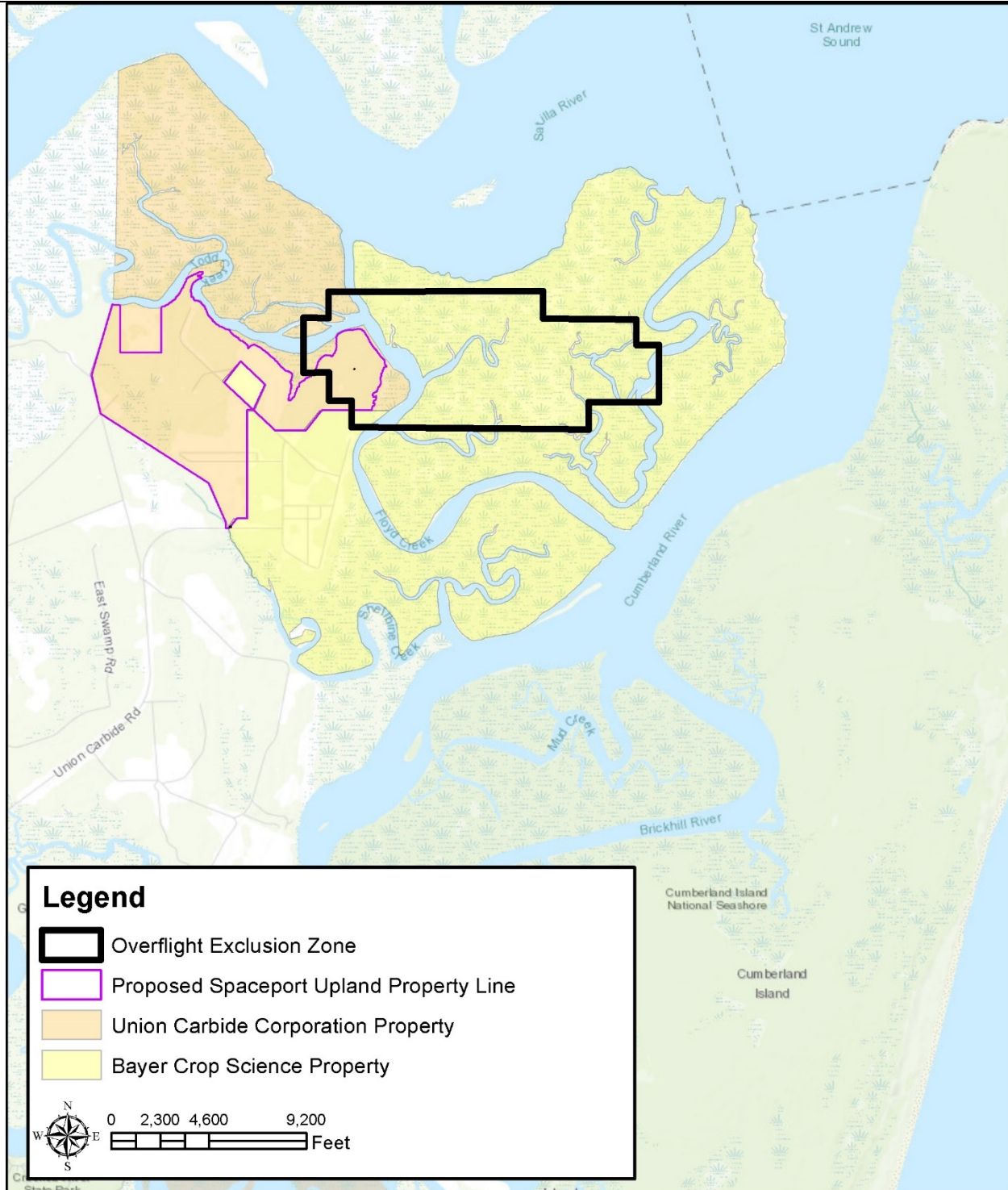


### Spaceport Camden – Launch Site Location Review

GORA EXEMPT – PROPRIETARY & TRADE SECRETS – REAL PROPERTY ACQUISITION EVAL ANALYSIS – NO PUBLIC RELEASE  
FOIA & GORA EXEMPT – Contains Technical Data that may be controlled pursuant to the Arms Export Control Act (AECA),  
22 U.S.C. 2778, as implemented in the International Traffic in Arms Regulations (ITAR), 22 CFR § 120 – 130 – NO PUBLIC RELEASE



**Exhibit 26. Simplified OEZ for the Small Representative Launch Vehicle – 100-Degrees Azimuth  
(From True North) Trajectory from Spaceport Camden**

## 5 14 CFR § 420.27 – Launch site location review—information requirements.

Paragraph 420.27 defines the LSOL information requirements for the review of a launch site location. These information requirements are defined as follows:

*An applicant shall provide the following launch site location review information in its application:*

- (a) A map or maps showing the location of each launch point proposed, and the flight azimuth, IIP, flight corridor, and each impact range and impact dispersion area for each launch point;*
- (b) Each launch vehicle type and any launch vehicle class proposed for each launch point;*
- (c) Trajectory data;*
- (d) Wind data, including each month and any percent wind data used in the analysis;*
- (e) Any launch vehicle apogee used in the analysis;*
- (f) Each populated area located within a flight corridor or impact dispersion area;*
- (g) The estimated casualty expectancy calculated for each populated area within a flight corridor or impact dispersion area;*
- (h) The effective casualty areas used in the analysis;*
- (i) The estimated casualty expectancy for each flight corridor or set of impact dispersion areas; and*
- (j) If populated areas are located within an overflight exclusion zone, a demonstration that there are times when the public is not present or that the applicant has an agreement in place to evacuate the public from the overflight exclusion zone during a launch.*

This information has been provided within this LSLR and its companion electronic files. Exhibit 27 (below) cross references these information requirements with the specific location within this LSLR where the information is found.

INFORMATION REQUIREMENT	LOCATION IN LSLR
(a) A map or maps showing the location of each launch point proposed, and the flight azimuth, IIP, flight corridor, and each impact range and impact dispersion area for each launch point;	1.1, 1.3, 2.4, 4.1.1, 4.2.2
(b) Each launch vehicle type and any launch vehicle class proposed for each launch point;	1.2, 1.4
(c) Trajectory data;	4.1.1, 4.2.2
(d) Wind data, including each month and any percent wind data used in the analysis;	4.1.2
(e) Any launch vehicle apogee used in the analysis;	4.1.1
(f) Each populated area located within a flight corridor or impact dispersion area;	4.1.3, 4.3
(g) The estimated casualty expectancy calculated for each populated area within a flight corridor or impact dispersion area;	4, 4.2.3
(h) The effective casualty areas used in the analysis;	4.1, 4.2.1, 4.3
(i) The estimated casualty expectancy for each flight corridor or set of impact dispersion areas; and	4.2, 4.2.3
(j) If populated areas are located within an overflight exclusion zone, a demonstration that there are times when the public is not present or that the applicant has an agreement in place to evacuate the public from the overflight exclusion zone during a launch.	Not Applicable (see 4.3)

**Exhibit 27. Cross Reference of 14 CFR § 420.27 Information Requirements vs Location in LSLR**

**6      14 CFR § 420.29 – Launch site location review for unproven launch vehicles.**

Paragraph 420.29 defines the launch site location review requirements for unproven launch vehicles. Specifically, the requirements are:

*An applicant for a license to operate a launch site for an unproven launch vehicle shall provide a clear and convincing demonstration that its proposed launch site location provides an equivalent level of safety to that required by this part.*

Spaceport Camden is not applying for these permissions in this application.

**7      14 CFR §417.107(b)(2) – Flight safety, Public risk criteria, Individual risk**

Although provisions of Part 417 are generally not required to be met by an applicant for a LSOL, Spaceport Camden had this analysis completed to demonstrate to potential launch operators that meeting this requirement was likely, given the assumptions made for the analysis. Only later after the initial submission of this information as supplemental in this Section 7 did FAA/AST require this information for the Spaceport Camden LSOL application (FAA/AST, Kenneth Wong, letter of 12 February 2019).

Paragraph 417.107(b)(2) defines the requirement levied on launch operators to demonstrate the risk to any individual member of the public is highly remote for each hazard. Specifically, the requirements are:

*A launch operator may initiate flight only if the risk to any individual member of the public does not exceed a casualty expectation of  $1 \times 10^{-6}$  for each hazard.<sup>12</sup>*

This section includes a description of the methodology used in this analysis, the assumptions made, and the outcomes of the evaluations. This analysis was performed by The Aerospace Corporation using their Ec and individual risk tools that are proprietary, contain trade secrets, are believed to contain Technical Data that is controlled under ITAR, and is believed to constitute a Defense Service under the ITAR. It is considered that this methodology and the assumptions result in a conservative approach to individual risk evaluation, as described more fully below.

**7.1      Methodology – individual risk.**

The individual risk calculation is used to determine the highest risk of casualty to any particular person. The Aerospace Corporation tool calculates the individual risk for a particular  $i^{\text{th}}$  population grid cell as follows:

(b) (4)



---

<sup>12</sup> Revised as per Federal Register, Volume 81, Number 139, Wednesday July 20, 2016, pages 47017-47027.

The highest individual risk for the trajectory, overall population cells, is then given by:



For the Spaceport Camden analysis, the Monte Carlo technique used to determine the impact probabilities at every cell for each failure mode, showed that very few, if any, explosive impacts occurred in populated grid cells. As a result, while the effective casualty area for an explosive impact is quite large, the highest individual risk remains acceptable.

