☐ Congressional ☐ DHS ☐ Routine
☐ FYI ☐ Sig. Pkg.

U.S. Customs and Border Protection

Document Routing Form

Date: 4/16/12

FROM			
Writer's Name (b)(6);(b)(7)(C)	Office	Office Of Executive Secretariat Staff Tracking No.	
Telephone No. (b)(6);(b)(7)(C)	Room No.	Subject: Arizona Technology Plan Comments	

Destination	Initials	Date	Comments - Commissioner's Staff Only
Commissioner			
Deputy Commissioner			
Chief of Staff			
Deputy Chief of Staff			
Counselor			
OES Director			
OES Correspondence Manager			
OES Writer-Editor/Manager			

To	Destination	Initials/Date
Office of Air and Marine		
	Asst. Commissioner	
Office of Border Patrol	(b)(6);(b)(7)(C)	
1	Chief	
Office of Chief Counsel		
Office of Congressional Affairs		
	Asst. Commissioner	
Office of Diversity & Civil Rights		
	Exec. Director	
Office of Field Operations		
	Asst. Commissioner	
	DAC	
	COS	
	CMO	
Office of Administration		
	Asst. Commissioner	
	CFO	

To	Destination	Initials/Date
Office of Human Resources Management		
	Asst. Commissioner	
Office of Information & Technology		
	Asst. Commissioner	
Office of Intelligence & Operations Coordination		
	Asst. Commissioner	
Office of Internal Affairs		
	Asst. Commissioner	
Office of International Affairs		
	Asst. Commissioner	
Office of International Trade		
	Asst. Commissioner	

To	Destination	Initials/Date
Office of Policy and Planning		
	Exec. Director	
Office of Public Affairs		
	Asst. Commissioner	
Office of Technology Innovation and Acquisition		
	Asst. Commissioner	
Office of State, and Local, and Tribal Liaison		
	Director	
Office of Training & Development		
	Asst. Commissioner	
Office of Trade Relations		
	Director	

Office Comments

CONTACT (b)(6);(b)(7)(C) (OTIA) FOR PICKUP.

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

OTIA 2012216

Arizona Technology Plan Concept of Operations (CONOPS)
Operational Requirements Management Branch (ORMB)/SPPA
May 21th, 2012

How was this document created?

- This document was drafted by OTIA. However, the CONOPS was a lengthy effort dating back to March 2011 requirements workshops. ORMB invested heavy man hours in the numerous reviews of this document.
- Because the majority of the focus was on the Arizona Technology Plan Operational Requirement (ORDs) the CONOPS, equally important, had a small support staff – 1 OTIA representative and 1 ORMB agent supporting the entire effort.

What is the purpose of the Arizona Border Surveillance Technology Plan CONOPS?

- The CONOPS ties in all the specific capabilities of the Arizona Technology Plan and describes them, conceptually, with current operational capabilities in Arizona.

- "This document defines the overarching concept of operations (CONOPS) for a risk-based approach to border security that leverages a combination of surveillance systems according to local operational needs and constraints." – Per ABSTP CONOPS

(b) (7)(E)

[redacted]

U.S. Customs and Border Protection

ARIZONA BORDER SURVEILLANCE TECHNOLOGY PLAN

CONCEPT OF OPERATIONS DOCUMENT FOR UNITED STATES BORDER PATROL

DOCUMENT NO: OTIA05-ATP-00-000001

Initial Release, 12 March 2012

DEVELOPED BY:

OPERATIONAL INTEGRATION AND ANALYSIS DIRECTORATE (OIAD)
OFFICE OF TECHNOLOGY INNOVATION & ACQUISITION (OTIA)

~~FOR OFFICIAL USE ONLY~~

~~This document was prepared for authorized distribution only. Information contained herein is exempt from public disclosure under United States Code (USC) subsection (b), 5 USC 552. It has not been approved for public release.~~

STAKEHOLDER SIGNATURE PAGE

Submitted by: (b)(6);(b)(7)(C) 3/12/2012
Date
Executive Director (Acting), Operational Integration and Analysis Directorate

Endorsed by: (b)(6);(b)(7)(C) 3/14/2012
(b)(6);(b)(7)(C) United States Coast Guard Date
Program Manager, Integrated Fixed Towers

Endorsed by: (b)(6);(b)(7)(C) 3/15/2012
Date
Portfolio Manager, Mobile and Agent Centric Systems

Endorsed by: (b)(6);(b)(7)(C) 3/19/2012
Date
(b)(6);(b)(7)(C) urveillance System

Approved by: 7 JUNE 2012
Date
Chief, United States Border Patrol

TABLE OF CONTENTS

EXECUTIVE SUMMARY **5**
REVISION HISTORY **6**
1 INTRODUCTION **7**
1.1 PURPOSE 7
1.2 BACKGROUND 8
2 CAPABILITY NEED **8**
2.1 REQUIRED MISSIONS AND NEED 8
2.2 CAPABILITY GAPS 11
3 OPERATIONS AND SUPPORT DESCRIPTIONS **13**
3.1 MISSIONS 13
3.2 USERS AND OTHER STAKEHOLDERS 14
3.3 POLICIES, ASSUMPTIONS AND CONSTRAINTS 16
3.4 OPERATIONAL DESCRIPTION 20
3.5 MISSION SUPPORT DESCRIPTION 31
3.6 POTENTIAL IMPACTS 32
4 SCENARIOS **38**
4.1 MISSION OPERATIONS SCENARIOS 38
4.2 MISSION SUPPORT SCENARIOS 42
5 FUNCTIONAL CAPABILITIES **43**
5.1 MISSION OPERATIONS FUNCTIONAL CAPABILITIES 43
5.2 MISSION SUPPORT FUNCTIONAL CAPABILITIES 45
APPENDIX 1: TABLE OF CHANGES **47**
APPENDIX 2: REFERENCES **48**
APPENDIX 3: GLOSSARY OF TERMS **49**
APPENDIX 4: LIST OF ACRONYMS **51**
APPENDIX 5: EXTERNAL STAKEHOLDERS **53**
APPENDIX 6: SURVEILLANCE SYSTEM DESCRIPTIONS **54**

LIST OF TABLES

Table 2-1: CBP Mission Elements....9
Table 2-2: Capability Gap Summary....13
Table 3-1: CBP Personnel / Users....15
Table 3-2: System Surveillance Employment Summary....22
Table 3-3: Scheduling and Operations Planning....25
Table 3-4: Terrain Descriptions....26
Table A-1: Government Documents....47
Table A-2: Government Documents....48
Table A-3: Glossary of Terms....49
Table A-4: External Stakeholders....53

LIST OF FIGURES

Figure 3-1: Map of Federally Protected Lands in Southern Arizona....19
Figure 3-2: Operating Concept – Arizona Border Surveillance Deployment Plan....21
Figure 3-3: Surveillance Coverage Terminology....22
Figure 3-4: Surveillance System Interoperability (Current State)....29
Figure 3-5: Surveillance System Interoperability (Desired State)....30

EXECUTIVE SUMMARY

The October 2006 Secure Border Initiative (SBI) Mission Need Statement (MNS) identified a number of surveillance capability gaps that impact the United States Border Patrol's (USBP) ability to execute its mission. To address those capability gaps, the 2010 Arizona Border Surveillance Technology Plan (ATP) specifies a combination of agent-centric, aviation-centric, mobile ground, and fixed ground surveillance systems to be deployed along the Arizona border. Execution of the ATP will provide enhanced situational awareness, a more effective balance between cost and capability tailored to each area of the border, and rapid deployment of proven technology.

This document defines the overarching concept of operations (CONOPS) for a risk-based approach to border security that leverages a combination of surveillance systems according to local operational needs and constraints. This document compliments the system-specific CONOPS provided in each individual Operational Requirements Document by illustrating how the unique surveillance capabilities of each system are used together to enhance overall situational awareness along the border. This document also provides insight into the operational context, constraints, and expected outcomes for this enhanced surveillance capability.

