Homeland Security  
500 12th Street SW  
Washington, D.C. 20536  
Office (b)(6);(b)(7)(C)  
Cell (b)(6);(b)(7)(C)

**From:** (b)(6);(b)(7)(C)  
**Sent:** 27 Mar 2018 13:49:13 -0400  
**To:** (b)(6);(b)(7)(C)  
**Subject:** RE: due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Below is CTCEU's response to the tasking. Below that is my rough draft dossier write-up. (b)(6);(b)(7)(C) is going to send you specific GOST info.

(b)(5)

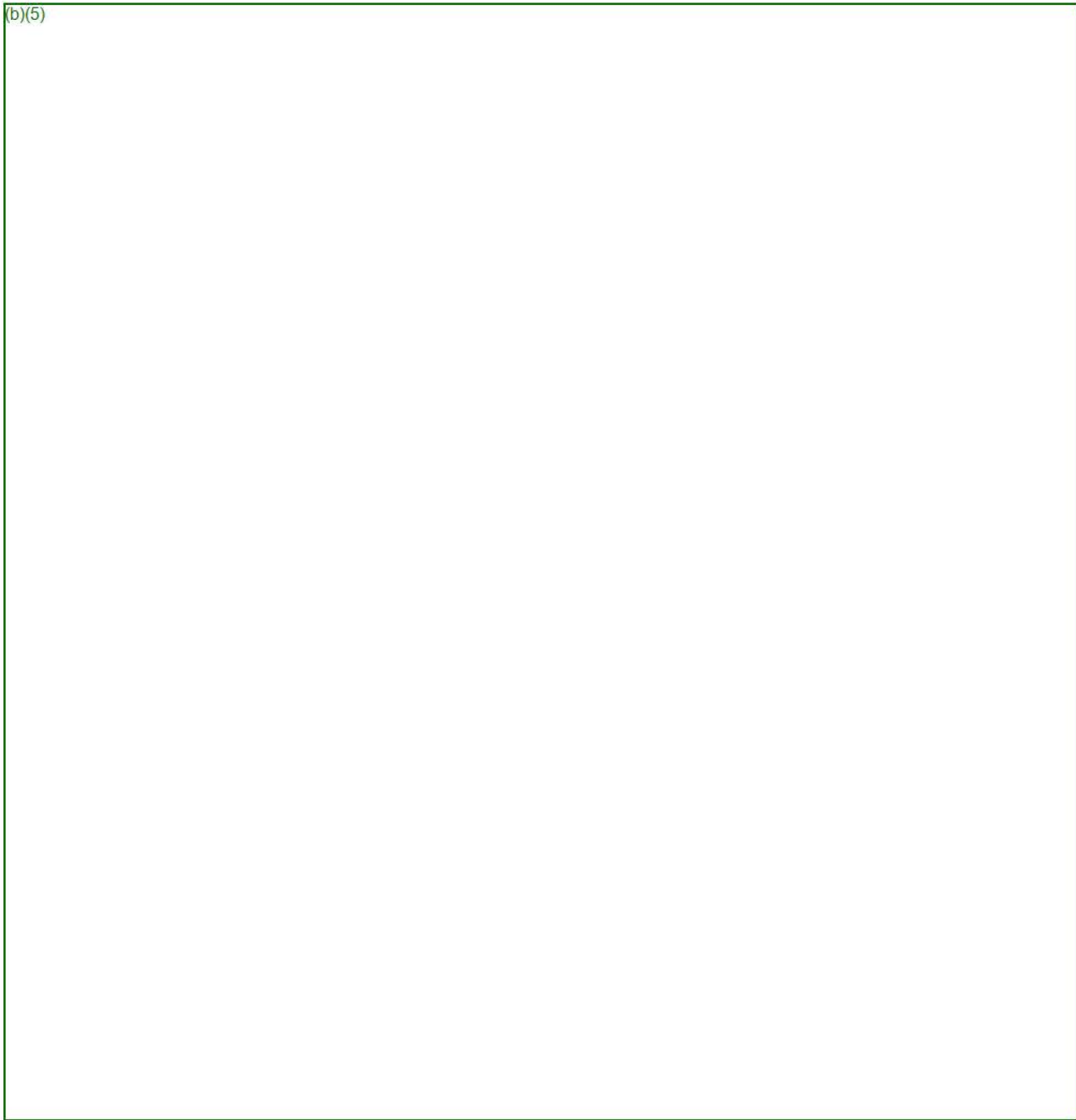
A large rectangular area of the document is completely redacted with a solid black fill. The text "(b)(5)" is visible in the top-left corner of this redacted area.

(b)(5)

A second large rectangular area of the document is completely redacted with a solid black fill. The text "(b)(5)" is visible in the top-left corner of this redacted area.



(b)(5)



v/r

(b)(6);(b)(7)(C) Program Manager/Special Agent

Homeland Security Investigations

Visa Security Coordination Center

National Security Investigations Division

Desk: (b)(6);(b)(7)(C) Mobile: (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)



~~CONFIDENTIALITY NOTICE: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.~~

**From:** (b)(6);(b)(7)(C)  
**Sent:** Tuesday, March 27, 2018 12:57 PM  
**To:** (b)(6);(b)(7)(C)  
**Subject:** FW: due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

Gents, I'm putting together a reply to the tasking below and need some info asap please.

(b)(6);(b)(7)(C) – Do you have any talking points on what GOST is and how it works? Something that succinctly explains that (b)(5)  
(b)(5)

(b)(6);(b)(7)(C) – Can you send me the most current version of the social media dossier that you've been working on?