## 7.2 Assumptions

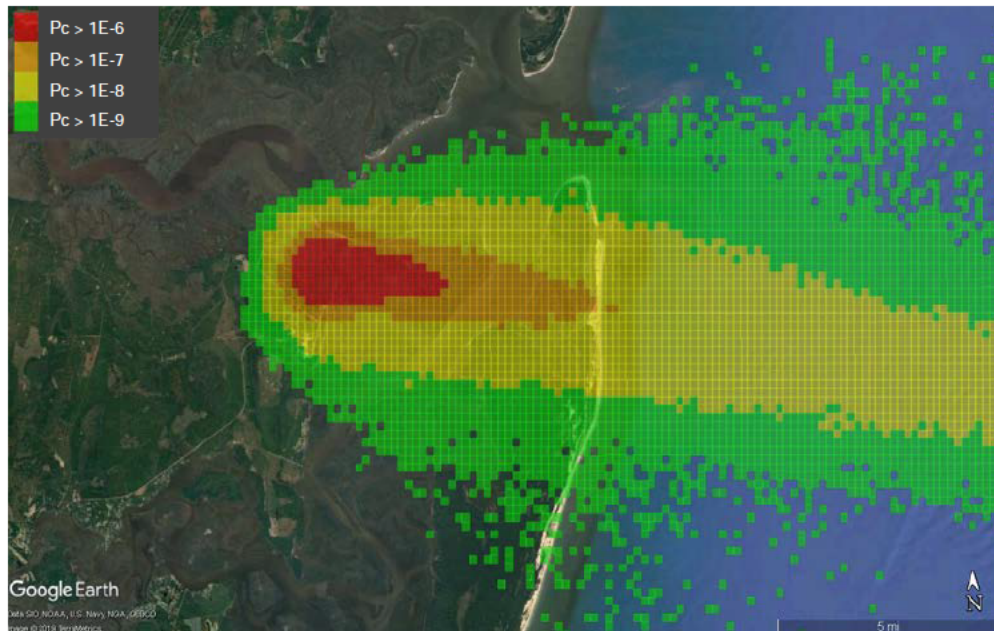
The assumptions used for the analysis included small launcher parameters that were defined earlier in this Appendix in the Ec analyses. This includes allocating 10% probability of failure to the first stage vehicle, and adding population to the islands and the previously identified 55 habitable vacation cottages on Cumberland Island and Little Cumberland Island.

## 7.3 Outcomes / Results

For the small representative launch vehicle the following individual risk Ec values were calculated, given the previously discussed conservative assumptions.

100-degree azimuth trajectory: Fly out =  $0.05 \times 10^{-6}$

The individual risk calculation grid for the small representative launcher is shown in Exhibit 28 (below). The red area is the area represented by grid squares where the  $1 \times 10^{-6}$  threshold was exceeded and hence is considered a “land hazard area” pursuant to 14 CFR 417. As can be seen, this area only reaches into the marsh and does not reach the Cumberland River (Intracoastal Waterway), Cumberland Island or Little Cumberland Island.



**Exhibit 28.** Individual Risk Grid Image for 100-degree trajectory launch of Small Launcher



**Attachment 3**

**USCG / Spaceport Camden Draft Letter of Agreement (Signed)**



# **U.S. Coast Guard Letter of Agreement**

Signed

As of 12 June 2019



**LETTER OF AGREEMENT**  
**between**  
**CAMDEN COUNTY, GA**  
**and**  
**UNITED STATES COAST GUARD**  
**SEVENTH DISTRICT**

**SUBJECT: Operations at Spaceport Camden, Camden County, Georgia**

- I. **PARTIES:** The parties to this agreement are the United States Coast Guard (USCG), Seventh District, (D7) and Camden County Board of Commissioners, Georgia (Camden County).
- II. **AUTHORITY:** The USCG's authority to enter into this Agreement can be found in the following sources: 14 United States Code (U.S.C.) § 93(a)(20), 14 U.S.C. §701. As a recognized political subdivision of the State of Georgia as defined in the Constitution of the State of Georgia, effective July 1, 1983, Camden County is authorized to enter into governmental agreements pursuant to Article IX, section 1, Paragraph 1 thereof, and O.C.G.A. 36-34-2(5).
- III. **BACKGROUND:** Camden County intends to operate a commercial space launch site called Spaceport Camden (SC) for use by vertical launch vehicle operators for the orbital and suborbital launch of small to medium-large, liquid propellant launch vehicles. Launch operations would include preparatory activities to ready and test launch vehicles and systems, including mission rehearsals and static tests, and for any first-stage landings on the space launch site or returns to the launch site after landing on a barge located approximately 200 to 300 miles offshore in the Atlantic Ocean. The USCG has the responsibility to protect public health, safety of property, safe navigation, and national security in the maritime domain, to include during launch or reentry activities associated with space transportation.
- IV. **PURPOSE:** As required under Title 14, Code of Federal Regulations (CFR) §420, this agreement between Camden County and D7 provides procedures for the issuance of Broadcast and/or Local Notice to Mariners prior to a launch operation, as well as any other conditions deemed necessary by the Coast Guard to protect public health and safety. This agreement does not cover air traffic control procedures, nor does it cover specific notifications necessary for operation of specific launch vehicles, as these are covered in separate agreements required as part of a Federal Aviation Administration (FAA) Launch Vehicle Operator License.
- V. **SCOPE:** This Agreement is specific to the site location listed above, to include proposed operations taking place there, and is designed to detail USCG conditions, responsibilities, and coordination procedures for preflight, flight, and post-flight operations. Procedures defined in this Agreement are to be part of and supplemental to all Launch Site Operator license requirements and are in no way intended to circumvent the terms and conditions

contained in any license issued. Procedures used for actual flight operations are subject to further coordination by vehicle operators during the development of a separate Launch Vehicle Operator License application. This Agreement is subject to compliance monitoring by FAA Office of Commercial Space Transportation (AST).

## **VI. DEFINITIONS:**

- A. Captain of the Port (COTP): Captains of the Port and their representatives enforce port safety and security and marine environmental protection regulations within their respective areas of responsibility, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities; anchorages; security zones; safety zones; regulated navigation areas; deepwater ports; water pollution; and ports and waterways safety. For the purposes of this agreement, USCG Marine Safety Unit Savannah (MSU Savannah) is the COTP under whose authority Spaceport Camden's launch operations primarily fall.
- B. Limited Access Area (LAA): Tool used to control movement of marine traffic and limit access to all or a portion of the waterway in order to provide safety and security for mariners, vessels and maritime critical infrastructure, and manage the use of navigable waterways for commerce and environmental protection. LAA's could be a tool used to mitigate risks identified through a Navigation Safety Risk Assessment (NSRA).
- C. Local U.S. Coast Guard District: A Coast Guard District Commander is in command of a Coast Guard District and the District Commander's office may be referred to as a Coast Guard District Office. For the purposes of this agreement, the "Local U.S. Coast Guard District" refers to the Seventh Coast Guard District in Miami, Florida.
- D. Navigation Safety Risk Assessment (NSRA): Tool used by the USCG COTP when preparing input for a permitting agency regarding port or waterway safety issues associated with a project located on, over, or near the navigable waters of the United States. The assessment helps the COTP identify potential navigation risks and is the basis of any recommendation to the permitting agency.
- E. Navigable Waters of the U.S. (navigable waterway): As defined in 33 CFR 2.36, Navigable Waters refers to the Territorial seas of the United States (all waters seaward to 12nm), internal waters of the United States that are subject to tidal influence, and internal waters of the United States that are not subject to tidal influence, but that may be used for substantial interstate or foreign commerce.
- F. Broadcast Notice to Mariners (BNM): Broadcast Notice to Mariners is the method by which important navigation safety information is disseminated in the most expedient manner. Two agencies within the United States, the USCG and the National Geospatial-Intelligence Agency (NGA) are responsible for broadcasting navigation information. Each agency has a particular geographic area of responsibility.



- G. Local Notice to Mariners (LNM): The Local Notice to Mariners is the USCG's primary means for disseminating navigation safety information concerning aids to navigation, hazards to navigation, and other items of interest to mariners navigating the waters of the United States, its territories, and possessions. Each District Commander is responsible for issuing a Local Notice to Mariners each week containing information that contributes to navigation safety and maritime security within the boundaries of the District.
- H. United States Coast Guard Local Authority: For the purposes of this agreement, the local Coast Guard authority refers to MSU Savannah.
- I. Vertical Launch Vehicle: A vehicle built to operate in, or place a payload in, outer space or a suborbital rocket, that launches vertically from a launch pad into space without assistance from an aircraft.

## **VII. RESPONSIBILITIES:**

### **A. Camden County agrees to the following:**

#### **1. Scheduling and Notification Activities:**

- a) Provide D7(dpw) an annual launch schedule forecast for the next federal fiscal year by 30 September each year.
- b) Submit launch information to D7(dpw), to request a LNM article no later than 30 days prior to scheduled launch. Launch information should include the following:
  - 1) Operation Number;
  - 2) Vehicle type and launch description;
  - 3) Primary and secondary launch date and time in local and GMT;
  - 4) Launch Hazard Areas, perimeter coordinates in degrees, minutes, and seconds to three decimal places, if applicable.
- c) No later than five (5) days prior to launch activity, Camden County shall:
  - 1) Contact MSU Savannah to request a BNM with launch information and any other specific information needed by mariners;
  - 2) Contact D7 (dpw) to confirm launch information for the LNM and to request broadcast of NAVTEX with launch hazard information for launch activities occurring over water up 150 nautical miles offshore;
  - 3) Contact NGA to request Navigation Area IV warning notifications for launch activities occurring over water from 150 nautical miles offshore to deep-ocean.

#### **2. Limited Access Areas:**

- a) NSRA: Submit a completed NSRA to the USCG COTP for use in identifying potential navigation risks with SC on or before ninety (90) days from the effective date of this agreement.

- b) Based on evaluation of risks assessed in the NSRA, request resumption of rulemaking in order to establish an LAA no later than 60 days prior to anticipated need.

B. D7 agrees to the following:

1. Scheduling and Notification Activities:

- a) Review annual forecast of scheduled launches and provisions of this agreement each year;
- b) Publish launch information 30 days prior to launch in the Local Notice to Mariners;
- c) Broadcast NAVTEX with launch information 5 days prior to launch;
- d) Fulfill any other statutory responsibility pertaining to USCG jurisdiction and authorities.
- e) Consult with Camden County on all matters related to navigation safety pertaining to commercial space transportation.

2. Limited Access Areas:

- a) D7(dpw) will coordinate the completion of a formal NSRA in accordance with Coast Guard policy separate from this agreement.

**VIII. POINTS OF CONTACT:** The primary points of contact for this Agreement shall be the D7(dpw), USCG Marine Safety Unit (MSU) Savannah, and the Administrator of Camden County. Specific points of contact are included in Appendix A.

