U.S. Customs and Border Protection

REMOTE VIDEO SURVEILLANCE SYSTEM (RVSS) OPERATIONAL REQUIREMENTS DOCUMENT (ORD)

DOCUMENT NO: **OTIA05-RVSS-00-000001**

VERSION: A, DECEMBER 23, 2011

Developed By:
Office of Technology Innovation & Acquisition (OTIA)
Operational Integration and Analysis Directorate (OIAD)
1901 South Bell Street
Arlington, Virginia 22202

~~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.~~

This Page Left Blank Intentionally

AUTHORITY SIGNATORIES

Submitted by: for (b) (6), (b) (7)(C) 1/10/12
Date
Executive Director (Acting), OIAD

Endorsed by: (b) (6), (b) (7)(C)
Date
Program Manager, Remote Video Surveillance System

Endorsed by: (b) (6), (b) (7)(C) 2·6·12
Date
for: Chief, United States Border Patrol

Endorsed by: (b) (6), (b) (7)(C) 4/20/2012
Date
Component Acquisition Executive

BW FOIA CBP 001938

REVISION HISTORY

Rev	Date	Description

EXECUTIVE SUMMARY

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) represents the front line in the defense of our nation's borders. In support of the CBP 2009-2014 Strategic Plan, the United States Border Patrol (USBP) is tasked with the responsibility of securing the nation's borders against the illegal entry of people and goods between Ports of Entry (POE). To this end, the ultimate goal is deterrence and USBP uses a mix of infrastructure, technology, and personnel to effectively manage land borders. These assets are used to execute the mission functions of predicting illicit activity, detecting and tracking border crossings, identifying and classifying the detections, and responding to and resolving cross border incursions.

The October 2006 Secure Border Initiative (SBI) Mission Need Statement (MNS) documented a number of capability gaps in USBP's ability to execute its mission. To address those gaps, the Arizona Border Surveillance Technology Plan identified a number of mature technologies to be deployed in accordance with local operational needs and constraints. One of the technology alternatives is Remote Video Surveillance Systems (RVSS), (b) (7)(E) [redacted] While existing RVSS have performed relatively well, shortfalls in both effectiveness and suitability combined with vendor obsolescence have generated a requirement for improved (b) (7)(E) [redacted]. This Operational Requirements Document (ORD) defines the operational requirements for the RVSS Program and provides the following information:

- Section 1: States the applicable mission needs and gaps, provides background regarding RVSS, and discusses initial and final operational capabilities.
- Section 2: Discusses the CBP mission functions and how RVSS supports those functions, provides a high level summary of the concept of operations, and defines the high level operational requirements for RVSS.
- Section 3: Defines the effectiveness requirements for RVSS.
- Section 4: Defines the suitability requirements for RVSS.
- Section 5: Summarizes the RVSS Key Performance Parameters (KPPs).

In order to execute the Arizona Border Surveillance Technology Plan and provide a persistent surveillance capability at designated geographical locations by the end of Fiscal Year 2013, CBP is seeking commercial or non-developmental items. Because commercial/non-developmental items may not meet all operational requirements, Table 4 in Appendix 2 prioritizes the requirements to facilitate cost-effectiveness and schedule tradeoffs. Deviations to operational requirements should be coordinated with USBP as described in Appendix 2.

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 PURPOSE 1
1.2 BACKGROUND 2
1.3 INITIAL OPERATIONAL CAPABILITY AND TIMELINE 2
1.4 FULL OPERATIONAL CAPABILITY AND TIMELINE 3

2 MISSION REQUIREMENTS 4

2.1 OPERATIONAL REQUIREMENTS 5
2.2 CONCEPT OF OPERATION 6
2.3 CONCEPT OF SUPPORT 14
2.3.1 MAINTENANCE AND SUPPORT 14
2.3.2 TRAINING 15

3 EFFECTIVENESS REQUIREMENTS 15

3.1 PERSISTENT SURVEILLANCE 15
3.1.1 DETECT AND TRACK 15
3.1.2 IDENTIFICATION AND CLASSIFICATION 17
3.2 COMMAND, CONTROL, COMMUNICATION, COORDINATION AND INTELLIGENCE 18
3.2.1 SYSTEM COMMAND AND CONTROL 18
3.2.2 COMMUNICATION 18
3.2.3 OPERATOR INTERFACE AND TOOLS 18
3.2.4 RESPONSE SUPPORT 20
3.3 DETERRENCE SUPPORT 20
3.4 PREDICT (INTELLIGENCE) AND RESOLVE (REPORTING) SUPPORT 21
3.5 INTEROPERABILITY 21