Thanks,

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Section Chief  
Visa Security Coordination Center  
National Security Investigations Division  
Homeland Security Investigations  
Cell (b)(6);(b)(7)(C)  
Office (b)(6);(b)(7)(C)  
(b)(6);(b)(7)(C)

**From:** NSID Tasking  
**Sent:** Tuesday, March 27, 2018 12:46 PM  
**To:** (b)(6);(b)(7)(C)  
(b)(6);(b)(7)(C)  
**Cc:** (b)(6);(b)(7)(C)  
**Subject:** due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

Afternoon everyone,

**Request:** DD is interested in accurate information on how both ERO and HSI use Facebook data. **Please describe your unit's current use of Facebook, and/or provide any context on current use/parameters or other clarifying factors.** (full background below)

Please send your responses to Tom and I by **4:00PM today**. **\*Negative responses required\***

Thank you,

(b)(6);(b)(7)(C) Wells | Program Manager/SADAD  
 DHS – ICE | Homeland Security Investigations | NSID  
 (b)(6);(b)(7)(C) (HSDN/SIPR) (b)(6);(b)(7)(C) (C-LAN/JWICS)  
 (b)(6);(b)(7)(C)




---

**From:** (b)(6);(b)(7)(C)  
**Sent:** Tuesday, March 27, 2018 11:49 AM  
**To:** (b)(6);(b)(7)(C)  
 (b)(6);(b)(7)(C)  
**Cc:** (b)(6);(b)(7)(C)  
**Subject:** TASKING REQUEST - HSI NSID USE OF FACEBOOK

Good morning Taskings/Units:

**Request:** DD is interested to get accurate information on how both ERO and HSI use Facebook data. **Please describe your unit’s current use of facebook, and/or provide any context on current use/parameters or other clarifying factors.**

Background:

- HSI is pulling together a briefing paper to describe how we utilize facebook data.: Input can be sent in brief paragraphs as this will be consolidated in short briefing paper with other HSI input (C2 and D23).
- Please review the article below for context. For instance, the story talks about use of backend data from facebook; it also mentions use of facebook page picture), and a request for proposal for a private contractor.

**Due:** If possible, please provide by **COB today**, or advise if an extension until tomorrow is needed.

*Please coordinate final submissions through the taskings team at Tysons.*

Thank you

(b)(6);(b)(7)(C)

**From:** Blank, Thomas <[Thomas.Blank@ice.dhs.gov](mailto:Thomas.Blank@ice.dhs.gov)>  
**Date:** Tuesday, Mar 27, 2018, 8:38 AM  
**To:** (b)(6);(b)(7)(C)

Cc: (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Subject: Facebook

(b)(6);(b)(7)(C)

DD is interested to get accurate information on how both ERO and HSI use Facebook data. See the story below and we expect this could stay in the news given what is going on with Facebook right now.

Thanks,

(b)(6);(b)(7)(C)

**ICE USES FACEBOOK DATA IN TRACKING DOWN IMMIGRANTS.** According to a [report](#) (3/26, 100K) from The Intercept, ICE “uses Facebook data to aid in tracking down immigrants, including finding their cell phone numbers, ahead of its roundups,” [Axios](#) (3/26, Kight, 1.31M) reports.

Citing the same Intercept piece, the [San Jose \(CA\) Mercury News](#) (3/26, Sanchez, 514K) reports ICE “used backend Facebook data to track down undocumented immigrants targeted for deportation,” adding that “documents and emails obtained by the publication through a public records request provided a rare glimpse into one of the tactics ICE used to monitor undocumented immigrants before rounding them up.” A spokesperson for Facebook said, “Facebook does not provide ICE or any other law enforcement agency with any special data access to assist with the enforcement of immigration law. We have strict processes in place to handle these government requests. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague demands for information.”

Thomas Blank  
Chief of Staff  
US Immigration and Customs Enforcement  
US Department of Homeland Security  
500 12th Street SW  
Washington, D.C. 20536  
Office (b)(6);(b)(7)(C)  
Cell (b)(6);(b)(7)(C)

---

**From:** (b)(6);(b)(7)(C)  
**Sent:** 27 Mar 2018 20:35:33 +0000  
**To:** NSID Tasking  
**Cc:** (b)(6);(b)(7)(C)  
**Subject:** RE: due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK

Good Afternoon,

Please see response below from VSCC:

The National Security Investigations Division (NSID) Visa Security Coordination Center (VSCC), in collaboration with the Counter-Terrorism and Criminal Exploitation Unit (CTCEU), implements a social media pilot program designed to track visa applicants from the time they file a visa application with the Department of State, to the time they enter the United States, and through such time they either depart the United States, become an overstay, or otherwise fail to comply with their terms of admission. As part of the program, visa applicants from five visa issuance posts (b)(7)(E)

(b)(7)(E) are screened by VSCC analysts utilizing the Giant Oak Search Technology (GOST) open source and social media tool. This process utilizes open source and publicly available information on the internet including social media websites (Facebook being one of them), media, blogs, academic websites, etc. to screen and vet visa applicants, and assists the VSCC in efforts to identify potentially derogatory online activity of applicants prior to issuance of the visa and entrance into the United States. It leverages social media, open source information, and analytic capabilities as a tool to provide enhanced knowledge about applicants' public facing social media postings and online presence not found in U.S. Government holdings. Social media and public source screening gives the U.S. Government better visibility regarding an applicant's possible engagement in criminal activity, terrorist acts or associations, and administrative immigration violations, and complements the Visa Security Program (VSP) Pre-Adjudication Threat Recognition Intelligence Operations Team (PATRIOT) process. All results returned through the search of public source and social media sites, including Facebook, is publicly available to anyone searching the internet. No backend data is obtained through the GOST tool.