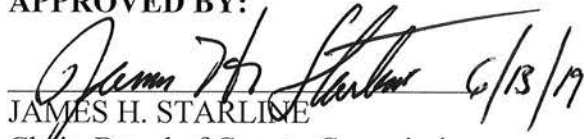
**IX. OTHER PROVISIONS:**


- A. Nothing in this agreement is intended to conflict with current law or regulation or the directives of the USCG, Department of Homeland Security, the Department of Transportation, or the State of Georgia. If the terms of this Agreement are inconsistent with existing directives of these agencies, then those portions of this Agreement which are determined to be inconsistent shall be invalid, but the remaining terms and conditions of this Agreement not so affected shall remain in full force and effect.
- B. This Agreement does not create any right or benefit, substantive or procedural, enforceable by law or equity by persons who are not a party to this agreement, against the USCG or Camden County, their officers or employees, or any other person.

- C. Each Party shall implement procedures to carry out their respective responsibilities under this Agreement in accordance with their respective departmental policies and procedures. This Agreement does not and should not be construed as a commitment, obligation, or transfer of funds. Should the transfer or obligation of funds become necessary in the future, both Parties agree that appropriate subordinate agreements will be executed in writing as necessary, in accordance with each agency's fiscal and contracting laws and regulations, including proper administrative review prior to obligation of those funds. Reimbursable expenses are charged at rates as provided by the USCG Reimbursable Standard Rates Commandant Instruction 7310.1S.
- D. Camden County or the SC Senior Manager will immediately notify the National Response Center, MSU Savannah, and the D7 Command Center in the event of a launch site accident adjacent to or affecting any navigable waterway.
- E. As specified in Paragraph VII.A.1., should Camden County fail to submit a final NSRA acceptable to the USCG within the identified time period, the USCG will have the option to terminate this Agreement by written notice to Camden County.

- X. **EFFECTIVE:** This Agreement shall become effective upon the date of signature by both approving officials for the parties.
- XI. **MODIFICATION:** This Agreement may be modified upon the mutual written consent of the parties. This Agreement shall be reviewed by the parties annually to determine the need for modification.
- XII. **TERMINATION:** This Agreement shall remain in full force and effect unless and until revoked in writing by either party. Either party, upon thirty (30) days written notice to the other party, may terminate this Agreement.

APPROVED BY:

  
JAMES H. STARLINE  
Chair, Board of County Commissioners  
Camden County Georgia

  
PETER J. BROWN  
Rear Admiral, U. S. Coast Guard,  
Commander, Seventh Coast Guard District

JUN 12 2019

Appendix (A) Specific Points of Contact  
Appendix (B) Conceptual Routes of Flight

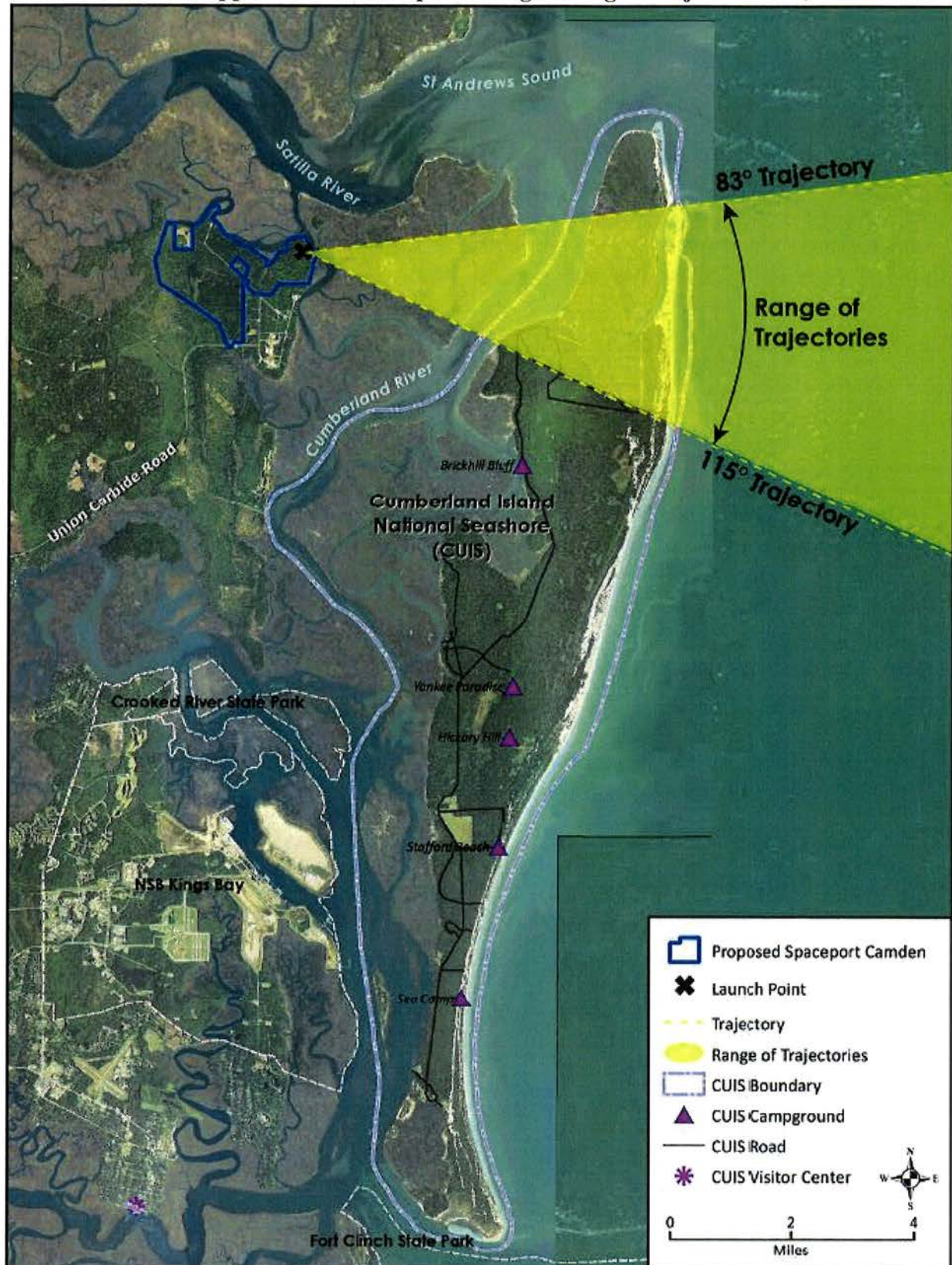
**AGREEMENT**  
**Appendix A – Specific Points of Contact**

<b>OFFICE</b>	<b>NUMBER</b>	<b>RESPONSIBILITY</b>
Camden County Administrator	912-510-0464	Launch Facility Development and Operations Coordination
Spaceport Camden Operations Coordinator	TBD	General Operations Coordination
USCG D7(dpw) LNM Editor D07-SMB-D7- LNM@uscg.mil	305-415-6752	Distribution/publication of Local Notice to Mariners.
USCG Marine Safety Unit Savannah, Command Duty Officer	912-247-0073	Broadcast Notice to Mariners
USCG Marine Safety Unit Savannah	912-247-0073	Incident and recovery coordination
USCG Seventh District Command Center	305-415-6800	Incident and recovery coordination
USCG D7(dpw) MP&I	305-415-6750	Navigation Safety Risk Assessment Coordination



# AGREEMENT

## Appendix B – Conceptual Range of Flight Trajectories







**Attachment 4**

**FAA ATO / Spaceport Camden Letter of Agreement (Signed)**



**FAA**

**Air Traffic**

**(Multi-Party)**

**Letter of Agreement**

FINAL

Effective 12 February 2018

---

**JACKSONVILLE CENTER, JACKSONVILLE TRACON, FLEET AREA CONTROL AND  
SURVEILLANCE FACILITY JACKSONVILLE, AIR TRAFFIC CONTROL SYSTEM  
COMMAND CENTER, AND CAMDEN COUNTY BOARD OF COMMISSIONERS, CAMDEN  
COUNTY, GEORGIA**

**LETTER OF AGREEMENT**

**EFFECTIVE: 12 February 2018**

**SUBJECT: Spaceport Camden Site Support**

---

**1. PURPOSE.** The Camden County Board of Commissioners plan to operate a commercial Space launch site in Camden County, Georgia called Spaceport Camden. This agreement between Jacksonville Center, Jacksonville TRACON, Fleet Area Control and Surveillance Facility Jacksonville, Air Traffic Control System Command Center and Camden County Board of Commissioners, Camden County, GA establishes the overall framework to support Spaceport Camden in anticipation of acquiring licensed operators who will perform sanctioned launch operations into the National Airspace System.

**2. CANCELLATION.** This Letter of Agreement will remain in effect while Spaceport Camden maintains proper licensing and/or until cancellation is requested by any signatory.

**3. SCOPE.** This agreement applies to launch site operations at Spaceport Camden. Issuance of a license to operate a launch site does not relieve a licensee of its obligation to comply with any other laws or regulations; nor does it confer any proprietary, property, or exclusive right in the use of airspace or outer space (reference CFR 420.41).

**4. RESPONSIBILITIES.** At such time as a vehicle operator applies for a license or permit to operate from Camden Spaceport, all parties named within this letter of agreement will work collaboratively to develop the following:

- a. Procedures for notification and scheduling of operations, to include procedures for the issuance of Notices to Airmen and SAA access.
- b. Plans for communication between the operator and the FAA as necessary, before, during, and after a scheduled operation.
- c. Plans and procedures for cancellations, contingencies and emergencies.
- d. Plans and procedures for any other measures deemed necessary by the FAA to ensure public health and safety.