The document is organized as follows:

- Section 1, Introduction: Discusses the basis for and the scope of the document.
- Section 2, Capability Need: Describes the mission need and details the capability gaps in terms of operational impact.
- Section 3, Operations and Support Description: Describes the stakeholders, constraints, scheduling and planning, interoperability needs, and how the proposed systems operate and interact. This section also discusses potential impacts to doctrine, organization, training, additional materiel needs, leadership, personnel, facilities, and the mission.
- Section 4, Scenarios: Provides operational examples that illustrate how the proposed functional capabilities are used in support of the mission and within the intended environment.
- Section 5, Functional Capabilities: Describes the key functional capabilities required to execute the ground surveillance mission which include: operations planning, relocating surveillance systems, detecting, tracking, identifying and classifying items of interest (IoI), planning responses, interdicting, communicating securely, collecting and reporting data, and analyzing trends. The operational requirements for each system further describe and quantify these functional capabilities.

To execute the ATP and address critical surveillance gaps within the targeted timelines, the acquisition strategy for the surveillance capabilities described herein will leverage existing non-developmental items (NDI), Government Off-the-Shelf (GOTS), or Commercial Off-the-Shelf (COTS) systems. As independent, stand-alone systems, each will contribute to situational awareness in the areas they are assigned to cover; this information will then be fused at the operational level by the operators. As USBP gains additional experience with these surveillance systems and the interoperability requirements are further refined, the CONOPS will be updated accordingly.

REVISION HISTORY

REV	DATE	DESCRIPTION
1	3/12/12	Initial Release

1 INTRODUCTION

The Department of Homeland Security (DHS) is charged with managing, securing, and controlling the Nation's borders with a priority mission focus of preventing terrorists and terrorist weapons from entering the United States (U.S.). U.S. Customs and Border Protection (CBP), an operational component of DHS, represents the front line in the security of our Nation's borders. CBP's activities are organized into three mission sets: (1) Securing America's Borders; (2) Securing and Expediting the Movement of People and the Flow of Goods; and (3) Sustaining Investment in its People and Capabilities.[1] The USBP, an operational component of CBP, is tasked with securing the Nation's borders against the illegal entry of people and goods between Ports of Entry (POE), and in particular, executing CBP's Goal 1.1: Secure the Southwest Border.[2] To accomplish this, USBP predicts illicit activity, detects and tracks illegal border crossings, identifies and classifies the incursions, and responds to and resolves those incursions using a risk-based approach to counter an evolving threat. USBP leverages surveillance capabilities to enable these mission tasks, increase situational awareness, and improve threat mitigation, and must do so in a cost-effective and efficient manner.

1.1 PURPOSE

This document describes the CONOPS for efforts to expand USBP's surveillance capabilities in accordance with the ATP. This document describes the current capability gaps and the CONOPS for additional surveillance capabilities achieved through the deployment of proven technology solutions tailored to the unique operational constraints along the border. This document also describes any operational and supportability impacts that may result from the implementation of these solutions. All of the surveillance solutions outlined in the ATP, with the exception of [redacted] (b) (7)(E) [redacted][3], are already employed by USBP – some to a greater extent than others. However, the CONOPS for a multi-layered, risk-based surveillance defense tailored to local operational needs has not been formally documented and is therefore done so herein. This document also describes the stakeholders, constraints, interoperability needs, and potential impacts of the ATP. As with all CONOPS, this is a living document intended to be periodically updated as the threat and/or CONOPS evolve.

The scope of this document is limited to USBP ground surveillance and does not address the surveillance of subterranean, air, or maritime/coastal incursions. Air and maritime/coastal incursions handled by CBP's Office of Air and Marine (OAM) are addressed elsewhere. The scope of this CONOPS document is also currently limited to the employment of these systems along the Arizona Border, and does not include the remainder of the southern, northern, or coastal borders at this time.

[1] CBP's Missions, Goals, and Priorities, FY2011-2013
[2] Ibid
[3] [redacted] (b) (7)(E) [redacted] have been deployed to the southern border for an operational utility evaluation.

1.2 BACKGROUND

In 2005, CBP established the SBI, a comprehensive, multi-year plan to help secure America's borders, and documented critical capability gaps in the 2006 SBI MNS. Since that time, CBP and USBP have refined the technology deployment plan for managing the border through the October 29, 2010 "Report on the Comprehensive, Science-Based Re-Assessment of the Secure Border Initiative-Network Program." This report documents CBP's reassessment of the overall surveillance technology approach through a DHS-requested analysis of alternatives (AoA).[4] The first phase (Phase 1A) of the AoA assessed solution alternatives to be deployed in key focus areas in Arizona according to the specifics of a given area, such as terrain, topology, population, and local enforcement tactics. The Phase 1A AoA also considered each alternative in terms of cost-effectiveness. The four technology alternatives are described in greater detail in Appendix 6 and include the following:

- Agent-centric systems (i.e. hand held systems)
- Mobile systems (i.e. stand-alone, transportable systems that can be redeployed)
- Fixed, integrated systems (i.e. a series of networked sensors with centralized, integrated control centers)
- Aviation-centric systems (i.e. aircraft equipped with surveillance systems)

After completion of the Phase I AoA, USBP used the results to develop a detailed surveillance technology deployment plan for the Arizona focus areas documented in the ATP. The ATP is a major change in direction compared to SBI*net*. Where SBI*net* represented an attempt to develop a system that would meet ambitious requirements, including a requirement for comprehensive networking and integration [redacted] (b) (7)(E) [redacted] the new plan is much more modest and leverages independent technology alternatives tailored to local operational needs and constraints. Where appropriate, the plan includes elements of the former SBI*net* program that have proven successful, [redacted] (b) (7)(E) [redacted] in SBI*net* Block 1 deployment.

2 CAPABILITY NEED

2.1 REQUIRED MISSIONS AND NEED

The DHS Quadrennial Homeland Security Report identifies the following missions:

- Mission 1: Preventing Terrorism and Enhancing Security
- Mission 2: Securing and Managing Our Borders
- Mission 3: Enforcing and Administering Our Immigration Laws

In support of these DHS missions, CBP is charged with managing, securing, and controlling the Nation's borders with a priority mission focus on preventing terrorists and terrorist weapons from entering the U.S. To that end, objective 1.1 in CBP's 2009-2014 Strategic

[4] SBInet Analysis of Alternatives: Final Report, 30 September 2011.

Plan states that CBP must: "*Establish and maintain effective control of air, land, and maritime borders through the use of the appropriate mix of infrastructure, technology and personnel. A segment of the border between ports of entry is considered under effective control when CBP can simultaneously and consistently achieve the following: (1)* ***detect*** *illegal entries into the United States; (2)* ***identify*** *and* ***classify*** *these entries to determine the level of threat involved; (3) efficiently and effectively* ***respond*** *to these entries; and (4) bring each event to a satisfactory law enforcement* ***resolution***."

CBP's key mission elements (i.e. mission essential tasks) are defined below in Table 2-1.

Table 2-1: CBP Mission Elements[5]

Mission Element	Definition
Predict	To anticipate illegal traffic actions prior to illegal activity
Detect	To discover possible illegal traffic
Track	To follow the progress/movements of an IoI
Identify	To determine what the IoI is (human, animal, conveyance)
Classify	To determine the level of threat or intent of the IoI
Respond	To employ the appropriate level of law enforcement resources to successfully address illegal traffic
Resolve	To take final action, whether legal, administrative, or otherwise. This includes capture data, process information, etc.

To successfully execute these mission elements, USBP requires a number of Foundational Operational Capabilities[6] that include:

- (b) (7)(E)
- (b) (7)(E)

[5] Secure Border Initiative (SBI) Design Reference Mission (DRM), Great Lakes and Southwest Border, V1.0 May 2010.

[6] These Foundational Operational Capabilities are defined in the USBP Operational Requirements-Based Budget Process Tool. They also include Impedance and Denial and Security Partnerships, which are beyond the scope of this document.

[7] See SBI DRM for additional information on the environmental conditions.

- (b) (7)(E)
- [redacted]

These capabilities directly impact situational awareness, the degree to which operators are able to perceive and process critical elements of information regarding the operational environment to project their status in the near future and to make effective operational decisions. Situational awareness is developed by blending reconnaissance, technology, and information sharing through partnerships and unified command structures, and intelligence to gain the best possible understanding of the threats we face along our Nation's borders. (b) (7)(E) capabilities are thus major enablers.