Thanks,

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)  
Section Chief  
Visa Security Coordination Center  
National Security Investigations Division  
Homeland Security Investigations  
Cell (b)(6);(b)(7)(C)  
Office (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

---

**From:** NSID Tasking  
**Sent:** Tuesday, March 27, 2018 12:46 PM  
**To:** (b)(6);(b)(7)(C)  
**Amy;** (b)(6);(b)(7)(C)  
 (b)(6);(b)(7)(C)  
 (b)(6);(b)(7)(C)  
**CC:** (b)(6);(b)(7)(C)  
**Subject:** due today at 4PM FW: TASKING REQUEST - HSI NSID USE OF FACEBOOK


Afternoon everyone,

**Request:** DD is interested in accurate information on how both ERO and HSI use Facebook data. **Please describe your unit’s current use of Facebook, and/or provide any context on current use/parameters or other clarifying factors.** (full background below)

Please send your responses to Tom and I by **4:00PM today**. **\*Negative responses required\***

Thank you,

SA (b)(6);(b)(7)(C) | *Program Manager/SADAD*  
 DHS – ICE | Homeland Security Investigations | NSID  
 (b)(6);(b)(7)(C) | HSDN/SIPR | CIWells@dhs.ic.gov (C-LAN/JWICS)  
 (b)(6);(b)(7)(C) | (b)(6);(b)(7)(C)




---

**From:** (b)(6);(b)(7)(C)  
**Sent:** Tuesday, March 27, 2018 11:49 AM  
**To:** NSID Tasking; (b)(6);(b)(7)(C)  
 (b)(6);(b)(7)(C)  
**Cc:** (b)(6);(b)(7)(C)  
**Subject:** TASKING REQUEST - HSI NSID USE OF FACEBOOK

Good morning Taskings/Units:

**Request:** DD is interested to get accurate information on how both ERO and HSI use Facebook data. **Please describe your unit’s current use of facebook, and/or provide any context on current use/parameters or other clarifying factors.**

Background:

- HSI is pulling together a briefing paper to describe how we utilize facebook data.: Input can be sent in brief paragraphs as this will be consolidated in short briefing paper with other HSI input (C2 and D23).

- Please review the article below for context. For instance, the story talks about use of backend data from facebook; it also mentions use of facebook page picture), and a request for proposal for a private contractor.

**Due:** If possible, please provide by **COB today**, or advise if an extension until tomorrow is needed.

*Please coordinate final submissions through the taskings team at Tysons.*

Thank you

(b)(6);(b)(7)(C)

**From:** (b)(6);(b)(7)(C)

**Date:** Tuesday, Mar 27, 2018, 8:38 AM

**To:** (b)(6);(b)(7)(C)

**Cc:** (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

**Subject:** Facebook

(b)(6);(b)(7)(C)

DD is interested to get accurate information on how both ERO and HSI use Facebook data. See the story below and we expect this could stay in the news given what is going on with Facebook right now.

Thanks,

(b)(6);(b)(7)(C)

**ICE USES FACEBOOK DATA IN TRACKING DOWN IMMIGRANTS.** According to a [report](#) (3/26, 100K) from The Intercept, ICE “uses Facebook data to aid in tracking down immigrants, including finding their cell phone numbers, ahead of its roundups,” [Axios](#) (3/26, Kight, 1.31M) reports.

Citing the same Intercept piece, the [San Jose \(CA\) Mercury News](#) (3/26, Sanchez, 514K) reports ICE “used backend Facebook data to track down undocumented immigrants targeted for deportation,” adding that “documents and emails obtained by the publication through a public records request provided a rare glimpse into one of the tactics ICE used to monitor undocumented immigrants before rounding them up.” A spokesperson for Facebook said, “Facebook does not provide ICE or any other law enforcement agency with any special data access to assist with the enforcement of immigration law. We have strict processes in place to handle these government requests. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague demands for information.”

Thomas Blank  
Chief of Staff  
US Immigration and Customs Enforcement

US Department of Homeland Security

500 12th Street SW

Washington, D.C. 20536

Office (b)(6);(b)(7)(C)

Cell (b)(6);(b)(7)(C)



Homeland Security Investigations  
National Security Investigations Division  
*Assistant Director*



**U.S. Immigration  
and Customs  
Enforcement**

---

## **Extreme Vetting-Visa Security Program-PATRIOT**

### **Overview**

The ICE Visa Security Program (VSP) is authorized by Section 428 of the Homeland Security Act of 2002 and implemented by a 2003 Memorandum of Understanding between the Secretaries of State and Homeland Security. International Operations for the VSP assigns Special Agents to diplomatic posts worldwide to conduct law enforcement and visa security activities and to provide training and law enforcement expertise to Department of State (DOS) Consular Affairs (CA) offices regarding threats, trends and other topics affecting the visa adjudication process. VSP operations are currently conducted at 30 visa-issuing posts in 25 countries. Homeland Security Investigations VSP operations are supported through the Pre-Adjudication Threat Recognition and Intelligence Operations Team (PATRIOT), with domestic screening and vetting operations conducted within the National Capital Region. PATRIOT identifies national security, public safety, fraud, immigration, and other visa eligibility concerns at the earliest point of an individual's visa application life-cycle.

ICE/HSI proposes an initiative to meet executive mandates concerning future VSP Extreme Vetting capabilities, a comprehensive operational and programmatic expansion of PATRIOT to all 225 non-immigrant visa issuance posts worldwide:

### **Requirements**

- Domestic PATRIOT expansion to accommodate planned visa security program growth to all 225 visa-issuing posts.
- Increased exploitation of information through a vigorous information sharing initiative with interagency and intra-agency stakeholders.
- Comprehensive utilization of innovative big-data programs to enhance current vetting procedures and processes.
- Research and development of web-crawler/social media programs to enhance vetting capabilities
- Develop interagency agreements and policy standards for screening, vetting and information sharing
- Develop international agreements and policy standards for screening, vetting and information sharing

(b)(7)(E)

(b)(7)(E)

The Visa Lifecycle Pilot Program, part of NSID's social media expansion, continuously vets individuals who have been approved for a non-immigrant visa from select DOS visa issuing posts. Working in coordination with HSI's VSP, the Counterterrorism and Criminal Exploitation Unit (CTCEU) will receive information from VSP on these visa applicants pulled from PATRIOT and the DOS Consular Consolidated Database (CCD). The CTCEU will ingest this data into LeadTrac and continuously monitor these non-immigrant visa holders through the use of an automated social media vetting platform and high-side vetting throughout the lifecycle of the visa's validity.