**5. ATTACHMENTS.**

- a. Attachment 1 - Depiction of Spaceport Camden
- b. Attachment 2 – Points of Contact

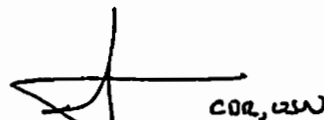
**JACKSONVILLE CENTER, JACKSONVILLE TRACON, FLEET AREA CONTROL AND  
SURVEILLANCE FACILITY JACKSONVILLE, AIR TRAFFIC CONTROL SYSTEM  
COMMAND CENTER, AND CAMDEN COUNTY BOARD OF COMMISSIONERS, CAMDEN  
COUNTY, GEORGIA**

**LETTER OF AGREEMENT**

**6. SIGNATURES.**



**Al Serrano (A)**  
**Air Traffic Manager**  
**Jacksonville Center**

  
CDR, USN

**Dustin B. Hendrix, CDR**  
**Commanding Officer**  
**FACSFACJAX**

\_\_\_\_\_  
**Sonya Busch**  
**Air Traffic Manager**  
**Jacksonville TRACON**

\_\_\_\_\_  
**Jimmy H. Starline, Chairman**  
**Camden County Board of Commissioners**  
**Camden County, GA**

**ROBERT J**  
**MCGRATH JR**

Digitally signed by  
ROBERT J MCGRATH JR  
Date: 2018.02.06  
09:29:26 -05'00'

**Robert McGrath**  
**FAA Air Traffic Representative**  
**Eastern Service Area**

\_\_\_\_\_  
**Virginia Boyle (A)**  
**Air Traffic Manager**  
**Air Traffic Control System Command Center**

JACKSONVILLE CENTER, JACKSONVILLE TRACON, FLEET AREA CONTROL AND  
SURVEILLANCE FACILITY JACKSONVILLE, AIR TRAFFIC CONTROL SYSTEM  
COMMAND CENTER, AND CAMDEN COUNTY BOARD OF COMMISSIONERS, CAMDEN  
COUNTY, GEORGIA

LETTER OF AGREEMENT

6. SIGNATURES.

  
\_\_\_\_\_  
Al Serrano (A)  
Air Traffic Manager  
Jacksonville Center

\_\_\_\_\_  
Dustin B. Hendrix, CDR  
Commanding Officer  
FACSFACJAX

  
\_\_\_\_\_  
Sonya Busch  
Air Traffic Manager  
Jacksonville TRACON

\_\_\_\_\_  
Jimmy H. Starline, Chairman  
Camden County Board of Commissioners  
Camden County, GA

\_\_\_\_\_  
Robert McGrath  
FAA Air Traffic Representative  
Eastern Service Area

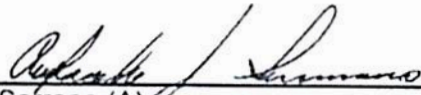
\_\_\_\_\_  
Virginia Boyle (A)  
Air Traffic Manager  
Air Traffic Control System Command Center



JACKSONVILLE CENTER, JACKSONVILLE TRACON, FLEET AREA CONTROL AND  
SURVEILLANCE FACILITY JACKSONVILLE, AIR TRAFFIC CONTROL SYSTEM  
COMMAND CENTER, AND CAMDEN COUNTY BOARD OF COMMISSIONERS, CAMDEN  
COUNTY, GEORGIA


LETTER OF AGREEMENT

6. SIGNATURES.

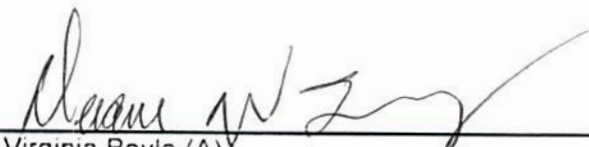
  
\_\_\_\_\_  
Al Serrano (A)  
Air Traffic Manager  
Jacksonville Center

\_\_\_\_\_  
Dustin B. Hendrix, CDR  
Commanding Officer  
FACSFACJAX

\_\_\_\_\_  
Sonya Busch  
Air Traffic Manager  
Jacksonville TRACON

  
\_\_\_\_\_  
Jimmy H. Starline, Chairman  
Camden County Board of Commissioners  
Camden County, GA

\_\_\_\_\_  
Robert McGrath  
FAA Air Traffic Representative  
Eastern Service Area

  
\_\_\_\_\_  
For Virginia Boyle (A)  
Air Traffic Manager  
Air Traffic Control System Command Center

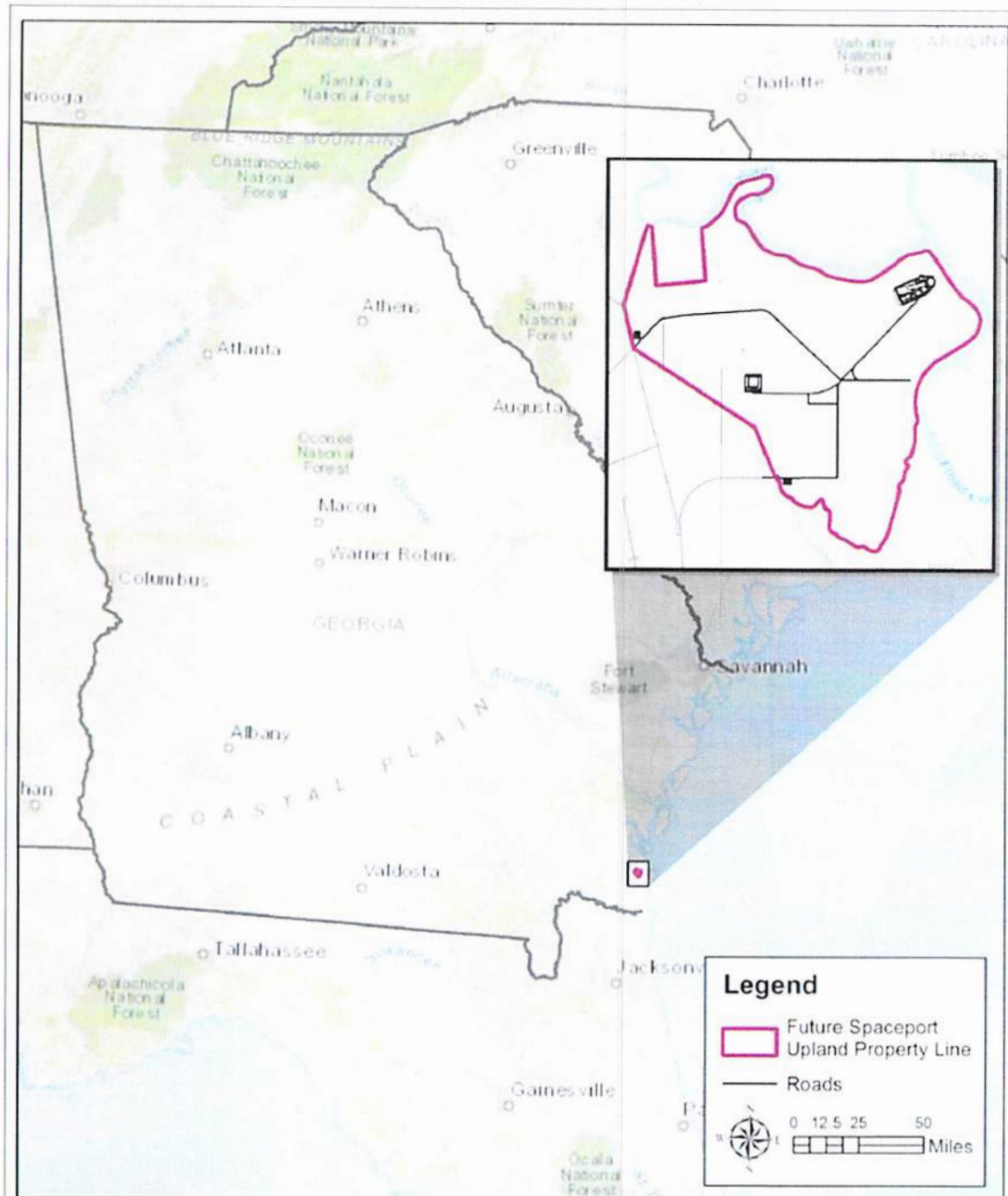
**JACKSONVILLE CENTER, JACKSONVILLE TRACON, FLEET AREA CONTROL AND  
SURVEILLANCE FACILITY JACKSONVILLE, AIR TRAFFIC CONTROL SYSTEM  
COMMAND CENTER, AND CAMDEN COUNTY BOARD OF COMMISSIONERS, CAMDEN  
COUNTY, GEORGIA**

**LETTER OF AGREEMENT**

**ATTACHMENT 1**

**EFFECTIVE: 12 February 2018**

**DEPICTION OF SPACEPORT CAMDEN**



**JACKSONVILLE CENTER, JACKSONVILLE TRACON, FLEET AREA CONTROL AND  
SURVEILLANCE FACILITY JACKSONVILLE, AIR TRAFFIC CONTROL SYSTEM  
COMMAND CENTER, AND CAMDEN COUNTY BOARD OF COMMISSIONERS, CAMDEN  
COUNTY, GEORGIA**

**LETTER OF AGREEMENT**

**ATTACHMENT 2**

**EFFECTIVE: 12 February 2018**

**POINTS OF CONTACT**

<b>NAME</b>	<b>PHONE</b>	<b>EMAIL</b>
<b>Jacksonville Center</b> Airspace and Procedures Traffic Management Unit	904-845-1553 904-845-1538	<u>Donald.J.Musser@FAA.Gov</u> <u>7-ASO-ZJX-MOS@FAA.Gov</u>
<b>Jacksonville TRACON</b> Airspace and Procedures	904-741-0704	<u>Sherry.Lawless@FAA.Gov</u>
<b>FACSFAC Jacksonville</b> Schedules Airspace & Procedures	904-542-2551 904-542-2112	<u>FACSFAC JAXS SKEDS@Navy.Mil</u> <u>Ronald.McNeal@Navy.Mil</u>
<b>Camden County Commission</b> Steven L. Howard	912-510-0464 (O) 912-552-3788 (C)	<u>SHoward@Co.Camden.GA.US</u>
<b>Air Traffic Control System Command Center</b> Space Operations	540-422-4100	<u>9-AWA-AJR-Space.Ops@faa.gov</u>