4 SUITABILITY REQUIREMENTS 22

4.1 DESIGN 22
4.2 AVAILABILITY / RELIABILITY 22
4.3 MAINTAINABILITY 22
4.4 SUPPORTABILITY AND SUSTAINMENT (INTEGRATED LOGISTICS SUPPORT) 23
4.5 SURVIVABILITY 23
4.6 SECURITY 23
4.7 SAFETY 23
4.8 HUMAN FACTORS/HUMAN MACHINE INTERFACE 23
4.9 ENVIRONMENTAL CONSIDERATIONS 24
4.10 TRAINING REQUIREMENTS 24

5 KEY PERFORMANCE PARAMETER SUMMARY 26

ACRONYMS 27

GLOSSARY 29

APPENDIX 1: REFERENCES 32

APPENDIX 2: REQUIREMENTS TRACEABILITY MATRIX 33

1 INTRODUCTION

1.1 PURPOSE

DHS is charged with managing, securing, and controlling the nation's borders with a mission focus of preventing terrorists and terrorist weapons from entering the U.S. CBP represents the front line in the defense 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] In support of mission set #1, USBP has the responsibility of securing the nation's borders against the illegal entry of people and goods between POE. To accomplish this, USBP employs a mix of infrastructure, technology, and personnel to manage the land borders. These three resources are used to execute the mission functions of predicting illicit activity, detecting and tracking illegal border crossings, identifying and classifying the incursions, and responding to and resolving those incursions.

To efficiently and effectively manage the nation's borders, USBP requires Persistent Surveillance and Command, Control, Communication, Coordination and Intelligence[2] (C4I) capabilities. Both enhance overall situational awareness and, coupled with the right mix of manpower and tactical infrastructure, enhance operational effectiveness to counter a dynamic and evolving border threat. However, critical gaps in these capabilities were articulated in the October 2006 SBI Mission Needs Statement (MNS):

1. Detection and Tracking
2. Identification and Classification
3. Situational Awareness

A number of technology approaches, whether air-based, Border Patrol Agent (BPA)-based, or ground-based, can be used in support of these mission needs; each offering distinct advantages depending upon the operational considerations within each Area of Responsibility (AoR). The Arizona Border Surveillance Technology Plan outlines a number of solutions to address these critical capability gaps along the Southwest Border. The plan moves away from a single "system-of-systems" technology approach for monitoring illegal incursions to a suite of different technologies tailored to specific operating areas and needs. The purpose of this document is to define the Operational Requirements and KPPs for the RVSS Program. Unless otherwise noted as "existing RVSS capability," reference to RVSS throughout the remainder of this document refers to the new and upgraded capability. RVSS are defined as (b) (7)(E) [redacted].[3]

The Arizona Border Surveillance Technology Plan is a major change in direction compared to SBI*net*. Where SBI*net* represented an attempt to develop a system that would meet ambitious

[1] CBP's Missions, Goals, and Priorities, FY2011-2013

[2] C4I capability is referenced from the Foundational Operational Capabilities, which are defined in the USBP Operational Requirements-Based Budget Process Tool.

[3] USBP Memorandum OBP40/11.3-C, Surveillance System Definitions

requirements, including a requirement for (b) (7)(E) [redacted] the new plan is much more modest. It consists of a tailored [redacted] (b) (7)(E) [redacted]. There is no initial effort intended to (b) (7)(E) [redacted]. Over time, as personnel become more familiar with the operations and potential use of these systems, their experience may provide a basis for future enhancements, increased performance, and integration. However, for now, the intent is to avoid "over-shooting" mission needs at all costs, and deliver low-risk systems that can give immediate support to the overall border security mission.

Within the new technology plan, one of the stand-alone systems is RVSS. Since the RVSS will be non-developmental, Government Off-the-Shelf (GOTS), or Commercial Off-the-Shelf (COTS), CBP will select from among commercial offerings which represent the best balance among performance and cost trade-offs. This ORD, therefore, is a framework for that trade-off, but it does not represent (nor is it intended to represent) a firm set of requirements that must be met by the eventual RVSS. In fact, this ORD will be supplemented to record and reflect the final acquisition decision that results from the trade-offs. Put another way, the RVSS will be a "capability-based" procurement. This ORD reflects the capabilities that are of general interest for RVSS.