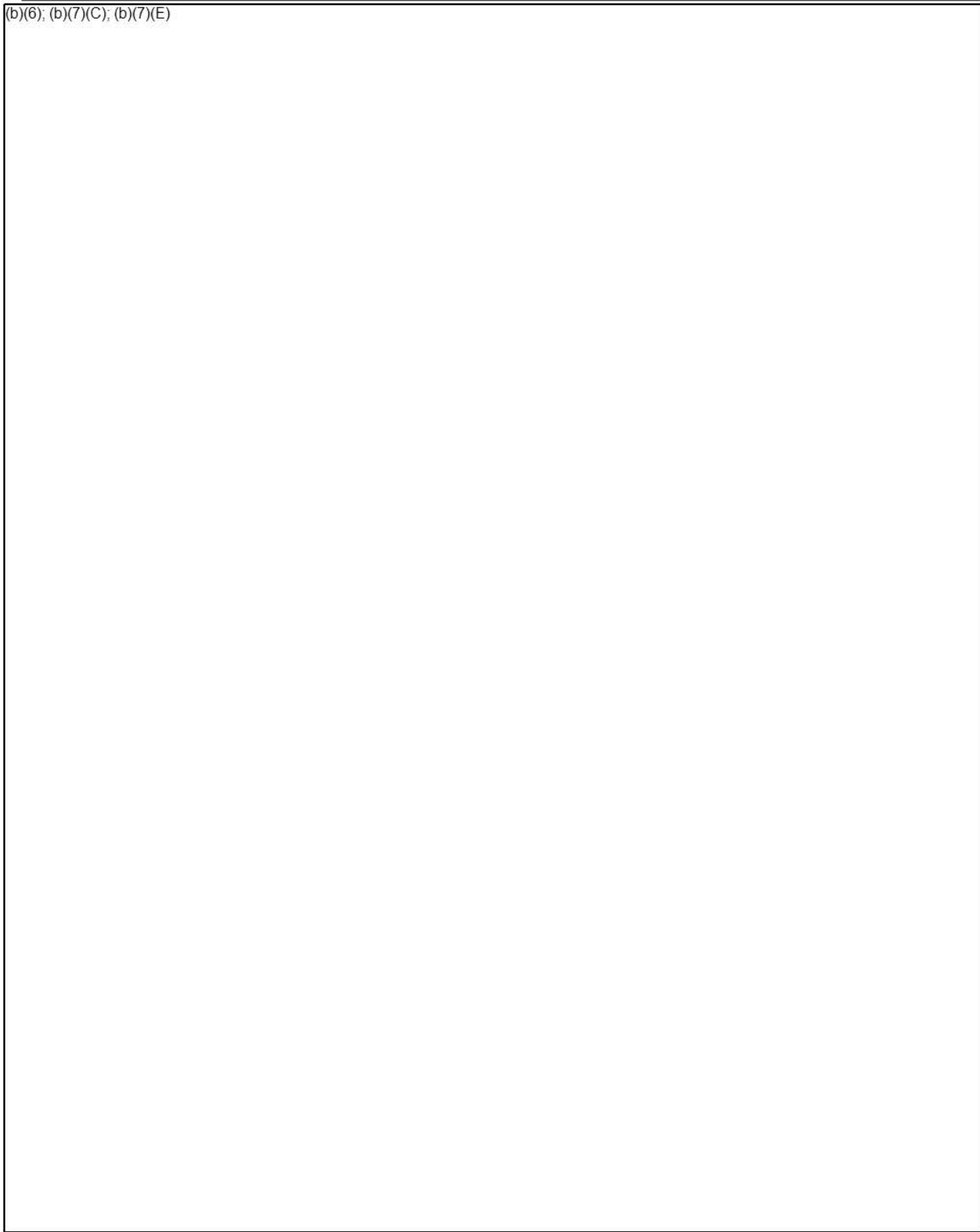
If the CTCEU uncovers derogatory information about a visa applicant, CTCEU analysts will manually work-up the lead. If it is determined that the individual has not yet entered the United States, the CTCEU will place a subject record in TECS/ICM to identify the individual for other government partners such as CBP, watchlist the individual if appropriate, notify the appropriate ICE Attaché Office, and notify DOS of the derogatory information so that DOS may revoke the visa if deemed appropriate. If the individual has entered the United States, CTCEU analysts will initiate a collateral investigative request which will be forwarded to the appropriate HSI field office for further investigation. The investigation at the field level will be coordinated through the Joint Terrorism Task Force (JTTF).