**Attachment 5**  
**Access Control Plan**



# Access Control Plan

As of 14 January 2020

**FOIA EXEMPT – PROPRIETARY DATA**

**GORA EXEMPT – SECURITY PLANNING INFORMATION**



## Contents

1.0	Introduction .....	3
2.0	Access Control Background Information .....	3
2.1	Overview of Basic Security Concepts .....	3
2.1.1	The Asset Triangle .....	3
2.1.2	The Threat Triangle .....	4
2.1.3	The Security Triangle.....	5
2.2	Security System Considerations.....	5
2.3	Major Elements / Functions Needed .....	6
2.3.1	Access Control System .....	6
2.3.2	Intrusion Detection and Alarm System .....	7
3.0	Access Control System Plan .....	11
3.1	Review of existing Documentation .....	11
3.2	Access Control Security Checkpoints .....	12
3.2.1	Land-based Checkpoint Types .....	12
3.2.2	Waterborne Checkpoint Types .....	13
3.2.3	Typical Operational Checkpoints .....	13
3.2.4	Checkpoint Staffing Scenario By Operation Type .....	15
3.2.5	Operations – Routine Day to Day Access Control .....	16
3.2.6	Operations – Wet Dress Rehearsals / Static Firings Access Control .....	17
3.2.7	Operations – Launch .....	18
3.3	Access Control System Features .....	19
3.3.1	Perimeter Fencing .....	19
3.3.2	Clear Zone Along Fences .....	20
3.3.3	Gates .....	20
3.3.4	Road to Main Gate & Speed Reduction .....	20
3.3.5	Interior Roadways and Parking .....	21
3.3.6	Property Coastline.....	21
3.3.7	Waterborne Patrols.....	22
3.3.8	Dock .....	22
3.3.9	Lighting.....	23
3.3.10	Guard Houses.....	24
3.3.11	Signage .....	28
3.3.12	Crime Prevention Through Environmental Design (CPTED) .....	28
3.4	Initial Plan – Camera Locations .....	28

### Revision History:

1/25/19 Initial Submittal.

01/14/20 Revisions include removal of medium-large launcher (only small launcher remains) and additional minor edits. Changes agreed with FAA/AST between January – December 2019 also included.

## 1.0 Introduction

This Spaceport Camden Access Control Plan has been prepared to meet the requirements of 14 CFR § 420.53, the control of public access as it relates to physical security (surveillance systems, physical barriers, etc.) and personnel policy / procedures. Specifically, 14 CFR § 420.53 states:

*§ 420.53 Control of public access.*

*(a) A licensee shall prevent unauthorized access to the launch site, and unauthorized, unescorted access to explosive hazard facilities or other hazard areas not otherwise controlled by a launch operator, through the use of security personnel, surveillance systems, physical barriers, or other means approved as part of the licensing process.*

*(b) A licensee shall notify anyone entering the launch site of safety rules and emergency and evacuation procedures prior to that person's entry unless that person has received a briefing on those rules and procedures within the previous year.*

*(c) A licensee shall employ warning signals or alarms to notify any persons at the launch site of any emergency.*

This document was largely prepared by Kimley-Horn with the coordination and assistance of Nelson Aerospace Consulting Associates for and on behalf of the Camden County Board of Commissioners.

## 2.0 Access Control Background Information

The following section reviews the general principles and overarching themes that were utilized to produce this Access Control Plan.

### 2.1 OVERVIEW OF BASIC SECURITY CONCEPTS

Three basic concepts of security were followed in developing the Spaceport Camden Access Control Plan including: the Asset Triangle, the Threat Triangle, and the Security Triangle.

#### 2.1.1 THE ASSET TRIANGLE

The goal of security is to protect assets. An asset is anything owned or wholly controlled by the organization and contributes to the successful completion of the organization's mission(s). Assets are best defined in three categories: infrastructure, information, and image. The Asset Triangle is shown in Figure 1.

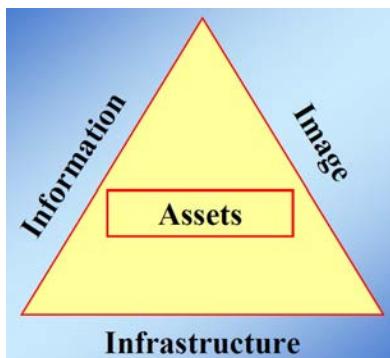


Figure 1. Asset Triangle

Infrastructure assets are tangible items that are part of the working structure of the organization – the things that make the organization’s mission(s) achievable. They include plant, property, equipment, and vehicles. Also included in this category are the persons who provide services to the organization – employees and contractors.

Information assets are those that contain data that is relevant to the execution and outcome of the organization’s mission(s). They include strategic plans, customer lists, financial and accounting records, design drawings, personnel information, and any other data collected or held by the organization. Information assets are divided into electronic (computer-based) and hard (paper) records.

Image assets are intangibles that influence the public and market perceptions of the value, reliability, and sustainability of the organization and its mission(s). Image assets include the public trust, market share, market capitalization, and competitive advantage.

Asset criticality is determined by evaluating assets in each of these three categories from both the operational and agency mission viewpoints. Operational personnel must be involved in the determination of operational mission-critical assets, and senior management must be involved in the identification of agency mission-critical assets.

### 2.1.2 THE THREAT TRIANGLE

Every threat has three critical elements, all of which must be present before the crime or event can occur. These include: motive, means, and opportunity, as shown in the Threat Triangle in Figure 2.



Figure 2. Threat Triangle

Motive is the willingness to commit a criminal act. There are many reasons a person may commit a criminal act, ranging from personal vendetta to political statement, including every possible motive in between. The organization cannot control what motivates a criminal.

Means refers to the capability of the person to perform an act. The means include such matters as equipment availability, time, the specific knowledge of the person, any available help from the inside of the organization, the person’s own native intelligence, and other resources. Once again, there is little that can be done to control the means available to a potential criminal or terrorist.

Opportunity is the open window, both literally and figuratively, to commit a malevolent act. It is the unlocked door, the unobserved fence, the unalarmed building, and the unlit perimeter that makes it easier for a criminal to gain entry to a site and to achieve their objectives, to the detriment of the organization. Opportunity is the one element of the threat triangle over which the organization has a great deal of control, and it is therefore where security efforts must be concentrated.

### 2.1.3 THE SECURITY TRIANGLE

Security plans should have three objectives, each a step further into a criminal act than the previous: deter, detect, and delay. These three objectives are shown as the Security Triangle in Figure 3.



Figure 3. Security Triangle

Deter: The first objective of a site security plan is to deter, which is, in effect, reducing opportunity. The intention is to will the potential criminal to abandon their plan of attack.

Detect: In the event that deterrence fails and the criminal proceeds with their plan of attack, it is desirable to ensure that the intrusion or other malevolent act is noted by the various components of the security system. In addition to the technology systems, detection also relies on the guards and the procedures and policies that are in place in order to note improper activities.

Delay: Once the act has been detected, the next objective is to delay the intruder as much as possible. A number of barriers can be created that the intruder must overcome, each of which slows their progress in reaching their objectives. The delay needs to be significant enough to allow for a response, from whatever mechanism is in place to respond. Contract security, employees on site, and outside agencies all may play a role in response, depending on the level of the intrusion.

## 2.2 SECURITY SYSTEM CONSIDERATIONS

Electronic security systems should be designed and installed with deliberate consideration for their ultimate goals. Security systems should be integrated seamlessly with each other, allowing a simple and effective user understanding and response to critical situations identified by the systems.

Integration is a central tenet of modern security design. Proper integration provides the end user with a greatly enhanced security capability, leading to a much higher level of comfort for the personnel that

are protected by the system. Additionally, effective integration reduces training costs, enhances the ability to quickly troubleshoot a system, and provides a notably more effective response from security personnel.

Integration is the interaction and sharing of information, features, and functionality between systems and people in order to effectively and efficiently perform a function. Strong integration will reduce the amount of interaction required between technology and people, which has two key benefits – the freeing up of personnel resources to perform other functions, and the reduction in possible points of failure in a system.

Conventional contracting methods in security usually end up with several systems from several different vendors, each supplying a different component of the system. While a certain amount of this is inevitable, it can create extra cost for the owner in the areas of training, installation, and maintenance. Developing a commonality in the systems under design is the preferred choice. This commonality is a methodology by which differing components can function as one, reporting through the same interface to an operator.

The advantages to the user are several. Functionally, this requires the operator to learn only one interface while operating multiple systems (e.g., CCTV, intrusion detection, access control, etc.). The cost of training is thus reduced while efficacy of operations is enhanced. Training or retraining processes on a single system is significantly easier and less costly than specialized training on each of the systems that are to be monitored and less complex systems enhances operational efficacy.

The integrated approach also allows the use of a single workstation for the monitoring personnel, as opposed to the need for multiple computers and workstations for separate systems. The savings are not just in the cost of the extra computers and peripheral devices, but also in actual real estate (space), which can be used for other things. And again, a simpler system to monitor and operate improves operational efficacy.

Integration has historically been performed by the firing of relays within a control panel or other device. This is a mechanical operation which, while effective, requires wiring of every integrated device to the control panel, in one form or another. On the other hand, software integration allows systems to interact at a software level. This means that wires are no longer needed for every contact that is part of the system. Now software can make the decisions, issue the commands, and invoke the necessary reactions from other systems. The savings in wiring alone from this capability at a large facility could be immense.

## **2.3 MAJOR ELEMENTS / FUNCTIONS NEEDED**

The following are high level descriptions of the major elements / functions that are envisioned to be utilized at the Spaceport Camden site.

### **2.3.1 ACCESS CONTROL SYSTEM**

The access control system will be the managing component of the entire security system. All gates, buildings, structures, and high priority areas of buildings will be equipped with a card access system to control entry and egress. Exceptions to this are anticipated for low priority storage sheds, and other



non-critical structures. High priority assets will be protected with access control requiring something in addition to a card, such as a PIN or biometrics.

An access control system provides a wealth of information that relates to both safety and security. The system should be able to provide reports that can be used as an investigative tool. The following matters, all of which can be determined via the software, should always be investigated:

- Propped doors;
- Cards read in unauthorized areas;
- Cards read at unauthorized times; and
- Compliance with entry/exit procedures at gates.