Using a risk-based approach, (b) (7)(E) capabilities are applied to ensure that CBP's limited resources are appropriately applied to the highest threats. To that end, USBP requires persistent surveillance in areas where there is a persistent threat, or in areas that are critical to USBP operations. USBP also requires a scalable, mobile response capability that provides the flexibility and agility to predict and rapidly respond to changes in risk along the border. The current environment in which the USBP and other law enforcement agencies operate is characterized by a variety of constantly evolving terrorist and transnational criminal threats that are both complex and variable. (b) (7)(E)

(b) (7)(E)

[8] Actionable intelligence is defined as information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process.

2.2 CAPABILITY GAPS

Three critical operational gaps directly related to surveillance were articulated in the October 2006 SBI MNS:

1. [redacted]
2. (b) (7)(E)
3. [redacted]

Since the release of the SBI*net* Mission Needs Statement in 2006, USBP and CBP have re-validated the need for [redacted]

(b) (7)(E)

[redacted]

2.2.1 Current Situation and Gaps

USBP characterizes the Arizona border according to the following three main environments: urban, rural and remote (these environments are defined in more detail in Section 3, and also in the SBI Design Reference Mission (DRM)). [redacted]

(b) (7)(E)

[redacted]

[9] See SBI DRM for additional information on threat tactics and capabilities.

(b) (7)(E)

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(b) (7)(E)

[redacted]

3 OPERATIONS AND SUPPORT DESCRIPTIONS

3.1 MISSIONS

Founded on May 28, 1924, the USBP manages border security across more than 6,000 miles of land border between POEs. In support of the CBP Mission Set #1, Securing America's Borders, USBP has several mission objectives:

[10] CBP's [redacted] System is a transactional enforcement application that captures all enforcement actions for Border Patrol Agents and CBP Officers. Note: [redacted]

- Prevent terrorists and terrorist weapons from entering the United States
- Manage risk
- Disrupt and dismantle Transnational Criminal Organizations (TCO)
- Increase and sustain the certainty of arrest
- Increase community engagement

These objectives align with the following missions and goals in the DHS Quadrennial Homeland Security Review Report:

- Mission 1: Preventing Terrorism and Enhancing Security
  - Goal 1.1: Prevent Terrorist Attacks
- Mission 2: Securing and Managing Our Borders
  - Goal 2.1: Effectively control U.S. Air, Land and Sea Borders
  - Goal 2.3: Disrupt and Dismantle TCOs
- Mission 3: Enforcing and Administering Our Immigration Laws
  - Goal 3.2: Prevent Unlawful Immigration

The USBP derives its authorities to manage the border from the Immigration and Nationality Act (INA) and is charged with enforcing laws that are primarily found in:

- Title 8: Aliens and Nationality[11]
- Title 18: Crimes and Criminal Procedure
- Title 19: Customs Duties
- Title 21: Food and Drugs

To effectively and efficiently accomplish its missions, USBP employs independent, stand-alone surveillance systems as a force multiplier to free agents from surveillance responsibilities and create a more agile force that can rapidly respond to changes in threat risks along the border. Using combined operational capabilities tailored to local operational risks, needs, and constraints, USBP will be capable of sustaining an acceptable baseline flow of illegal traffic and will be capable of anticipating and rapidly responding to a dynamic threat.

3.2 USERS AND OTHER STAKEHOLDERS

3.2.1 User Roles/Personnel

More than 20,000 Border Patrol Agents (BPA) are deployed across the country to prevent the illegal entry of persons and contraband between official POEs. Table 3-1 describes the roles of

[11] The jurisdiction of the USBP is based on 8 United States Code (USC) Section 1103, which charges the United States Attorney General with administering and enforcing the Immigration and Nationality Act (INA) and all other laws relating to the immigration and the naturalization of aliens. In addition, 8 USC Section 1103 (a)(5) specifies "the Attorney General shall have the power and the duty to control and guard the boundaries and the borders of the United States against the illegal entry of aliens and shall, in his discretion, appoint for that purpose such number of employees of the Bureau of Customs and Border Protection (CBP) as to him shall appear necessary and proper." The Homeland Security Act of 2002 transferred these responsibilities from the Attorney General to the Secretary of DHS.

personnel who use or are impacted in some way by surveillance technology or the operational outcomes.

Table 3-1: CBP Personnel / Users

User Role	Description
CBP Headquarters (HQ) Staff	Senior management personnel who set high-level goals, strategies, and priorities for CBP's operational components: USBP, OAM, Office of Field Operations (OFO) and Office of Intelligence and Investigative Liaison (OIIL).
HQ Office of Border Patrol (OBP) Staff	Through a unified chain of command, OBP oversees strategic planning, supporting operations, projects and national strategy for USBP. OBP receives reports from the field elements in support of decision making. OBP supplies reports to CBP, DHS and outside agencies.
USBP Supervisors	Management personnel who provide guidance and oversight for USBP operations. (b) (7)(E)
Border Patrol Agents (BPA)	Frontline personnel who carry out the day-to-day USBP mission in the field. (b) (7)(E) (b) (7)(E)
Sector Enforcement Specialists (SES)	SES's are government service personnel who assist enforcement personnel (b) (7)(E) (b) (7)(E)
Intelligence Research Specialists	Personnel who collect, analyze, and disseminate intelligence Information to support the CBP mission. (b) (7)(E) (b) (7)(E)
Intelligence Supervisors	Management personnel who provide guidance and oversight for the collection, analysis, and dissemination of intelligence information to support the CBP mission. (b) (7)(E)
Mission Support Specialists	Civilian personnel who provide various business and technology services to support the CBP mission. These services include maintenance, logistics, human resources, training, Information Technology (IT) support, and others.

User Role	Description
Joint Field Command (JFC)	The JFC, established in 2011, is a localized, organizational realignment to ensure CBP's Arizona-based leadership can direct a joint and integrated approach to border security, commercial enforcement, and trade facilitation missions throughout the Arizona area of operations. (b) (7)(E) (b) (7)(E)
Office of Intelligence and Investigative Liaison (OIIL)	Through prioritization and mitigation of emerging threats, risks, and vulnerabilities, OIIL enables CBP to better function as an intelligence-driven operational organization. (b) (7)(E) (b) (7)(E)

3.2.2 Other Stakeholders

In support of its mission, CBP and USBP have increased partnerships with Federal, State, Local, and Tribal law enforcement agencies, as well as with the public and private sectors to achieve a "whole-of-government approach" to border security. A complete list of external stakeholder agencies, both foreign and domestic, can be found in Appendix 5. Border Patrol operational elements work together with Federal, State, Local, Tribal and Foreign law enforcement partners to achieve a unity of purpose and maximize operational integration to achieve a holistic approach to border security. Unity of purpose, operational integration, intelligence fusion, and integrated partnerships all serve to define the current and collective efforts in border security. The sharing of resources, coupled with other enforcement efforts, provides the capability necessary to ensure USBP and its partners can address threats or emergencies within a region.

The ATP will provide additional situational awareness, which will increase information sharing with our partners and enhance the USBP mission as a whole. Coordination and data sharing with these stakeholders will continue through legacy USBP / CBP / DHS systems and operating procedures - the surveillance capabilities described within this CONOPS (b) (7)(E) (b) (7)(E)

3.3 Policies, Assumptions and Constraints

3.3.1 Operational Policies

A number of policies define the scope of responsibilities for USBP personnel and the manner in which border operations are conducted. They include:

- USBP National Strategy
- M68 – Officer's Handbook
- M69 – Law of Search Manual
- Collective Bargaining Agreement

- Immigration and Nationality Act
- CBP Use of Force Policy Handbook
- USBP Uniform Policy
- USBP K9 Policy
- USBP Vehicle Pursuit Policy
- Homeland Security Act of 2002
- Memorandum of Understanding (MOU) with Department of Interior (DOI)
- MOU with Drug Enforcement Agency (DEA)
- MOU with Immigrations and Customs Enforcement (ICE)
- DHS National Security Systems Policy Directive 4300B
- DHS Certification and Accreditation Guide (2010)
- DHS Management Directive 140-001, Handling Sensitive and Non-Sensitive Personally Identifiable Information
- DHS Management Directive 4900, Individual Use and Operation of DHS Information Systems/Computers
- DHS Management Directive 5200.1, Occupational Safety and Health Programs