HOMELAND SECURITY INVESTIGATIONS  
*National Security Investigations*



Homeland  
Security

(b)(6); (b)(7)(C); (b)(7)(E)

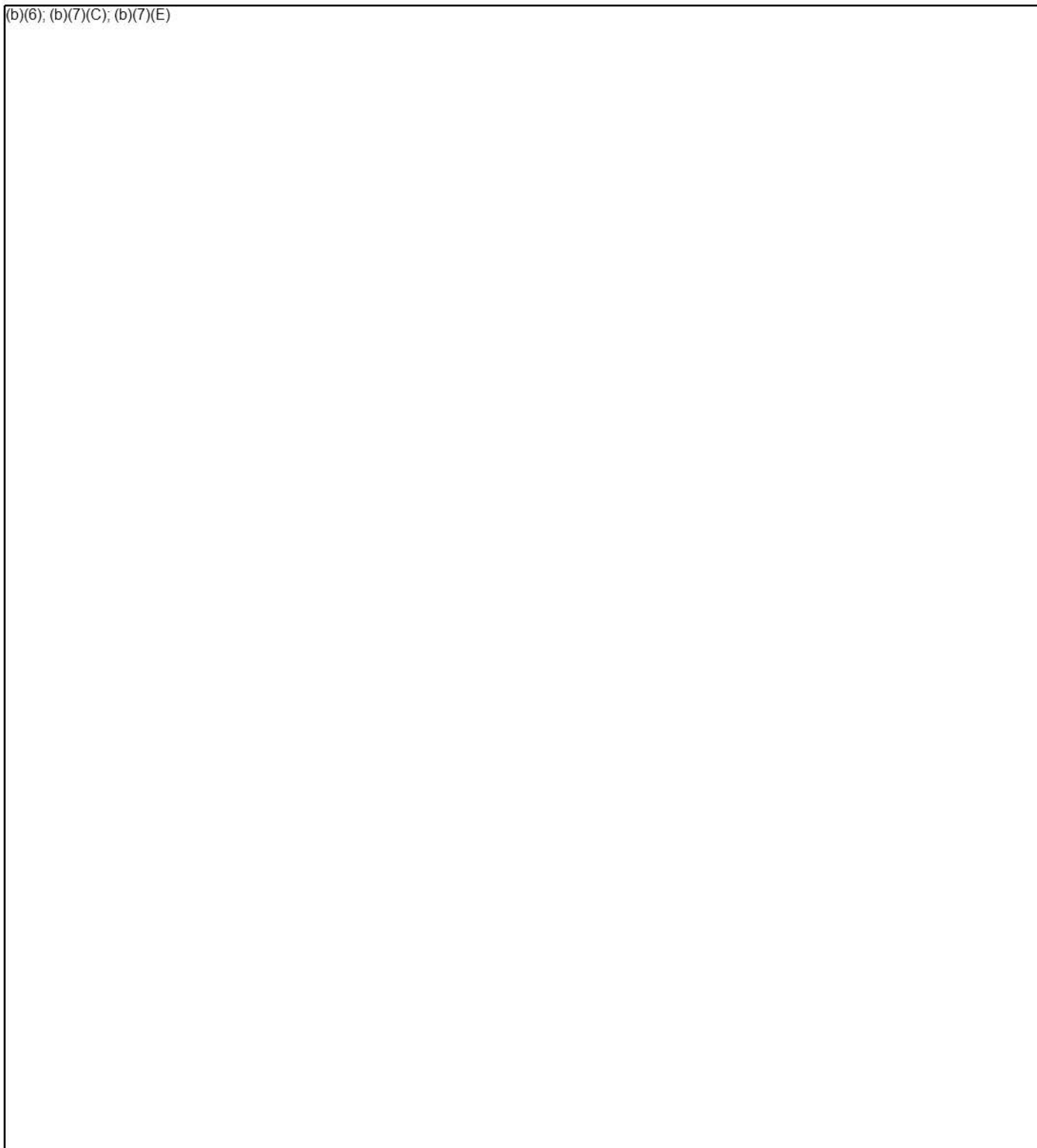


HOMELAND SECURITY INVESTIGATIONS  
*National Security Investigations*



Homeland  
Security

(b)(6); (b)(7)(C); (b)(7)(E)



**From:** (b)(6); (b)(7)(C)  
**Sent:** 2 Feb 2018 15:29:40 -0500  
**To:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** Companies for Market Research

(b)(6);  
(b)(7)(C)

From the 140 vendors which attended our Industry Days, the VLVI team met with 25 companies for individual one-on-one meetings. Of the 25 companies, the following nine are on the MOBIS PSS:

- CSRA
- Deloitte
- General Dynamics Information Technology
- Woolpert, Inc.
- Booz Allen Hamilton
- Ernst & Young
- Unisys Corporation
- Arc Aspicio, LLC
- Engility Corporation

We have decided that we will send solicitations to all nine of the above companies. If you could please add this to the Market Research Document it would be greatly appreciated. I believe that should be our final step with the MR.

Thanks,

(b)(6); (b)(7)(C)  
Intelligence Research Specialist  
Counterterrorism and Criminal Exploitation Unit  
ICE – Homeland Security Investigations  
Office: 703-235-(b)(6);  
Cell: 703-258-(b)(6);  
Email: (b)(6); (b)(7)(C)

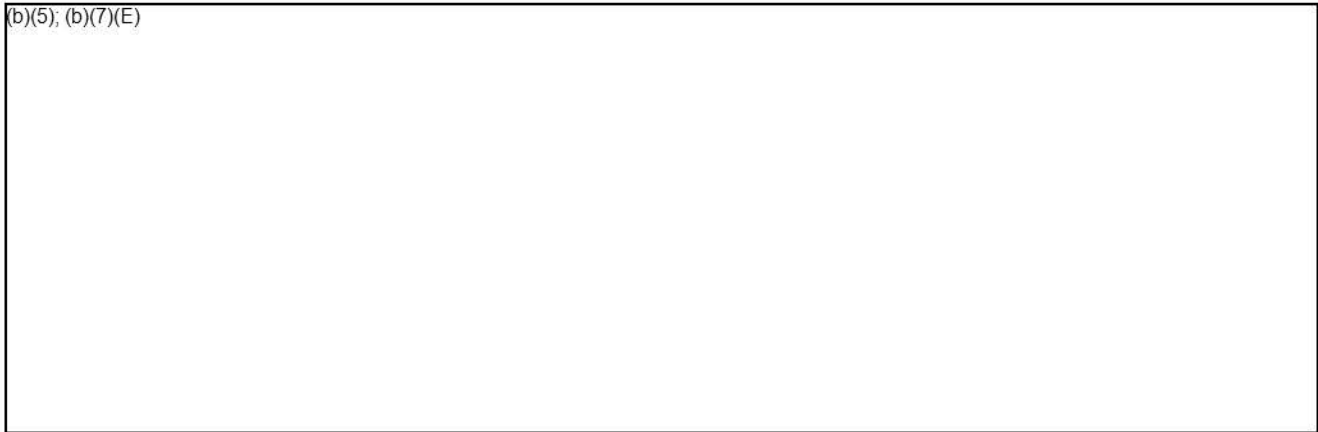
Homeland Security Investigations  
*National Security Investigations Division*