The last point above relates to the problem of personnel not always properly carding into the site or a building or secure room / space. For example, when carpooling, there are often times when only the driver will read their card to gain entry, no one else will. This creates both security and safety issues, as no one can be sure who is on site. Personnel procedures will be put in place as appropriate to ensure accurate awareness of site presence by authorized staff, contractors, and visitors.

Card access systems provide access via authentication (e.g., an access card) and authorization (where a given card is accepted). Authorization links authenticated individuals to the specific buildings or areas to which they are entitled to have access by establishing rules for each controlled access point. The authorization process is rightly in the hands of the access-system administrator and management.

Authenticity can be provided via three factors:

- Something you have (a card, a key);
- Something you know (a PIN number); and/or
- Something you are (biometrics).

The more factors required, the better the security. At the same time, there is a need to balance security requirements with operational efficiency. For the most part, using a card (something you have) as single factor authentication is strong enough security. However, for high priority assets multiple-factor authentications will be used, as appropriate.

## **2.3.2 INTRUSION DETECTION AND ALARM SYSTEM**

The entire length of the perimeter should be equipped with intrusion detection devices that are integrated into the alarm system. All entry points into buildings and structures, including windows and roof hatches, as well as high priority areas within buildings, should be monitored as well.

### **2.3.2.1 Camera Systems**

Closed Circuit Television (CCTV) should be used for four purposes: alarming, assessment, surveillance, and investigation. For each secure facility, the entire length of the perimeter, clear zones, and high priority assets should be monitored by video surveillance. A combination of pan-tilt-zoom (PTZ) and fixed cameras should be used as necessary to provide the best possible coverage. The system should have a sophisticated video management system capable of geographic information system (GIS) integration, camera control, video distribution and analysis, sensor integration, and alarm notification.

The CCTV component of the security plan should be viewed as an entire system that is greater than the sum of its parts. It is important not to attempt to consider the cameras separate from the management system, nor the reverse.

Video cameras now have the video analytic capability to note motion in their field of view by several different technologies and can trigger an alarm situation when that occurs. CCTV cameras should also be used to provide assessment when the access control system or video analytic detection system creates an alarm. They should also be capable of filling a general surveillance role, being used for pre-programmed tours of the compound when not responding to alarms. Finally, the system should provide a high degree of investigative capability, with easy retrieval of stored video and assurance that the video was not tampered with, in the event that it is ever required as evidence.

The system of cameras should include a combination of PTZ and fixed cameras. The PTZ cameras should be used for over-watch and alarm assessment, while the fixed cameras should be responsible for creating a recorded video record of the area for future investigations, as well as, real-time alarm assessment, general surveillance, and, in some cases, alarm detection.

#### **2.3.2.2 Video Management System (VMS)**

The Video Management System (VMS) should provide a distributed, scalable set of technologies for detection, transmission, and notification of alarm events. The fundamental objectives of the technology are to be able to easily integrate with standard devices and sensors in the field, process the information from the devices, derive alarms based on significant changes in the devices' state, and then annunciate the alarm through a set of open interfaces. This will require open architecture at the head end of the system so it can be easily integrated beneath more sophisticated command and control software. In particular, the system should include a suite of technologies for managing and analyzing digital video, controlling cameras, and interfacing to the perimeter intrusion detection and access control system. The VMS should be capable of working with a large number of different manufacturers' PTZ cameras.

#### **2.3.2.3 Camera and VMS Selection**

The camera selection process is simplified since cameras from most of the major manufacturers (Panasonic, Axis, Vicon, Pelco, Flir, Cohu and several others) are very similar in their optics and video streaming capabilities, but may differ significantly in their ability to support video analytic detection and/or ability to support low light or no light viewing of an area.

In making a selection of the VMS and cameras, the following factors should be considered:

- Manufacturer support;
- GIS integration;
- Camera control;
- Video distribution;
- Video analysis;
- Sensor integration; and
- Alarm notification.

#### **2.3.2.4 Geographic Information System (GIS) Integration**

The use of mapping technology to locate and position devices, cameras, and alarms within the real world provides several benefits, including enhanced situational awareness when identifying potential intrusions, incidents, and emergencies, and the response to these situations.

The system should be able to associate latitude and longitude coordinates with objects and alarms. This allows the production of map displays of the location of devices, cameras, and alarms. The map displays can incorporate industry-standard GIS data files, such as aerial photographs, street names, critical building locations, etc. Users can zoom or pan maps to any level, and they can interact with the objects represented on the map. For example, clicking on a camera icon immediately causes video to be displayed from the corresponding camera. These capabilities should allow the operator to spatially associate and navigate video and alarm data and their locations in an intuitive manner, without requiring any special user interface programming on the part of the system integrator. GIS mapping capability should provide a high level of situational awareness for the operator.

An additional benefit of having a native GIS capability is that the VMS could then automatically relate the sources of events with a means to evaluate or corroborate them. For example, if the system knows where each camera is and can determine where an alarm from an access control system is occurring, it can automatically position PTZ cameras to look directly at the point of intrusion without requiring any camera preset programming or relay contacts between the camera and the area of the detected intrusion. In the case of a large perimeter, this feature can save hundreds of hours of system integration time because the entire automated video surveillance response along a perimeter can be configured from a simple drawing that might take a few hours to produce.

#### **2.3.2.5 Camera Control**

An important part of remote site surveillance is corroboration and assessment of alarm conditions. The use of PTZ video cameras is an efficient way to provide alarm assessment prior to a response team being dispatched. Automating the control of PTZ cameras reduces both the time required to perform an assessment, and the skill required of a human operator to track an object interactively. This can occur in two different ways.

The two key capabilities of high-end camera control software are 1) providing remote control techniques that drastically reduce the effect of latency and bandwidth on camera positioning, and 2) using native GIS capabilities. This increased level of situational awareness should increase the capabilities of the monitoring personnel.

Typical joystick camera control presents problems to operators when used with digital video. The problem is that the up/down, left/right, in/out control actions are all “relative” positioning commands. The operator depends on feedback from the video to determine when to stop moving the camera. If there is enough latency in the video feed (due to bandwidth limitations or streaming compression characteristics) then the operator will consistently overshoot their target. The problem is compounded if the operator is trying to track a moving target.

If the VMS can position cameras using absolute coordinates, it would be able to support an alternate camera control methodology. Instead of moving the camera left/right or up/down, the operator would simply click on a spot on the video image where they would like the camera to point. The camera would

automatically move so that this point becomes the center of its field of view. Within the constraints of the camera's optics, the camera should automatically position and zoom to match the operator's request. This point-and-click camera control capability would greatly reduce the effects of video latency and increase the ability of an operator to track a moving object, while reducing the manual skill required to control the camera.

Another advanced feature of modern camera control technology is the ability to automatically direct a PTZ camera to track one or more objects in its field of view in an outdoor environment. The advantage of this is two-fold: it drastically reduces the need for a human operator to control the position of a camera, and since the control technology is based in an independent processor, it is independent of camera make and model.

#### **2.3.2.6 Video Distribution**

The VMS should provide centralized access to all remote video camera feeds through a central server, eliminating the need for the user to figure out which remote device needs to be accessed in order to get video from a camera. The central server system (control and archive functions) should include both a local server within the secured site and a back-up server that is located at a remote location off site. Video should be distributed using standard IP networking protocols, so that it is available to any device that has an IP network connection, including web browsers and handheld devices. This capability can be important during a manned response to an alarm, where the responder can quickly view and take control of a PTZ camera before entering the subject location.

#### **2.3.2.7 Video Analysis**

Most VMS manufacturers with network video recording (NVR) include some kind of video motion detection algorithms in their camera or VMS. Typically, these algorithms work well in indoor and outdoor environments. For this project, there is a need for the video processing and motion detection algorithms to work in the various lighting and weather conditions encountered in the outdoors, within reason.

#### **2.3.2.8 Sensor Integration**

The VMS should be capable of integrating with third-party devices through RS-232/RS-422/RS-485 serial communications and Ethernet. The information provided by these devices can be used to generate alarm conditions, turn on programmed camera motion detection configurations, move one or more cameras to specified locations, or send a control signal to another type of device.

#### **2.3.2.9 Alarm Notification**

The alarm notification system should be sophisticated and flexible in order to distribute alarm information both to monitoring personnel and to other systems.

Alarm enunciation should be available through aural (speakers / horns), visual (lights / flags), e-mail, pagers, and voice telephone calls. In addition, there should be a graphical map-based console to provide operators with an intuitive view of a system by incorporating aerial photographs, Google Earth and other geographical contexts for alarms and video display.

The notification system is intended to let users define a contact hierarchy, where each individual has designated methods of contact and a schedule for contact. The methods for contact may include e-mail, texting, voice telephone call, or any other contact method plug-in the system integrator supplies. The contact schedule specifies rules for when each contact method may be used, along with exceptions to those rules. Contacts can subscribe to different alarms either globally or on a per-site basis. More than one contact may subscribe to the same alarm. Each level in the hierarchy has a defined emergency contact that will be used if a designated contact for an alarm cannot be successfully reached. Each contact action taken for an alarm should be logged, along with an indication of acknowledgement.

#### **2.3.2.10 Perimeter Intrusion Detection Systems (PIDS)**

In selecting a PIDS technology for each secure facility, there are typically four main factors to consider:

Probability of Detection: An ideal detector would have a perfect probability of one. However, there are no perfect detectors, so the closer the detection technology performs to an ideal condition (i.e., higher probability of detection) the better the PIDS will be.

Nuisance alarm rate: A nuisance alarm (false alarm) occurs when an alarm is generated, but there is no target present. The ideal nuisance alarm rate would be zero. The most likely cause of nuisance alarms are environmental factors such as wildlife, vegetation, and weather conditions.

Coverage Area and Tracking: The coverage area is the area in which the detection device can detect a target and track the movement of the target within the coverage area. In general, a larger the coverage area provides a longer duration for tracking a target's movement. Larger coverage areas also provide the ability to define multiple electronic barrier limits within the coverage area and only trigger an alarm when the target crosses over a specific barrier limit.

Visible Light Level: For this specific project, the ability to detect a target in areas where there is zero visible light is a critical technology selection factor in some site areas, since adding visible light is not a practical option along the outer most site perimeter.