3.3.2 Operational Assumptions

For the purposes of the ATP deployment and this CONOPS document, the following key assumptions have been made:

- Illegal traffic trends and flows will remain consistent with historical trends (b) (7)(E) [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted]
- USBP staffing levels will remain consistent with current and projected numbers
- Surveillance system operators will come from the existing USBP personnel force
- International partnerships and cooperation with the Mexican Government and local Mexican authorities will remain consistent with current conditions (or improve)
- [redacted] (b) (7)(E) [redacted][12]

3.3.3 Operational Constraints

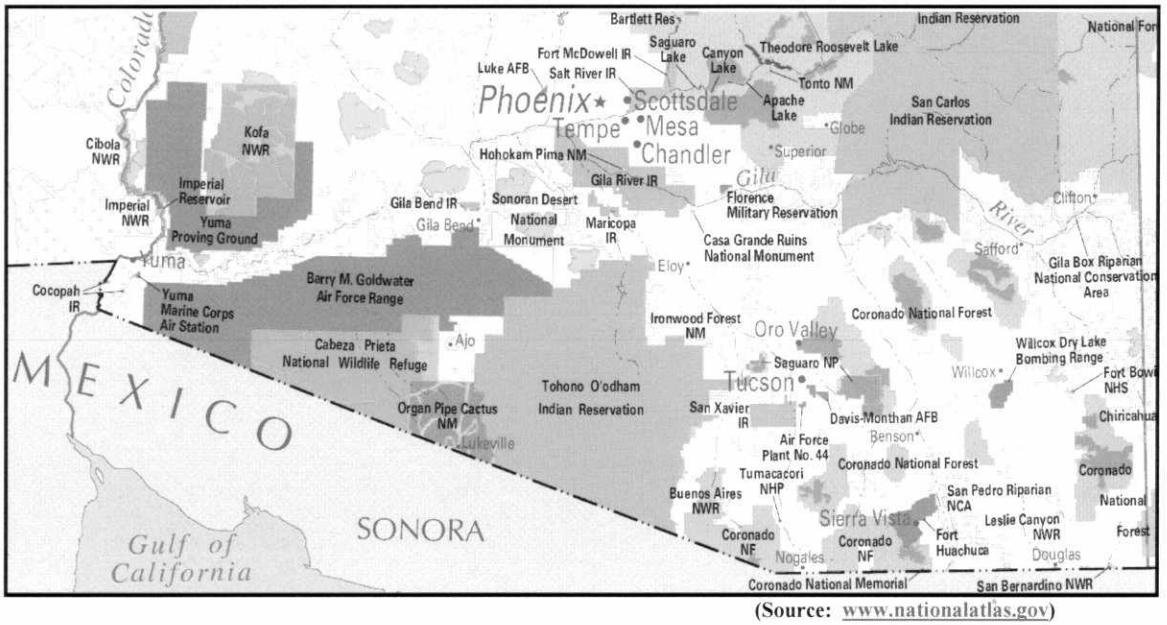
Operational constraints may adversely influence a surveillance system's ability to successfully perform the USBP mission. These constraints include the following:

- [redacted] (b) (7)(E) [redacted]
- [redacted] (b) (7)(E) [redacted]

[12] [redacted] (b) (7)(E) [redacted]

(b) (7)(E)

- [redacted]
- [redacted]
- [redacted]
- [redacted]



(Source: www.nationalatlas.gov)

Figure 3-1: Map of Federally Protected Lands in Southern Arizona

DHS has signed a Memorandum of Understanding (MOU)[13] with the Department of the Interior (DOI) and the Department of Agriculture (USDA). The MOU is intended to provide consistent goals, principles, and guidance related to border security activities such as law enforcement operations, tactical infrastructure installation, and utilization of roads, while recognizing the need to execute the DHS missions. It demands minimization and/or prevention of significant impacts on natural and cultural resources in accordance with the Wilderness and Endangered Species Acts and other related environmental laws, regulations, and policies across land management agencies. An excerpt of relevant portions of the MOU is provided below:

"USBP may operate motor vehicles on existing public and administrative roads and/or trails and in areas previously designated by the land management agency for off-road vehicle use at any time, provided that such use is consistent with presently authorized public or administrative use. USBP may drag existing public and administrative roads that are unpaved for the purpose of cutting sign, subject to compliance with conditions that are mutually agreed upon by the local Federal land manager and the USBP Sector Chief. If BPAs pursue or apprehend suspected Cross Border Violators in wilderness areas or off-road in an area not designated for such use, USBP will use the lowest impact mode of travel practicable to accomplish its mission and operate all motorized vehicles in such a manner that will minimize the adverse impacts on threatened or endangered species and on the resources and values of the particular Federal lands, provided officer safety is not compromised by the type of conveyance selected. Additionally, USBP will notify the local Federal land manager of any motorized emergency pursuit, apprehension, or incursion in a wilderness area or off-road in an area not designated for such use as soon as is practicable."

[13] NATIONAL DHS DOI USDA MOU, signed 3/31/06

3.4 OPERATIONAL DESCRIPTION

3.4.1 Operating Concept

USBP operations are founded on the mission essential tasks of detecting and tracking illegal entries, identifying and classifying those entries (to the greatest extent possible), responding to interdict, and resolving the incident through the appropriate law enforcement actions. Illegal entrants include dismounted humans walking alone or in groups, humans traveling on animals such as horses and conveyances such as all terrain vehicles (ATV), light and heavy vehicles, and more recently, low flying aircraft such as ultra-lights.[14] Anything or anyone that fits these descriptions is considered an IoI to USBP, whether legal or not.

Increasingly, USBP is achieving operational efficiencies by employing independent, stand-alone surveillance systems to enable the mission essential tasks. The ATP describes the deployment of existing, proven surveillance technology solutions according to the unique needs of each AoR in Arizona. Key elements of USBP's technology deployment approach include:

- The deployment of capabilities to effectively manage current risks
- Using technology as a force multiplier to free personnel to respond to areas of increasing risk
- Increasing mobile response capability to respond to changes in risk along our Nation's borders
- Joint, integrated operations and intelligence analysis and sharing at the operational level

The ATP includes a combination of the following stand-alone surveillance system solutions across urban, rural and remote areas:

- Agent-centric systems (e.g. [redacted] (b) (7)(E) [redacted])
- Aviation-centric systems (e.g. Unmanned Aerial Systems (UAS), [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted])
- Mobile systems (e.g. [redacted] (b) (7)(E) [redacted]
- Fixed systems (e.g. IFT and [redacted] (b) (7)(E) [redacted]

With the exception of [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted], these solutions are all currently employed by USBP as a part of current operations. [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] These additional resources, coupled with the investments within the 2010 Southwest Border Supplemental appropriation, are expected to significantly reduce the flow of illegal traffic in Arizona and provide the necessary situational awareness of targeted areas along the Arizona border. Figure 3-2 provides a high level overview of the surveillance technology operating concept.

[14] Although low flying aircraft are an item of interest, air surveillance is beyond the scope of this document.

(b) (7)(E)

Figure 3-2: Operating Concept – Arizona Border Surveillance Deployment Plan

The combination of operational capabilities illustrated in Figure 3-2 is intended to increase situational awareness within selected focus areas, which are referred to as areas of interest (AoI) throughout the remainder of this document. An AoI is a targeted area within a USBP station's AoR that requires surveillance due to the risk level associated with border threat exploitation. USBP may use one or more systems to monitor an AoI, as illustrated in Figure 3-2, and there may be more than one AoI within a USBP station's AoR. Once deployed to an AoI, each system provides a resulting area of coverage (AoC) that depends on factors such as (b) (7)(E) (b) (7)(E) and (b) (7)(E) Figure 3-3 illustrates these concepts notionally for an IFT system.

Because a system's AoC depends (b) (7)(E) (b) (7)(E) (b) (7)(E) The system/unit lay-down should maximize each system's AoC and the overall AoC provided by all the surveillance systems (which may include a hybrid solution of ground, air and maritime surveillance resources) in the most cost-effective manner possible to address the threat within the AoI.