As part of a layered approach augmenting other surveillance capabilities including (b) (7)(E) [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted], the upgraded RVSS capability will help enable Persistent Surveillance and C4I capabilities to address current mission needs and mitigate capability gaps. Note – (b) (7)(E) [redacted].

1.2 Background

CBP relies on highly trained and dedicated BPAs to maintain the security of the nation's borders and to safeguard those borders against illegal incursions. The introduction of new technologies has been an integral component in successfully accomplishing mission objectives. The existing RVSS consist of [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] (b) (7)(E) Existing RVSS provide BPAs with enhanced situational awareness which aids their ability to respond to border incursions and also increases agent/officer safety. However, a recent assessment of existing Arizona RVSS conducted by the CBP Fixed and Mobile Surveillance System Integrated Product Team (IPT) has found the current technology and operator interfaces to be antiquated and obsolete. An upgrade of existing RVSS capabilities and extension of deployed coverage is required in order to provide the Persistent Surveillance and C4I capabilities required by the BPAs to respond to the evolving threats.

1.3 Initial Operational Capability and Timeline

CBP is seeking commercial or non-developmental items that provide a persistent surveillance capability to enable the detection, tracking, identification, and classification of illegal entries in rural, urban, and remote areas. Because it is unlikely that commercial or non-developmental items can meet all requirements in Sections 3 and 4 of this ORD, USBP has prioritized the

requirements in Table 4, Appendix 2, to facilitate cost-effectiveness and schedule tradeoffs. The objective timeline for the initial operational capability (IOC) is planned for Fiscal Year 2013.

IOC is defined as the following geographical segment (pending final USBP analysis):

(b) (7)(E) AoR – install one new RVSS that includes:
- One Command and Control (C2) facility
- New RVSS units[4]
- New (b) (7)(E) and communication capability on existing towers

1.4 Full Operational Capability and Timeline

The operational requirements for the RVSS Upgrade Program Full Operational Capability (FOC) are the same as the IOC requirements. FOC timeline is estimated for completion in Fiscal Year 2013 and is defined as the following additional geographical segments (pending final USBP analysis):

- (b) (7)(E) AoR – install one new RVSS that includes:
  - One RVSS C2 facility
  - New RVSS units
  - New (b) (7)(E) and communication capability on existing towers
- (b) (7)(E) AoR – install one new RVSS that includes:
  - One RVSS C2 facility
  - New RVSS (b) (7)(E) and communication capability on existing towers
  - New RVSS (b) (7)(E) on relocated towers

(b) (7)(E) AoR – install one new RVSS that includes:
- One RVSS C2 facility
- New RVSS units
- New RVSS (b) (7)(E) and communication capability on existing towers

- (b) (7)(E) AoR – install one new RVSS that includes:
  - One RVSS C2 facility
  - New RVSS (b) (7)(E) and communication capability on an existing tower
- (b) (7)(E) AoR
  - One RVSS C2 facility
  - New RVSS units
  - New RVSS (b) (7)(E) and communication capability on existing tower installations
  - New RVSS (b) (7)(E) on relocated towers

While FOC is currently limited to the Arizona border, operational requirements also consider the environments along the remainder of the Southern, Northern, and Coastal borders in anticipation that upgraded RVSS will be needed beyond Arizona.

[4] An RVSS unit consists of the platform, sub-platform and (b) (7)(E)

2 MISSION REQUIREMENTS

Objective 1.1 in CBP's 2009-2014 Strategic 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 key mission elements are defined below in Table 1.

Table 1 - CBP Mission Elements

Mission Element	Definition
(b) (7)(E)	
(b) (7)(E)	

To successfully execute these mission elements, USBP requires a number of operational capabilities that include:

- Persistent Surveillance Capability: the ability to continuously detect, track, identify and classify border incursions 24 hours a day, 7 days a week (24/7) in targeted areas under expected weather, terrain, vegetation and lighting conditions[5]
- C4I Capability: the ability to collect and analyze information, exchange information and intelligence, allocate and control resources according to operational needs, and make informed operational command decisions in support of the mission
- Sustainment and Support Capability: the ability to maintain and sustain the surveillance systems in accordance with mission needs and operational requirements

[5] Border environments are described in detail in the Secure Border Initiative Design Reference Mission Document.