### **3.0 Access Control System Plan**

This section provides the Spaceport Camden Access Control System Plan. It includes an overview of the existing documentation; plans for the spaceport access control system elements; and those organizations that were part of the coordination group interviewed that influenced this plan.

#### **3.1 REVIEW OF EXISTING DOCUMENTATION**

In the development of this Access Control System Plan, the following documents were reviewed:

- Detailed Site Description for Spaceport Camden,
- Draft Spaceport Camden potential safety zone charts,
- US Coast Guard navigational charts for the region,
- Various satellite and low altitude aerial photographs,

- Publicly available maps, images, guides, and related material (e.g., National Park Service),
- Spaceport Camden County EIS DOPAA, and
- Spaceport Camden County EIS Noise Study.

Preliminary client input for controlling the public access to Spaceport Camden included the following:

- Checkpoints along access roads,
- Checkpoints for waterborne patrols,
- Perimeter fencing along western boundary of property and each secure facility,
- Appropriate clear zone on secure and unsecure side of fencing,
- Existing and potential future security camera locations, and
- Alternative surveillance systems (unmanned aerial systems, motion detection, etc.).

In addition to studying these materials and inputs, onsite visits, interviews with local experts (e.g., NPS staff, local first responders from the Sheriff's Office and Camden Fire and Rescue, and residents) were held that included both on-land, and on-water investigations.

### **3.2 ACCESS CONTROL SECURITY CHECKPOINTS**

Based on the activities and investigations discussed in Section 3.1, significant time was spent in identifying and confirming the location of security checkpoints and patrol areas that most efficiently and thoroughly provided controlled coverage of the critical launch areas for a representative launcher. Figures 4 through 6 later in this section and its subsections show and discuss these checkpoints including land and water-based check points for access control and management.

Also discussed in the subsections below is Access Control for three operational scenarios: 1) Routine Day-to-Day Operations, 2) Static Test and Wet Dress Rehearsals, and 3) Launch Operations. All access control and notifications for a specific launch will be captured in a Comprehensive Launch Plan (CLP).

Pursuant to 14 CFR §420.53(b), and as a matter of routine operations, all persons who enter the site will be briefed on safety / security rules, any special provisions required from the EIS mitigation measures, and emergency / evacuation procedures. Such briefing will be valid for one calendar year, unless updates dictate a shorter period.

Pursuant to 14 CFR §420.53(c), during any emergency at the launch site, warning systems and alarms, as are described in section 2.3.2.9, will be employed. Each launch or test operation (e.g., wet dress rehearsal or static fire test) will have a defined set of warnings and alarms tailored to that operation. These warning systems and alarms will be captured and described in the CLP process, documented and rehearsed prior to the intended operation, as appropriate.

#### **3.2.1 LAND-BASED CHECKPOINT TYPES**

There are several land-based checkpoint types that are identified in the Spaceport Camden Access Control Plan including gate-entrance checkpoints, road / trail checkpoints, and various secure facility entrances with access control systems. These are briefly described below.



Main Entrance – The main gate entrance is anticipated to be gated and manned 24/7. This is the primary entrance to the property.

Secondary Entrance – The secondary entrance to the property has a typically unmanned guard house and may include a vestibule type aviation gate. During launch operations, this location will be manned.

Road & Trail Checkpoints – These check points are established to control unauthorized access to the launch site and along the intended trajectory during launch operations.

Secure Facility Entrances – Each secure facility such as the welcome center, vertical launch complex, launch control center complex, and mission preparation area will have a security gate and guard house. Depending on operations the entrances will either be manned or unmanned.

### 3.2.2 WATERBORNE CHECKPOINT TYPES

There are several waterborne checkpoint types that are identified in the Spaceport Camden Access Control Plan including fixed and roaming checkpoints and zones. It is assumed that the identified Safety Zones are approved and authorized pursuant to US Coast Guard standard operating procedures and established in accordance with 33 CFR §165. It is further assumed that this establishment procedure will include appropriate letters of authorization and agreement between US Coast Guard and local first responders such as the Camden County Sheriff's Department. These are briefly described below.

Fixed Patrol Zones / Checkpoints – Several locations along the controlled access area require that a Sheriff's boat (or other stakeholder first responder watercraft authorized by the US Coast Guard) patrol and remain essentially in a fixed location. These areas have an open field of view.

Roaming Patrol Zone – Some locations along the controlled access area require that a Sheriff's boat (or other stakeholder first responder watercraft authorized by the US Coast Guard, who is part of the official security team) roam and patrol a larger area that may be narrow and have a narrow field of view.

### 3.2.3 TYPICAL OPERATIONAL CHECKPOINTS

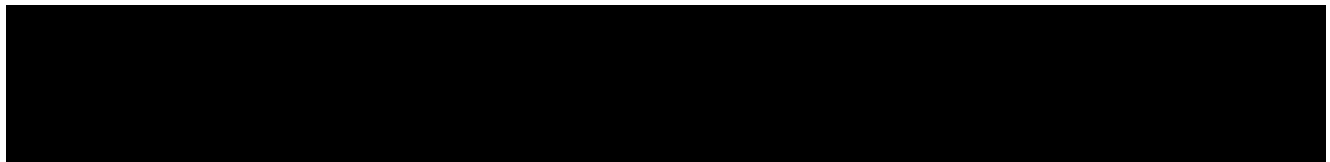


Table 1. Typical Operational Checkpoints

(b) (7)(F)



#### 3.2.4 CHECKPOINT STAFFING SCENARIO BY OPERATION TYPE

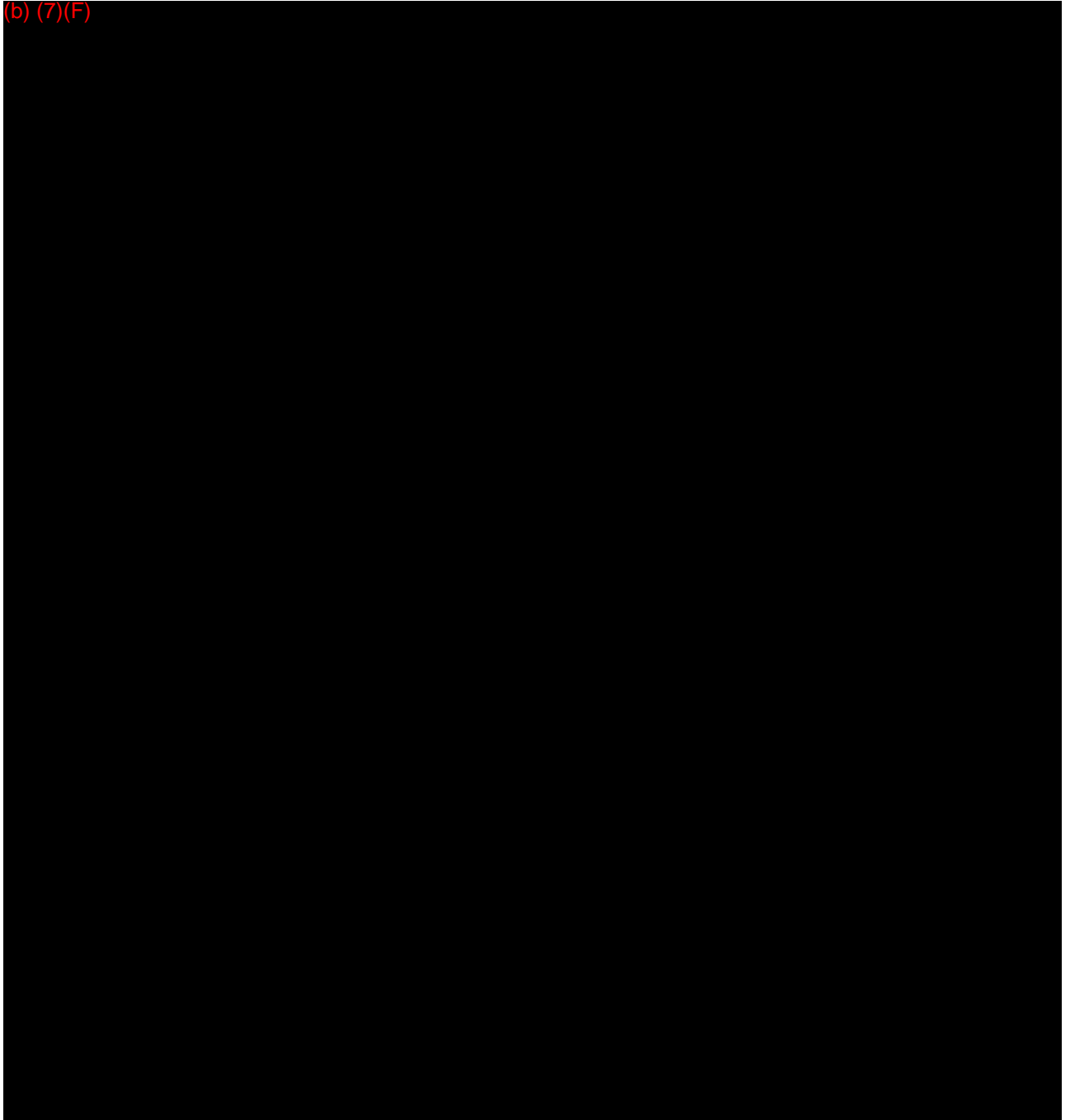
(b) (7)(F)



### 3.2.5 OPERATIONS – ROUTINE DAY TO DAY ACCESS CONTROL

During routine, day to day access control operations, the checkpoints shown in Figure 4 will be active as per the assignments shown in the table of section 3.2.4.

(b) (7)(F)



**3.2.6 OPERATIONS – WET DRESS REHEARSALS / STATIC FIRINGS ACCESS CONTROL**

(b) (7)(F)



### 3.2.7 OPERATIONS – LAUNCH

(b) (7)(F)





### 3.3 ACCESS CONTROL SYSTEM FEATURES

The Spaceport Camden Access Control Plan utilizes various physical and electronic features to ensure adequate security to meet FAA licensing and operational requirements. These are discussed below in the following subsections. These discussions take the form of the baseline plan for that system feature, and a potential added capability should the baseline feature be found to need augmentation.