(b) (7)(E)

- Area of Interest (AoI): A targeted area within a USBP Station's AoR that requires surveillance due to the risk level associated with border threat exploitation.
- Surveillance Area: The area within which a single system unit is capable of detecting, tracking and identifying illegal incursions at any specific instant (b) (7)(E) (b) (7)(E) (b) (7)(E)
- Area of Coverage (AoC): The resulting area, (b) (7)(E) (b) (7)(E), within which USBP can successfully conduct surveillance activities using the system, or a combination of systems.

Figure 3-3: Surveillance Coverage Terminology

3.4.2 Employment Modes

USBP uses stand-alone surveillance systems to support persistent surveillance operations, mobile response operations, which can include special operations, and training to provide a layered approach to border surveillance that ensures the ability to address the highest risk threats and adjust accordingly. Table 3-2 summarizes the modes of surveillance employment. The ranges shown are as measured from the system/unit, with the exception of the aviation-centric systems, (b) (7)(E)

Table 3-2: System Surveillance Employment Summary

Employment Mode	Urban	Rural	Remote
(b) (7)(E)	(b) (7)(E)		
(b) (7)(E)			
(b) (7)(E)			

Employment Mode	Urban	Rural	Remote
(b) (7)(E)	(b) (7)(E)		
(b) (7)(E)			
(b) (7)(E)			

(b) (7)(E)

3.4.2.1 ***Persistent Surveillance***

USBP employs fixed systems in areas where there is a persistent threat or in areas that are critical to USBP operations. To maximize operational efficiency, the fixed systems all provide remote monitoring capability of (b) (7)(E) at the USBP station and enable a single operator to manage a much larger AoC as compared to the other system alternatives (i.e. mobile, aviation-centric and agent-centric). (b) (7)(E) (b) (7)(E) These surveillance systems include:

- (b) (7)(E)
-
-
-

[15] A unit, such as an (b) (7)(E) or IFT unit (b) (7)(E) (b) (7)(E)

(b) (7)(E)

3.4.2.2 ***Mobile Response***

USBP employs mobile/transportable systems to conduct surveillance operations according to (b) (7)(E) and daily operational needs. These surveillance systems include:

- (b) (7)(E)

USBP employs aviation-centric systems according to (b) (7)(E) and daily operational needs as follows:

- (b) (7)(E)

Agent centric (i.e. hand held) systems [redacted] (b) (7)(E) are redeployed with agents on a daily basis [redacted] (b) (7)(E) according to [redacted] (b) (7)(E) daily operational needs. These needs may include [redacted] (b) (7)(E)

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

3.4.2.3 *Degraded Surveillance Operations*

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

3.4.2.4 *Training Operations*

USBP leverages on-the-job-training (OJT) for many of its surveillance systems as well as on-line training using CBP's Virtual Learning Center (VLC). OJT typically occurs [redacted] (b) (7)(E)

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

3.4.3 Scheduling and Operations Planning

USBP employs surveillance systems in support of operations 24 hours a day, 7 days a week. Table 3-3 discusses typical scheduling and operations planning for the four surveillance system alternatives.

Table 3-3: Scheduling and Operations Planning

Alternative Type	Description
Agent-Centric	Agent-centric devices are issued to the appropriate Patrol Agents (PA) [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] Supervisors and asset managers ensure the equipment goes to the most appropriate locations for the optimal duration/law enforcement effect.
Aviation-Centric	Aviation-centric surveillance is scheduled/requested according to tactical and [redacted] (b) (7)(E) needs. Requirements for aviation-centric surveillance can occur anytime during USBP operations.
Fixed	Fixed assets such as IFT and [redacted] (b) (7)(E) are operated 24 hours a day, 7 days a week, except when down for scheduled or unscheduled maintenance.

Alternative Type	Description
Mobile	Mobile assets (b) (7)(E) are typically operated 24 hours a day, 7 days a week (b) (7)(E) (b) (7)(E)

3.4.4 Operating Environment

3.4.4.1 *Geographic Area*

The geographic areas of operation for the Phase 1A AoA surveillance systems are limited to the Arizona border. Geographic details and challenges along this border are summarized in Table 3-4, and are described in greater detail in the SBI DRM.

Table 3-4: Terrain Descriptions

Topology/Terrain	Description[16]	Primary Key Attributes[17]
Urban/Suburban	This class includes flat or hilly terrain with prevalent artificial structures (i.e. houses, buildings, fences). (b) (7)(E) (b) (7)(E)	• • • • • • (b) (7)(E)
(b) (7)(E) (Rural)	(b) (7)(E)	• • • • • •
(b) (7)(E) (Rural)		• • • • • •

[16] SBI DRM

[17] Primary key attributes as defined by the SBI DRM represent those characteristics of the mission space that are (b) (7)(E)

Topology/Terrain	Description[16]	Primary Key Attributes[17]
(b) (7)(E) (Remote)	(b) (7)(E)	
(b) (7)(E) (Remote)		
Water Body	This class includes flat, open water-body surfaces. (b) (7)(E) (b) (7)(E)	(b) (7)(E)
Special	This class contains areas that could not be easily binned in one of the other classifications due to certain unique attribute mixes (i.e. (b) (7)(E) (b) (7)(E)	N/A

As noted in Table 3-4, (b) (7)(E) (b) (7)(E)

3.4.4.2 ***Environmental Conditions***

Surveillance technologies will be deployed outdoors and exposed to the elements, so the systems should be sufficiently ruggedized to withstand the climates where deployed. (b) (7)(E) (b) (7)(E)

3.4.5 Threats and Hazards

Surveillance systems are subject to both man-made and environmental threats. Drug trafficking organizations, smuggling organizations, illegal immigrants, and other international cross-border threats (b) (7)(E) [redacted] (b) (7)(E) [redacted] The system design should minimize vulnerabilities (b) (7)(E) [redacted]

Agent-centric, aviation-centric and mobile systems are also subject to constant shock and vibration during transit, and, as discussed in Section 3.4.4.2, weather extremes also impact the systems through exposure. Sufficiently ruggedized equipment deployed to the field is necessary to meet performance and availability requirements.

3.4.6 System Command and Control Facilities

The deployment of these surveillance systems (b) (7)(E) [redacted] Ideally, all [redacted] (b) (7)(E), (b) (5) [redacted] (b) (7)(E) [redacted] System interoperability is discussed in greater detail in Section 3.4.7.

3.4.7 Interoperability with External Systems

Currently, [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] as illustrated in Figure 3-4.

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

Figure 3-4: Surveillance System Interoperability (Current State)

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

Alternatively, Figure 3-5 reflects the desired level of inoperability to further enhance situational awareness across an AoR.

(b) (7)(E), (b) (5)

Figure 3-5: Surveillance System Interoperability (Desired State)

Desired interoperability among systems, achieved either through (b) (7)(E) (b) (7)(E) or through the implementation of (b) (7)(E) includes the following capabilities:

- (b) (7)(E), (b) (5)
-
-
-

(b) (7)(E), (b) (5)

(b) (7)(E)

3.5 MISSION SUPPORT DESCRIPTION

3.5.1 Training

Training for many of the surveillance systems in the ATP already exists, and consists primarily of OJT along with checklists for new operators to demonstrate proficiency with the tools. On-line training via CBP's VLC is also available where appropriate. Current training programs will need to expand as the number of systems/operators increases. Common functionality and hardware among systems can minimize training requirements. Where there are training gaps, the Program Office, in partnership with the Office of Information and Technology (OIT) and the Office of Training and Development (OTD), will ensure the necessary modules and material are developed to support training needs for each surveillance system. Any new training requirements should leverage existing training resources such as OJT, VLC computer-based training, intranet connectivity on the mobile data terminals (MDT) as well as classroom tutorial / syllabus training. The training must cover initial training, train the trainer (T3) training and recurrent training as necessary for the operation and maintenance of the systems. New training requirements that change the work environment must be coordinated with the National Border Patrol Council.

3.5.2 Maintenance and Logistics Support

The surveillance systems perform mission-critical functions 24 hours a day, 7 days a week. Each system must employ health and status monitoring capability in order to predict and identify mission critical failures (such as (b) (7)(E) (b) (7)(E) etc.) and quickly report them to the operator for corrective action. (b) (7)(E) (b) (7)(E) (b) (7)(E) Mission critical failures include any failure condition that prevents the system from performing the necessary functional capabilities. Once a mission critical failure occurs, the system is no longer considered mission capable (full or partial).