U.S. Immigration  
and Customs  
Enforcement

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



~~FOR OFFICIAL USE ONLY~~

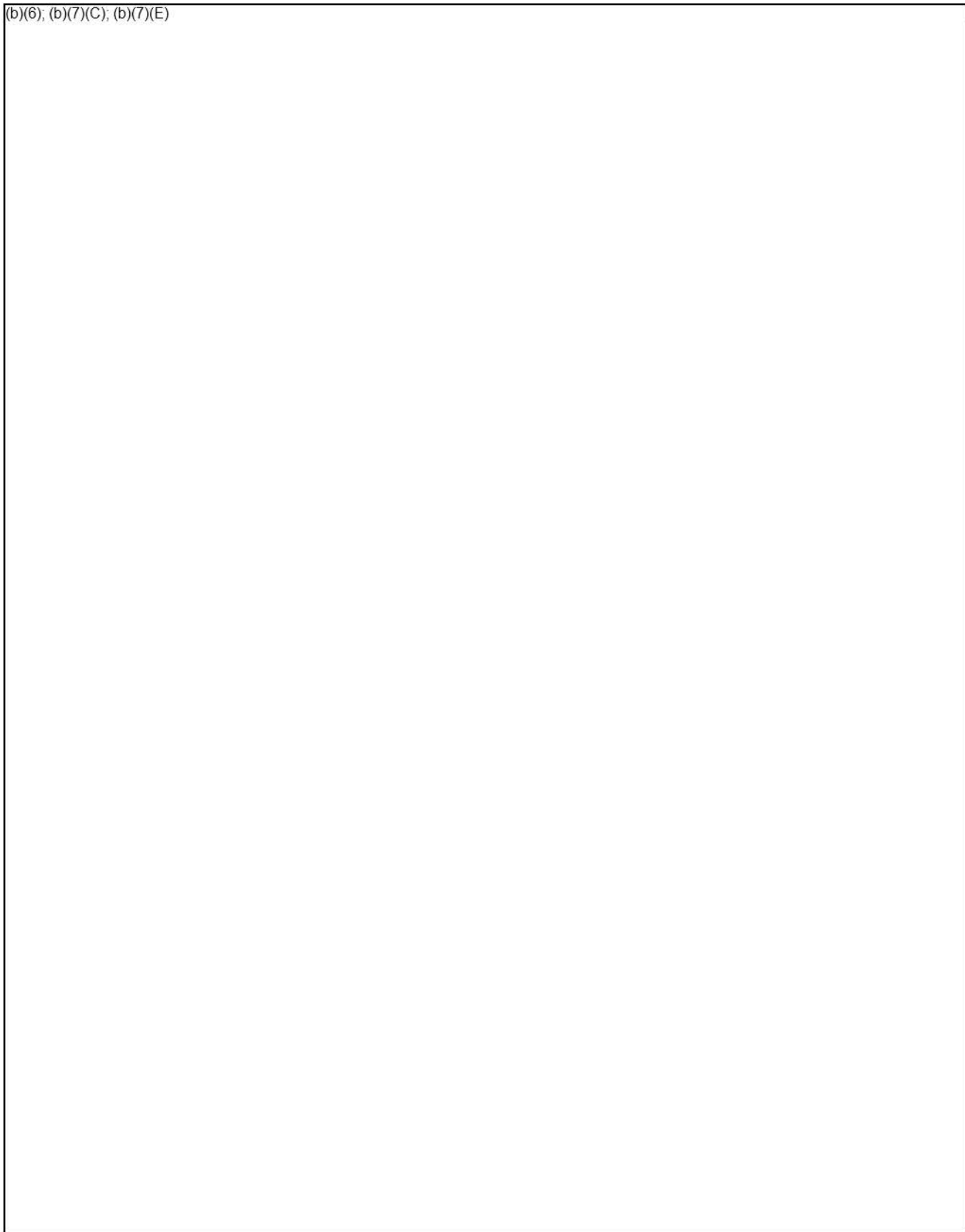


HOMELAND SECURITY INVESTIGATIONS  
*National Security Investigations*



Homeland  
Security

(b)(6); (b)(7)(C); (b)(7)(E)



HOMELAND SECURITY INVESTIGATIONS  
*National Security Investigations*



Homeland  
Security

(b)(6); (b)(7)(C); (b)(7)(E)

HOMELAND SECURITY INVESTIGATIONS  
*National Security Investigations*



Homeland  
Security

(b)(6); (b)(7)(C); (b)(7)(E)