Persistent Surveillance is a critical capability needed to manage border areas exploited by the threat. Short, Medium, and Long Range persistent surveillance, coupled with C4I capabilities, enables USBP to efficiently and effectively manage rural, urban, and remote Areas of Interest (AoI).[6] Historical data demonstrates how border threats adapt quickly to counter CBP operations. Accordingly, USBP leverages mobile surveillance capabilities to the greatest extent possible because of the ability to redeploy these resources as border threats are deflected or otherwise influenced to change their routes of operation at and along the border. However, these systems can only be deployed where sufficient (b) (7)(E) [redacted]. Furthermore, these systems are (b) (7)(E) [redacted]

RVSS units (comprised of the individual tower and (b) (7)(E) [redacted]) provide a long range surveillance alternative with additional height that enables better coverage of a surveillance area.[7] When multiple RVSS units are integrated into a command and control center, RVSS enables USBP to monitor very large Areas of Coverage (AoC)[8] within an AoI with fewer agent and equipment resources. RVSS contribute to situational awareness, agent safety, and are a preferred solution in certain rural, urban, and remote areas that are (b) (7)(E) [redacted] and/or where USBP has a need for long term/permanent persistent surveillance because of a persistent threat and or vulnerability. As one part of a multi-layered approach to border surveillance, RVSS will contribute to both the persistent surveillance and C4I capabilities needed by USBP.

To reiterate – with respect to the RVSS program, these requirements are a framework for evaluating and selecting among non-developmental, GOTS, or COTS systems. The actual procurement will be capability-based and reflect appropriate trade-offs among performance and cost. As indicated elsewhere in this document, all performance requirements are prioritized and may be waived to reflect the results of the capability-based procurement, consistent with the terms of this ORD.

2.1 Operational Requirements

USBP requires Persistent Surveillance of a targeted AoI 24/7 to enable the detection, tracking, identification, and classification of traffic, as follows:

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

[6] An AoI is defined as a targeted area within a USBP Station's AoR that requires surveillance due to the risk level associated with the border threat exploitation. For the purposes of this document, the AoI refers to the total operational area where one or more RVSS units are the preferred surveillance solution. Note – there may be more than one AoI within an AoR, so an RVSS may cover more than one AoI.

[7] The "surveillance area" is defined as the area within which a single RVSS unit is capable of detecting, tracking, identifying and classifying illegal incursions.

[8] The AoC is defined as the resulting area, considering installation location of all RVSS units, view shed and line of sight obstructions, etc., within which USBP can successfully conduct surveillance activities using the RVSS. When used in a broader context, AoC can also refer to the coverage provided by a combination of surveillance systems.

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

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

The operational requirements articulated above are high level. The specific RVSS operational requirements that support these needs are contained in Sections 3 and 4 to further quantify the RVSS features and attributes necessary to achieve these operational needs. Table 4 in Appendix 2 summarizes these requirements and provides traceability to the mission elements and capabilities. Because the operational needs, tactics, and geographical constraints vary widely across the AoI where RVSS will be used, several of the effectiveness requirements focus on the level of capability expected from a given surveillance subsystem (i.e. installation structure and (b) (7)(E) such as a single RVSS tower (b) (7)(E) (b) (7)(E)

2.2 Concept of Operation

Figure 1 illustrates notionally how USBP employs a layered, defense-in-depth surveillance approach to manage land borders between POE to provide the most effective balance between capability and cost. This layered approach will incorporate fixed surveillance capabilities including RVSS, IFT, (b) (7)(E) and SBI*net* Block 1 towers, coupled with mobile surveillance capabilities including (b) (7)(E) (b) (7)(E) , to augment natural and fixed barriers in providing USBP the comprehensive capabilities needed to effectively manage the border. The *Arizona Border Surveillance Technology Plan Concept of Operations Document* provides additional details on the layered approach and the employment of these technologies. Specific technology implementations will be tailored for each specific environment along the border, such as threat tactics, terrain/topography (flat/rugged/maritime), weather (visibility, winds, etc), human development (urban, rural, and remote), operational considerations and tactics, etc.

(b) (7)(E)

Along with IFT, RVSS technologies are one of the preferred solutions in AoI where CBP has a need for long term/permanent persistent surveillance because of a persistent threat or threat potential.