At least two levels of maintenance are necessary to support operations – operational level and depot level. At the operational level, maintainers (either government or contractor) are required to conduct both preventive (such as refueling, oil filter changes, (b) (7)(E) etc.) and corrective maintenance (such as troubleshooting, (b) (7)(E) and LRU replacements), either in the field or at the applicable CBP facility. Preventive maintenance should have little to no impact on operations. BPAs may be relied on to conduct very limited maintenance activities in the field, such as monitoring system health and status, conducting sub-system or system reboots, (b) (7)(E) provided those actions do not require any special tools or training outside of standard operator/system training. Maintenance support staff is

required to conduct all maintenance activities in those areas where agent staffing cannot support the level of effort.

The maintenance and logistics support approach must ensure that each system's availability requirements are met. Because factors such as terrain, land-use, weather, etc. can affect system access, the need for preventive and corrective maintenance conducted at the site must be minimized and limited in duration. Once a mission critical failure is identified (such as (b) (7)(E) (b) (7)(E), the system operator reports the failure in accordance with applicable maintenance procedures. On-call support from a trained technician may be necessary to assist operators with troubleshooting the equipment. On-call technical support is particularly useful (b) (7)(E) (b) (7)(E) If the problem cannot be resolved at the operational level, an authorized maintenance technician performs site repairs on the deployed assets and uses site level spares to replace faulty line replaceable units (LRUs). Alternatively, mobile and agent-based systems can be returned by the operator to a designated CBP facility, such as a USBP station, where faulty LRUs can be replaced. Depot level maintenance is necessary for those corrective actions that cannot be done at the operational level, such as the repair of unserviceable LRUs. The need for intermediate level maintenance depends upon the logistics support approach required to ensure system capability and availability.

Operators must be aware of any system performance degradation so that they can plan operations and address capability gaps accordingly. To this end, regular operational analyses must be conducted over the life of the system to assess and ensure continued capability at best cost. This includes the regular collection and reporting of Key Performance Parameters, supporting Critical Technical Parameters and other metrics useful for predicting/planning ongoing operations and maintenance as detailed in the applicable integrated logistics support plans.

Supply chain management capabilities, depot level sparing and software maintenance must ensure availability requirements are met and that system down time is minimized at best cost. The operational plan for equipment setup, operations, disassembly, packaging, and field-level maintenance, along with operations and maintenance manuals and vendor technical support will be detailed in the applicable integrated logistics support plans.

(b) (7)(E)

3.6 POTENTIAL IMPACTS

3.6.1 Threat Measures

USBP has traditionally recorded threat measures (b) (7)(E) in official CBP databases. The data in these systems, such as the (b) (7)(E) system, is sensitive and is not available to the public. All things being equal, the addition of these surveillance capabilities is expected to increase the number of apprehensions in the near term within each system's AoC, and then reduce the number of apprehensions as the systems deter or deflect traffic to areas outside the AoC. However, the number of apprehensions over any period of time

is also a function of [redacted] (b) (7)(E) [redacted] As a result, the impact of the systems on number of apprehensions is difficult to quantify.

The impact of these surveillance systems is likely to cause statistical fluctuation in apprehensions as a function of the increased situational awareness they provide. Similarly, the additional situational awareness will decrease the number of "got-aways" in any given AoC by improving USBP's detection and response capabilities.

It should be noted that USBP is currently in the process of refining its measures of performance to assess mission success, but those measures are not available at this time.

3.6.2 Mission Elements

The ATP is expected to have the following impacts on the CBP mission essential tasks:

- Predict - [redacted] (b) (7)(E) [redacted]
  [redacted] (b) (7)(E) [redacted]
- Detect / Identify / Classify – These mission elements are the cornerstone of situational awareness. [redacted] (b) (7)(E) [redacted]
  [redacted] (b) (7)(E) [redacted]
- Track - [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted]

(b) (7)(E)

- Respond – (b) (7)(E)

(b) (7)(E)

- Resolve – (b) (7)(E)

(b) (7)(E)

3.6.3 Doctrine

The USBP approach to border security focuses on a number of strategic goals and initiatives that include, but are not limited to:

- (b) (7)(E)
- Increasing and sustaining the certainty of arrest for illegal crossings

The implementation of the ATP and the CONOPS defined herein align with these goals and initiatives in that the technology will increase situational awareness, (b) (7)(E)

(b) (7)(E)

(b) (7)(E) and increase the certainty of arrest through increased situational awareness.

As USBP gains additional experience with these systems and further refines its CONOPS and TTPs, there may be a need to adjust doctrine as follows:

- (b) (7)(E), (b) (5)

(b) (7)(E)

maritime borders. (Note: maritime, air and tunnel threats are beyond the scope of the document.) It should be noted that current plans and initiatives to address deflection and displacement are outlined in the new USBP National Strategy (currently in draft form).

- USBP may need to develop and implement new policy plans to address a more violent threat as it becomes increasingly difficult to cross the border. The threat will be more likely to resort to violence, bribery, and other methods to increase the chance of success.
- USBP may need to expand or develop TTPs to optimize the utility and performance of the surveillance systems and operator proficiency, and to adjust to changes in threat tactics and techniques.

Changes to the USBP policies listed in Section 3.3.1 are not anticipated.

3.6.4 Organization

As these surveillance systems are deployed to USBP stations, each station will need to adjust its organization as necessary to account for the teams of operators, maintainers and logistics support personnel. For example, many stations have teams, or pools, of operators or SESs dedicated to a particular system or area of expertise, and they may elect to create a team for IFT or (b) (7)(E) operators (which may require coordination with the National Border Patrol Council).

(b) (7)(E)

(b) (7)(E)

(b) (7)(E) As a result, (b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

3.6.5 Training

USBP already has training in place for many of the surveillance systems it currently uses and heavily leverages practical experience, OJT and VLC. Because (b) (7)(E) and IFT feature greater operator functionality and complexity with the operating picture, the deployment of more of these systems will require additional classroom training, (b) (7)(E)

(b) (7)(E) As a result, (b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

(b) (7)(E), (b) (5) Changes to CBP's/USBP's overall training methodologies are not anticipated as result of these surveillance system deployments; however, USBP must consider (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E) Regardless, the training approach must remain flexible and tailored to address unique training needs at each USBP station.

It should be noted that changes or additions to training requirements may require coordination with the National Border Patrol Council.

3.6.6 Materiel

The deployment of these surveillance systems necessitates a number of additional materiel needs in order to maximize the return on the investment. Additional material requirements include the following:

- (b) (7)(E), (b) (5)
- Data Analysis Capability: (b) (7)(E), (b) (5) (b) (7)(E), (b) (5)
- Access: Tactical infrastructure facilitates (b) (7)(E) (b) (7)(E), (b) (5)
- (b) (7)(E)ransport: (b) (7)(E), (b) (5) (b) (7)(E), (b) (5)
- (b) (7)(E), (b) (5)

3.6.7 Leadership

Impacts to leadership or USBP chain of command as a result of surveillance system deployment are not anticipated. However, (b) (7)(E), (b) (5) (b) (7)(E), (b) (5)

3.6.8 Personnel

The deployment of these systems will impact personnel (operators, SESs, government employees, and/or contractors) as follows:

- System operators will be required as defined in Table 3-5.

Table 3-5 Surveillance System Operator Requirements

Type	USBP Operator Requirements
Agent-Centric	(b) (7)(E)
Aviation-Centric	
Fixed	
Mobile	

- (b) (7)(E)
- Personnel will be required to support and sustain the equipment in accordance with the availability and reliability requirements and ensure each system's continued readiness.
- (b) (7)(E)

3.6.9 Facilities

The deployment of these systems will impact facility requirements as follows:

- Facility space will be necessary to support (b) (7)(E), (b) (5) (b) (7)(E), (b) (5)
- Facility space will be necessary for the associated processing equipment.
- Facility space will be necessary for line level and depot maintenance of these systems.
- Facility space will be necessary for operator and maintainer training.