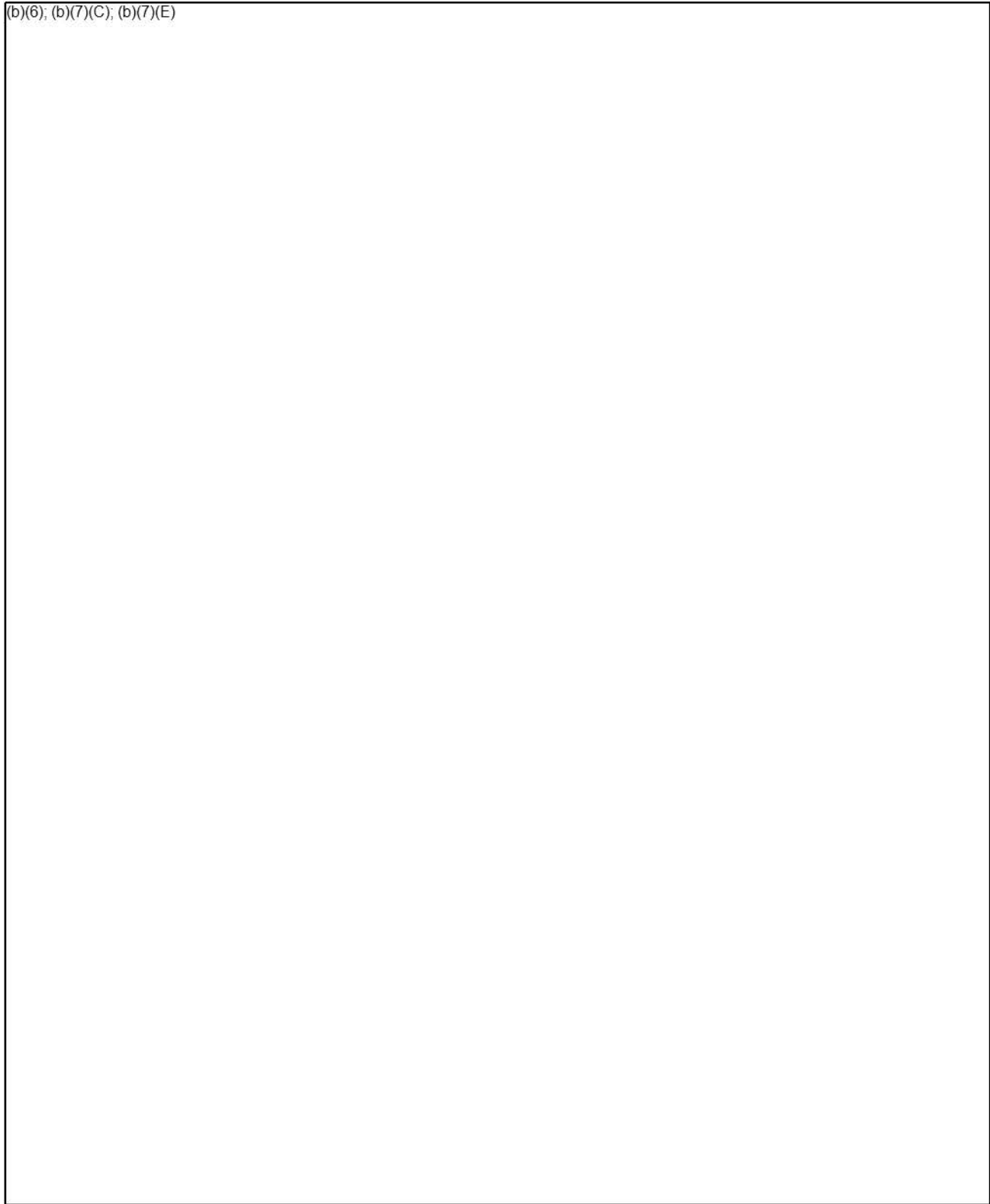
Homeland Security Investigations  
*National Security Investigations Division*



U.S. Immigration  
and Customs  
Enforcement

(b)(7)(E)

(b)(6); (b)(7)(C); (b)(7)(E)