#### 3.3.1 PERIMETER FENCING

A barrier is often used as the initial line of defense in protecting a facility and thus is a critical element of the first security layer. The chain-link fence is the most common of these barriers, owing to its durability and relatively low cost. Security fencing as per FAA Airport requirements will be installed along the western boarder of the planned Spaceport Camden property and along the perimeter of each individual facility of the spaceport.


(b) (7)(F)



### 3.3.2 CLEAR ZONE ALONG FENCES

All fenced areas will have clear zones with planted grass to enable enhanced electronic security systems to function properly.

(b) (7)(F)



### 3.3.3 GATES

Gates are a key part of any access control plan. Although a critical element of the perimeter, gates are also, typically, a weak point for entry. One of the major issues in gating is the strength of the gate when attacked or hit by a vehicle. Swing gates that join in the middle of the road provide minimal protection from this type of attack. The center point where the gates meet is the weakest area, and a vehicle attacking this point can easily breach the gate. The use of a sliding or rolling gate eliminates this weak point and establishes the quality of the gate material itself as the major variable in its ability to withstand attack. The following is planned for Spaceport Camden.

(b) (7)(F)



### 3.3.4 ROAD TO MAIN GATE & SPEED REDUCTION

Approaches to checkpoints are a critical element of securing a site. At Spaceport Camden, there is a (approximate) half mile straight section prior to the main gate that can enable a vehicle to gain significant speed. The following are plans for speed reduction.

(b) (7)(F)



### 3.3.5 INTERIOR ROADWAYS AND PARKING

Should there be an anticipated increase in traffic causing congestion or concern with excessive speed on the Spaceport Camden site, interior road design may help alleviate these issues.

(b) (7)(F)



### 3.3.6 PROPERTY COASTLINE

The spaceport property is bounded on three sides by water and marshland. The ground elevation varies between 10-15 feet above the water level and provides a natural barrier to access. Warning signs exist along the whole of the property that note “Danger – Unexploded Ordnance – Keep Out.” New or additional signs will be installed, as appropriate. See signage subsection for additional plans. No additional security fence along the coastline is required, although electronic surveillance is envisioned.

(b) (7)(F)



Figure 8. Fallen Trees Along Bluff near Silo Site

### 3.3.7 WATERBORNE PATROLS

During the day of launch or during wet dress rehearsals / static tests, at the direction and jurisdiction of the US Coast Guard pursuant to 33 CFR 165, Safety Zones will be established. The USCG's designated first responder (e.g., the Camden County Sherriff's Department (CCSD) and/or other affiliated first responders, as appropriate) will set up waterborne perimeter checkpoints / patrol areas in accordance with Figure 5 and Figure 6. Waterways between the checkpoints, within the controlled access area should be cleared of unauthorized vessels prior to launch / test and reopened following a successful launch / test. In the event of a mishap that results in debris in the controlled access area, the perimeter should be maintained in accordance with the launch site accident investigation plan.

(b) (7)(F)



### 3.3.8 DOCK

The dock on the property (see Figure 9 and 10) may present an access point onto the property that is easier than other waterborne points of entry, due to the old boat ramp on the south side of the dock. Access control here may be necessary. Should the dock be brought back into use, a ramp installed, and the structure appropriately permitted, additional measures (augmented plan) may be necessary for access control as described below.

(b) (7)(F)





Figure 9. Dock along Floyd Creek



Figure 10. View from Dock looking North

### 3.3.9 LIGHTING

To facilitate night time access control and security, lighting will be necessary.

(b) (7)(F)

A large black rectangular redaction box covering the majority of the page content below the lighting section header.

### 3.3.10 GUARD HOUSES

The Spaceport Camden site and individual facilities inside the property line will have several guard houses (e.g., main gate and a guard house at each facility). The guardhouses will consider the best practices of other government launch sites. Here is a brief discussion of these other guard houses.

The main entrance to Wallops Flight Facility consists of a 2,500 sqft badging office and a 15' x 20' guard house at the main gate. These are shown in Figures 15 and 16.

Kennedy Space Center has several guard houses that provide access to the large secure area “inside the fence”, and additional guard houses at each secure facility, such as Launch Complex 39A (LC-39A) and LC-39B. At the two main entrances to KSC, along NASA Parkway (SR-405) and North Courtney Parkway (SR-3), are vehicle checkpoints that consist of multiple lanes for badge check as well as a roughly 20' x 40' security building (See Figure 11 and Figure 12). The buildings have power, communications, and water. One 6,500 sqft badge office supports the center at the main entrance along SR-405. Both LC-39A and LC-39B have guard houses along the main roadways to the launch pads (see Figure 13) as well as guard houses at the entrance to each pad (see Figure 14). The guard house at each launch complex is approximately 20' x 45' with power, communications, and water. The facility is also equipped with Common Access Card technology allowing authorized personnel to scan their badge to gain access. The guard houses along Saturn Causeway and Beach Road are approximately 8' x 10' with power and communication only. Each guard house features a red warning light alerting traffic to upcoming launch/test.

(b) (7)(F)







**Figure 11. Kennedy Space Center Main Entrance at SR-405 (Source: Google Maps)**



**Figure 12. Kennedy Space Center Main Entrance at SR-3 (Source: Google Maps)**



Figure 13. Roadway Guard House (Source: Google Maps)

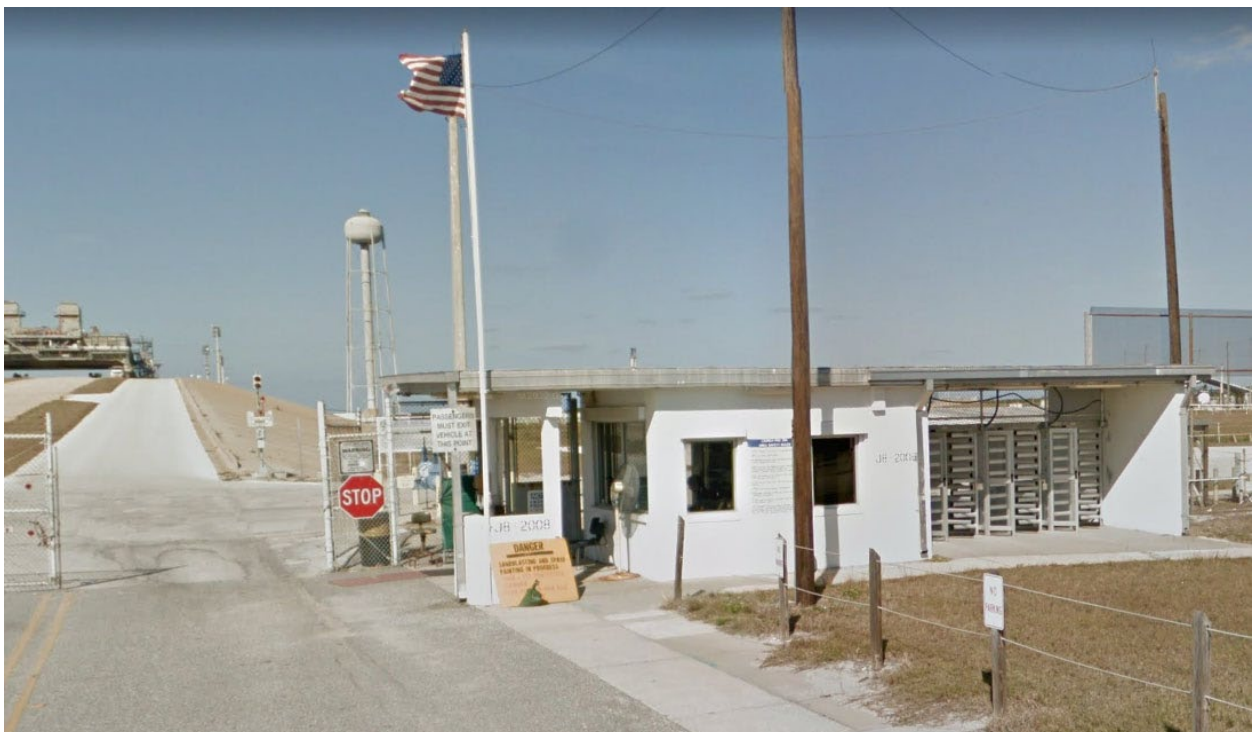


Figure 14. LC-39A Launch Site Guard House (Source: Google Maps)





Figure 15. Wallops Flight Facility Main Entrance (Source: Google Maps)



Figure 16. Wallops Flight Facility Main Entrance (Source: Google Maps)

### 3.3.11 SIGNAGE

Signage design should balance two critical needs: (1) to provide information to persons on the grounds, and more importantly to police, fire, or ambulance responders, and (2) to not provide so much information that they can aid intruders in their actions. Signs for public use should only detail areas the public is allowed to access, and not mission-critical or high-risk areas where the most damage can be achieved. The design approach to signage at the site should consider three types of signs: (1) Building-identifying; (2) Wayfinding; and (3) Regulatory/warning.

Warning signs are of particular importance at a spaceport, which contains ample opportunity for someone to accidentally cause harm to themselves or others, particularly if they do not know their way around. This is not merely a security issue, but speaks directly to safety and liability as well.

(b) (7)(F)



### 3.3.12 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

In evaluating the landscape in terms of security, there are two main concerns to address. The first is whether any landscape feature would enable unauthorized entry into the property. This primarily addresses large trees or bushes that are adjacent to the perimeter fence, on either side, that facilitates access to the property. The second issue is whether the landscape provides screening or hiding areas for intruders. The type and placement of landscaping is also affected by the addition of proposed security devices. Security cameras need clear views of the perimeter fence around secure facility areas, unobstructed by large shrubs or trees. Sensing devices (i.e., video analytics) on perimeter fencing need clear space adjacent to the fence to avoid constant alarms caused by moving branches or tree limbs. The tree line along the outer most west perimeter fence and just beyond the clear zone will remain as a barrier to deter and delay a vehicle from breaching the fence line.

(b) (7)(F)



## 3.4 INITIAL PLAN – CAMERA LOCATIONS

The Spaceport Camden Access Control Plan has as its initial approach to install cameras as per Figure 17. Many camera technologies were evaluated including:

(b) (7)(F)