- Facility space will be necessary for the detention of the individuals apprehended. As noted previously, [redacted] (b) (7)(E), (b) (5) [redacted] (b) (7)(E), (b) (5) [redacted]
- Facility space may be necessary [redacted] (b) (5) [redacted] (b) (5) [redacted]

3.6.10 Regulations

The need for new or modified regulations as a result of the surveillance system deployment is not anticipated. However, [redacted] (b) (7)(E), (b) (5) [redacted] (b) (7)(E), (b) (5) [redacted]

3.6.11 Grants

Not applicable.

3.6.12 Standards

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

4 SCENARIOS

The scenarios below are a conceptual notion of how USBP will use a combination of surveillance systems along the border. More detailed scenarios unique to each system (e.g. [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] etc) are provided in each system's Operational Requirements Document. The SBI DRM also provides tactical situations that further illustrate criminal tactics.

4.1 MISSION OPERATIONS SCENARIOS

4.1.1 Urban

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

(b) (7)(E)

4.1.2 Rural

(b) (7)(E)

(b) (7)(E)

[redacted]

4.1.3 **Remote**

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

4.2 Mission Support Scenarios

The following sections illustrate how preventive and corrective maintenance will be conducted according to the system alternative type.

4.2.1 Agent-centric systems (hand held systems)

Preventive maintenance will be conducted at the operational level (either at the site or a designated CBP facility such as a USBP station) by the operators and will include items such as replacing batteries, [redacted] (b) (7)(E)

For corrective maintenance, failed items will be returned to the station / sector point issue and replacements drawn from station / sector point of issue. Station/ sector field support personnel will return the failed units to Government Primary Inventory Control Activity (PICA), or the applicable repair location as designated by the PICA, for repair or disposition. Replacement units will be requisitioned via the Government supply chain to replace failed units.

4.2.2 Mobile systems: (b) (7)(E)

Preventative maintenance may be conducted at the operational level at either the site where the unit is being used or at a designated CBP facility such as a USBP sector/station (e.g. (b) (7)(E) (b) (7)(E) at the site; battery change-out may have to be accomplished at the USBP station).

For corrective maintenance, the removal and replacement of LRUs (e.g. (b) (7)(E) (b) (7)(E)) will be done either at the site or a designated CBP facility. Limited repairs, such as repairing (b) (7)(E), etc. can also be done by trained maintenance technicians at the operational level. Failed LRUs will be returned to the PICA/Government Depot or designated Original Equipment Manufacturer (OEM) for repair and/or disposition.

4.2.3 Fixed systems: IFT and (b) (7)(E)

Preventative maintenance will be conducted at the site level by trained maintenance technicians assigned to the area of operations. These personnel will be assigned on a system level basis (e.g. (b) (7)(E) Station, etc.).

Corrective Maintenance will be performed by removing and replacing LRUs at the site level and returning failed LRUs to either a PICA/Government depot or OEM manufacturer for repair and/or disposition.

4.2.4 Aviation-centric systems: (b) (7)(E) (b) (7)(E)

Support scenarios for aviation-centric systems are beyond the scope of this document.

5 FUNCTIONAL CAPABILITIES

5.1 Mission Operations Functional Capabilities

The operational activities illustrated in the scenarios can be categorized into the following functional capabilities. Also noted in the table is whether the capability is a primary capability in support of the USBP mission objectives defined in Section 3.1, or a secondary, supporting mission enabler. The operational requirement documents for each system further describe these functional capabilities.

Table 5-1: Mission Operations Functional Capabilities

Functional Capability	Capability Description	Mission Contribution
Plan Surveillance Operations	(b) (7)(E)	Primary

Functional Capability	Capability Description	Mission Contribution
Relocate Surveillance Assets	(b) (7)(E)	Primary
Detect Iols		Primary
Track Iols		Primary
Identify Iols		Primary
Classify Iols		Primary
Track (b) (7)(E) (b) (7)(E)		Primary
Plan Response		Primary
Interdict		Primary
Communicate (b) (7)(E)		Primary

Functional Capability	Capability Description	Mission Contribution
Collect and Report Iol Data	(b) (7)(E)	Primary
Analyze Trends		Primary

5.2 Mission Support Functional Capabilities

Table 5-2 describes the mission support functional capabilities.

Table 5-2: Mission Support Functional Capabilities

Functional Capability	Capability Description	Mission Contribution
Conduct Maintenance	The ability to conduct scheduled and unscheduled system maintenance as follows: Site (Organizational) Level Maintenance: Maintenance conducted at the location at which equipment is operated (e.g. (b) (7)(E) site location). This also includes maintenances areas such as station or sector level CBP facilities. Intermediate Level Maintenance: Maintenance / repairs conducted at "forward" maintenance area such as vendor provided facilities as required by the integrated logistics support plan. Depot Level Maintenance: Maintenance / repairs conducted at a designated Government industrial facility designated as a depot. OEM Maintenance: Depot level maintenance conducted at a vendor's production or designated depot level repair facility.	Primary
Manage Supply Chain	The ability to provide and manage the supply chain in support of system maintenance as follows: Forward Supply Points: This activity will provide a location at which to pre-position spares, consumables, and support and test equipment. It will have limited administrative capability for field technicians to use to report daily maintenance activities. An example of this is a forward supply point located at (b) (7)(E) station supporting Block 1 systems. Warehouse(s) and Inventory Control Points: The activity will be located in a major area of operation (typically a sector) supporting many forward supply points and systems with spares, consumables, test and support equipment,	Secondary

Functional Capability	Capability Description	Mission Contribution
	administrative support facilities and intermediate level maintenance. An example of this is the Primary Support Facility / Warehouse located in (b) (7)(E) and supporting Block 1 systems and (b) (7)(E) (b) (7)(E)	
Provide Independent Second Level Engineering Activities (ISEA) Support	The ability to provide technical and operational support as follows: (b) (7)(E)	Secondary

APPENDIX 1: TABLE OF CHANGES

Table A-1: Table of Changes

Change Number	Date	Reference (Table, Figure, or Paragraph Sections)	A=Add M=Modify D=Delete	Brief Description of Change

APPENDIX 2: REFERENCES

Table A-2 lists applicable government documents.

Table A-2: Government Documents

Doc #	Document Title	Date
NA	CBP Strategic Plan	2005-2010
NA	CBP's Missions, Goals, and Priorities, FY2011-2013	March 24, 2011
NA	National Border Patrol Strategy, Office of Border Patrol	September, 2004
NA	Arizona Border Surveillance Technology Plan Briefing	July 2010
NA	SBI*net* Mission Needs Statement (MNS)	October 1, 2006
NA	Secure Border Initiative (SBI) Design Reference Mission (DRM) – Great Lakes and Southwest Border, Office of Border Patrol Sectors, Version 1.0	May 2010
NA	Secure Border Initiative Integrated Concept of Operations (CONOPS) and Requirements Specification 2.1	July 2007
NA	National DHS DOI USDA MOU	March 31, 2006
N/A	Memorandum to the DHS Secretary: Report on the Comprehensive, Science-Based Re-Assessment of the Secure Border Initiative-Network Program	October 29, 2010
N/A	SBI*net* Analysis of Alternatives: Final Report	September 30, 2011
OTIA05-IFT-00-000001	Integrated Fixed Tower System Operational Requirement Document, Rev A, Draft	August 10, 2011
OTIA05-MVSS-00-00001	(b) (7)(E) [redacted] Operational Requirements Document, Version V0.01d Draft	October 4, 2011
OTIA05-RVSS-00-00001	(b) (7)(E) [redacted] Operational Requirements Document, Version V0.13 Draft	August 04, 2011
OTIA05-SRTS-01-000001	Unattended Ground Sensor Operational Requirements Document, Draft	October 26, 2011