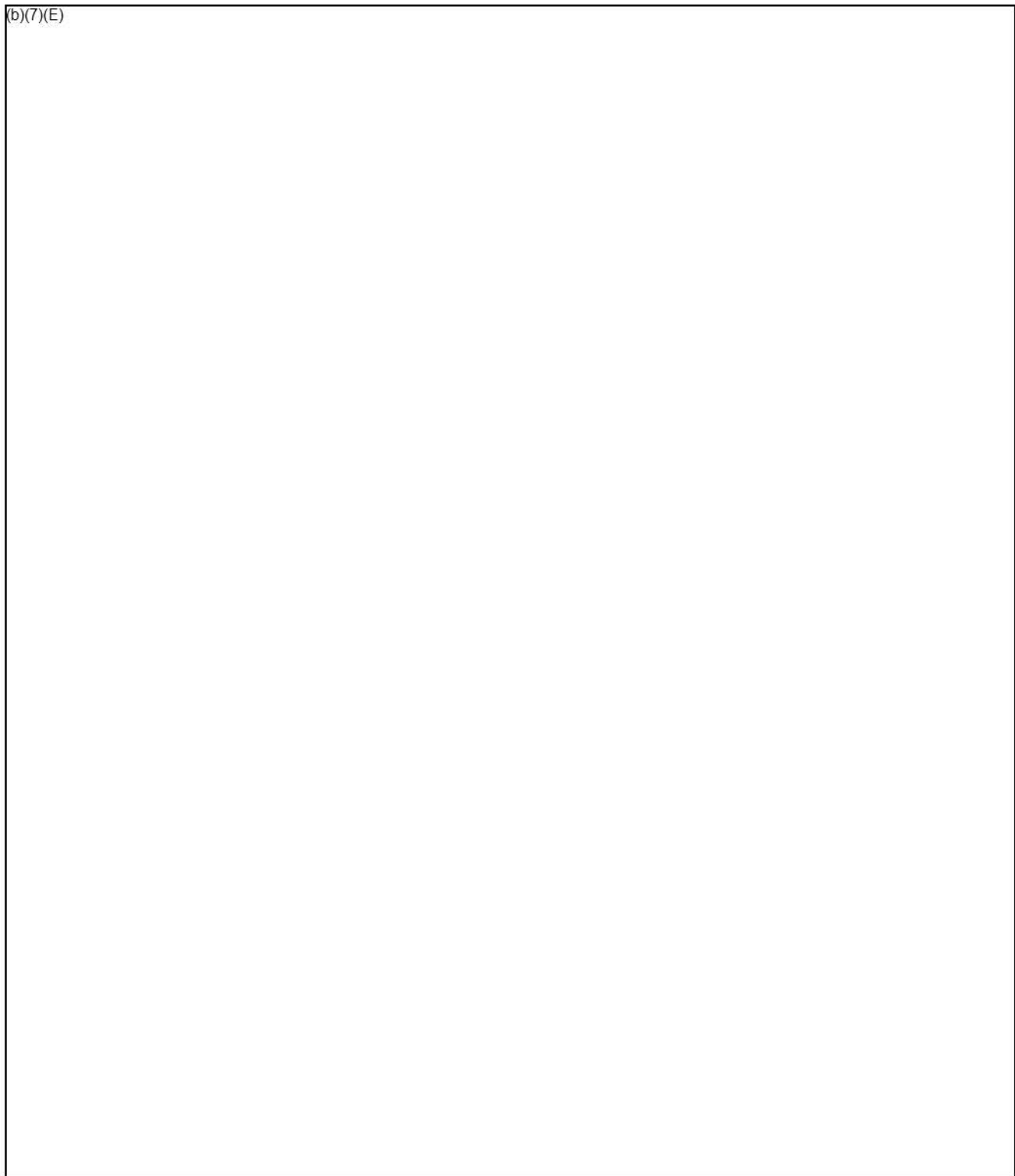
~~FOR OFFICIAL USE ONLY~~

Homeland Security Investigations  
National Security Investigations Division  
*Assistant Director*

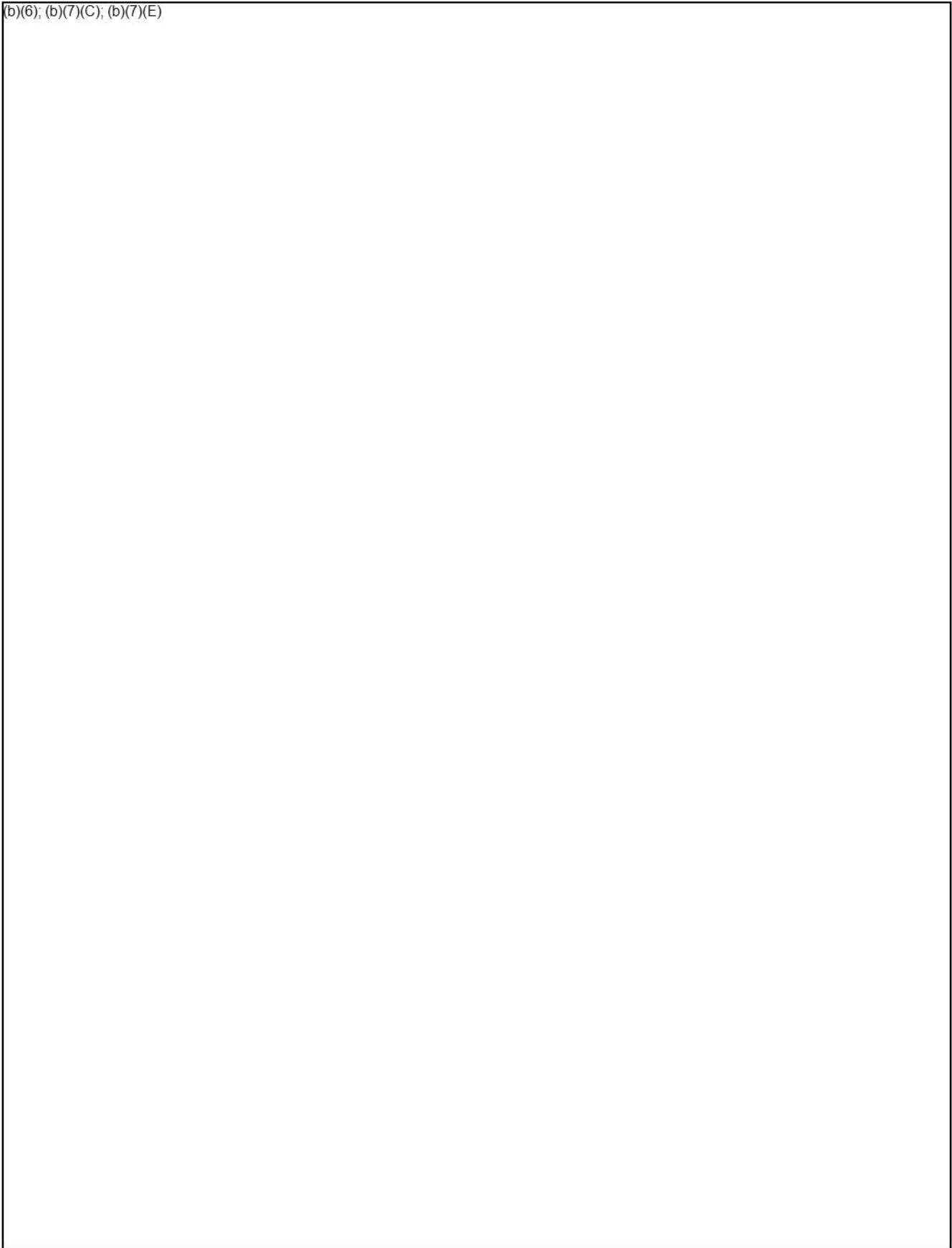


U.S. Immigration  
and Customs  
Enforcement

(b)(7)(E)



(b)(6); (b)(7)(C); (b)(7)(E)



(b)(7)(E)



~~FOR OFFICIAL USE ONLY~~



(b)(7)(E)



~~FOR OFFICIAL USE ONLY~~