Each upgraded RVSS, displayed notionally in Figure 2, will consist of (b) (7)(E)

(b) (7)(E)

AoR. Each RVSS unit will consist of the necessary (b) (7)(E), and, as applicable, the necessary supporting structure. Supporting power and data communications sub-systems may also be included as a part of the upgraded RVSS as necessary. The operator interface subsystem (b) (7)(E) will be installed in CBP Sector, Station, and/or Forward Operating Base (FOB) facilities.

(b) (7)(E)

(b) (7)(E)

The numbers and capabilities of RVSS deployed within each CBP sector will vary by geography and operational needs. In the urban environment, USBP relies heavily on RVSS to monitor and thus requires (b) (7)(E) to the greatest extent practical. (b) (7)(E)

(b) (7)(E)

The requirements for range vary depending on threat and deployment location. For example, an urban AoI may be within a (b) (7)(E) [redacted] Rural and remote AoIs also have different deployment needs – (b) (7)(E) [redacted] Regardless of whether the AoI is in an urban, rural, or remote environment, the final RVSS unit lay down should maximize coverage of the AoI while minimizing the number of fixed site installations because of land ownership and environmental constraints prevalent along the U.S. border.

(b) (7)(E)

RVSS will support accomplishment of the following USBP functions and tasks:

(b) (7)(E)

An RVSS Operator will accomplish the following tasks:

- Direct and adjust the sensor FOV as necessary to monitor the AoC for IoI(s)
- (b) (7)(E) [redacted]
- Coordinate control of the RVSS units with other operators as necessary

- (b) (7)(E)
- Prioritize detections for further investigation
- (b) (7)(E)
- Direct and adjust the surveillance subsystems as necessary to track IoI and support interdiction
- (b) (7)(E)
- (b) (7)(E)
- Save video or imagery as required to investigate IoIs or support follow-on law enforcement activities
- Disposition of IoI, including filing of any required reports and log entries, annotation and archiving of selected imagery, etc
- Monitor the system for critical failures and report them in accordance with local procedures

In accordance with the CBP AoA and ongoing CBP analysis of technology deployment options within the various border sectors, CBP will both replace aging RVSS with upgraded RVSS as well as deploy the upgraded RVSS in new locations as part of a tailored, layered approach to improve situational awareness along the border. During the transition from legacy to upgraded RVSS configurations, operational impacts and infrastructure requirements should be minimized. The incorporation of open architecture and scalability to allow potential interoperability and/or integration with future border surveillance systems is desired to facilitate future expansion and minimize the equipment's logistical footprint.

For additional information on the concept of operations and employment of RVSS as a part of a layered approach to manage the Arizona Border, see the *Arizona Border Surveillance Technology Plan Concept of Operations Document*.

2.2.1 Climate

Climates along the U.S. borders are described by Sector in the *Secure Border Initiative Design Reference Mission, Version 1.0, May 2010*.

2.2.2 Operational Scenarios

The following scenarios provide examples of the activities BPAs will perform to execute their missions and how they will utilize the RVSS capability.

2.2.2.1 Scenario 1 – (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

2.2.2.2 Scenario 2 – (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

[redacted]

2.2.2.3 Scenario 3 - (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

2.2.2.4 Scenario 4 – (b) (7)(E)

(b) (7)(E)

BW FOIA CBP 001954

(b) (7)(E)

2.3 CONCEPT OF SUPPORT

2.3.1 MAINTENANCE AND SUPPORT

The RVSS will perform mission-critical functions in support of 24/7 operations. As such, maintenance and sustainment support is required to minimize system down time associated with scheduled and unscheduled maintenance.

The maintenance approach will employ two levels of maintenance: organizational and depot. The system will (b) (7)(E) . Mission critical failures include any condition or conditions that prevent the system from performing the mission elements it is designed to perform. The time that the system is unavailable due to a mission critical failure is considered down time, and includes both logistics delay time (time between the failure report and the maintainer's arrival on site with replacement parts) and the actual time to repair the system (time for fault isolation, line replaceable unit (LRU) replacement and system checkout). Once a mission critical failure has been identified, the operator will contact a helpdesk for assistance with troubleshooting the problem. If the problem is not resolved, authorized technicians will perform site repairs on the assets. (b) (7)(E)

Appropriate measures will be documented and used to assess the following metrics: Mean Time Between Critical Failures (MTBCF), Mean Time To Repair (MTTR) the system and the failed LRU, Mean Logistics Delay Time (MLDT), Mean Down Time (MDT)[10], operational availability

[10] MDT is the sum of MTTR and MLDT.