APPENDIX 3: GLOSSARY OF TERMS

Table A-3: Glossary of Terms

Term	Definition
Actionable Intelligence	Information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process.
Area of Coverage (AoC)	The resulting area, considering installation location (b) (7)(E) (b) (7)(E) etc., within which USBP can successfully conduct surveillance activities using the system or a combination of systems.
Area of Interest (AoI)	A targeted area within a USBP station's AoR that requires surveillance due to the risk level associated with border threat exploitation
Area of Responsibility (AoR)	The geographical area where border security operations are authorized. USBP formally defines AoRs at the sector level and station level. USBP also informally assigns AoRs at the individual agent level according to operational needs. USBP Sector AoRs are shown at the following link: (b) (7)(E)
(b) (7)(E)	(b) (7)(E)
	(b) (7)(E)
Got-Away	A border patrol metric that estimates the number illegal entrants who have been identified through surveillance means but are not successfully interdicted. There is some error in this number due to the inability to positively confirm whether individuals ultimately apprehended were previously documented as got-aways.
Item of Interest (IoI)	Dismounted humans, humans mounted on animals, animals, and conveyances such as all terrain vehicles (ATV), motorcycles, automobiles, and trucks.
Long Arms	Large man-portable firearms (i.e. Rifles, Shotguns, etc) that cannot generally be concealed beneath clothing
Line Replaceable Unit (LRU)	A component of a system or subsystem which is capable of being removed and replaced at the field level.
Maritime Environment	Near-coastal area along large bodies of water including lakes, bays, and oceans including proximal shorelines. (b) (7)(E) (b) (7)(E)
Near Real Time	A low-latency delay of approximately (b) (7)(E) or less.
Operational Availability, Ao	The percentage of time that a system will be available to perform its operational functions; Ao = Up Time/Total Time, where Up Time includes both full and partial mission capability. Once a mission critical failure occurs, a system is no longer considered mission capable (full or partial).
Operational Readiness Rate	The number of mission capable (full or partial) systems divided by total systems, or in the case of system with a series of integrated units (such as IFT), the number of mission capable units divided by total units.

Persistent Surveillance	The ability to continuously detect, track, identify and classify border incursions 24 hours a day, 7 days a week in targeted areas (b) (7)(E) (b) (7)(E)
Remote Environment	Border areas characterized by (b) (7)(E) (b) (7)(E)
Rural Environment	Border areas characterized by (b) (7)(E) (b) (7)(E)
Situational Awareness	The degree to which operators are able to perceive and process critical elements of information regarding the operational environment to project their status in the near future and to make effective operational decisions.
Surveillance Area	The area within which a single system unit is capable of detecting, tracking and identifying illegal incursions at any specific instant (b) (7)(E) (b) (7)(E)
Unit	The deployed equipment that includes the tower and the sensor suite.
Urban Environment	Areas on the U.S. border with "built-up" characteristics such as industrial, business, commercial, and residential infrastructure (b) (7)(E) (b) (7)(E)
Video	A sequential or continuous streaming of images, digital or analog, that appears unbroken to the human eye, typically at a specified temporal rate greater than (b) (7)(E)

APPENDIX 4: LIST OF ACRONYMS

ATP	Arizona Border Surveillance Technology Plan
AMOC	Air & Marine Operations Center
(b) (7)(E)	
Ao	Operational Availability
AOA	Analysis of Alternatives
AoC	Area of Coverage
AoI	Area of Interest
AoR	Area of Responsibility
(b) (7)(E)	
ATV	All Terrain Vehicle
C2	Command and Control
C4I	Command, Control, Communication, Coordination and Intelligence
CBP	Customs and Border Protection
CCTV	Closed-Circuit Television
CONOPS	Concept of Operations
COP	Common Operating Picture
CTDD	Controlled Tire Deflation Device
COTS	Commercial Off-The-Shelf
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOI	Department of Interior
DRM	Design Reference Mission
FoR	Field of Regard
FOS	Field Operations Supervisor
FoV	Field of View
GOTS	Government Off-The-Shelf
GPS	Global Positioning System
HQ	Headquarters
IC	Information Center
(b) (7)(E)	
ICE	Immigration and Customs Enforcement
IFT	Integrated Fixed Tower
IoI	Item(s) of Interest
IS	Imaging Sensor
ISEA	Independent Second Level Engineering Activities
IT	Information Technology
JFC	Joint Field Command
LMR	Land Mobile Radio
LoS	Line of Sight
LP/OP	Listening Point/Observation Point
LRF	Laser Range Finder
LRU	Line Replaceable Unit

MDT	Mobile Data Terminal
MNS	Mission Need Statement
MOU	Memo of Understanding
(b) (7)(E)	
NCIC	National Crime Information Center
NDI	Non Developmental Item
NLETS	National Law Enforcement Telecommunications System
NVG	Night Vision Goggles
NTIA	National Telecommunications and Information Administration
OAM	Office of Air and Marine
OBP	Office of Border Patrol
OEM	Original Equipment Manufacturer
OFO	Office of Field Operations
OIAD	Operational Integration and Analysis Division
OIIL	Office of Intelligence and Investigative Liaison
OIT	Office of Information and Technology
OJT	On the Job Training
OTD	Office of Training and Development
OTIA	Office of Technology Innovation & Acquisition
PA	Patrol Agent
PICA	Government Primary Inventory Control Activity
POE	Port(s) of Entry
PTZ	Pan Tilt Zoom
RF	Radio Frequency
(b) (7)(E)	
SBI	Secure Border Initiative
SES	Sector Enforcement Specialist
SPPA	Strategic Planning, Policy and Analysis
T3	Train the Trainer
TCO	Transnational Criminal Organizations
TECS	Treasury Enforcement Communications System
TTP	Tactics, Techniques and Procedures
UAS	Unmanned Aerial System
UGS	Unattended Ground Sensor
US	United States
USBP	United States Border Patrol
USC	United States Code
USCG	United States Coast Guard
USDA	United States Department of Agriculture
V&S	Visibility and Surveillance
VLC	Virtual Learning Center
WSA	Wilderness Study Area

APPENDIX 5: EXTERNAL STAKEHOLDERS

Table A-4: External Stakeholders[18]

		Mission Area	Anti-Terrorism	Immigration	Counter-Drug	General Criminal Activity	Land Use Environment	Public Safety
Domestic	Acronym							
American Indian Tribes	None					•	•	
Bureau of Alchohol, Tobacco, Firearms and Explosives	ATF		•			•		
Bureau of Indian Affairs	BIA						•	
Bureau of Land Management	BLM						•	
Bureau of Reclamation	USBR						•	
Center for Disease Control	CDC							•
Central Intelligence Agency	CIA		•		•	•		
Citizenship and Immigration Services	USCIS			•				
Domestic Nuclear Detection Office	DNDO		•					
Drug Enforcement Agency	DEA				•			
Environmental Protection Agency	EPA						•	
Federal Bureau of Investigation	FBI		•			•		
Federal Emergency Management Agency	FEMA		•					
Financial Crimes Enforcement Network	FinCEN		•		•	•		
Food and Drug Administration	FDA							•
Immigration and Customs Enforcement	ICE			•				
Local Law Enforcement Agencies	LEA				•	•		
National Park Service	NPS						•	
Transportation Security Administration	TSA		•			•		•
United State Departmtent of Defense/United States Northern Command	DoD/USNORTHCOM		•					
United States Coast Guard	USCG		•	•	•			
United States Department of Agriculture	USDA							•
United States Department of Energy	US DoE							•
United States Department of Justice	US DoJ				•	•		•
United States Department of State	US DoS							•
United States Department of the Interior	US DoI						•	
United States Fish and Wildlife Service	FWS						•	
United States Forest Service	USFS						•	
United States Secret Service	USSS					•		
Foreign	Acronym							
Aduanas de Mexico	None						•	•
Canadien Border Services Agency	CBSA			•				•
International Criminal Police Organization	Interpol		•		•	•		
Procuraduria General de la Republica and Mexican Authorities	PGR					•		
Royal Canadian Mounted Police	RCMP		•	•	•	•		•

APPENDIX 6: SURVEILLANCE SYSTEM DESCRIPTIONS

A.6.1 Agent-centric systems

USBP currently employs agent centric support equipment for mobile surveillance; this category of equipment is man-portable, or transportable in a vehicle. The equipment includes (b) (7)(E)

(b) (7)(E)

A.6.2 Aviation-centric systems

Aviation-Centric systems include (b) (7)(E)

(b) (7)(E)

A.6.3 Mobile / Redeployable Systems

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

A.6.4 Fixed, Integrated Systems

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)