



**KNIK ARM CROSSING  
FINAL  
SECURITY EVALUATION  
FINDINGS  
TECHNICAL  
REPORT**

Agreement No: P 42070  
Federal Project No:  
ACSTP-0001(277)  
AKSAS Project No: 56047

Prepared for:

**Knik Arm Bridge and  
Toll Authority  
550 W. 7<sup>th</sup> Ave., Suite 1850  
Anchorage, AK 99501**

**Alaska Department of  
Transportation & Public Facilities  
P.O. Box 196900  
Anchorage, AK 99519-6900**

**Federal Highway Administration  
P.O. Box 21648  
Juneau, AK 99802**

Prepared by:

**HDR Alaska, Inc.  
2525 C Street, Suite 305  
Anchorage, AK 99503**

**PND Engineering, Inc.  
1506 W. 36<sup>th</sup> Ave.  
Anchorage, AK 99503**

**FEBRUARY 2006**



**Abbreviations and Acronyms**

AASHTO	American Association of State Highway and Transportation Officials
ACS	Alaska Communication Systems
APD	Anchorage Police Department
AS	Alaska Statutes
AWWU	Anchorage Water and Wastewater Utility
CCTV	Closed Circuit Television
CDAA	Circularly Disposed Antenna Array
CFR	Code of Federal Regulations
EIS	Environmental Impact Statement
Elmendorf	Elmendorf Air Force Base
EMC	Electro-Magnetic Compatibility
FAR	Federal Aviation Regulations
Fort Richardson	Fort Richardson Military Base
GCI	General Communications Inc.
FHWA	Federal Highway Administration
KABATA	Knik Arm Bridge and Toll Authority
KAC	Knik Arm Crossing
Mat-Su	Matanuska-Susitna
NCHRP	National Cooperative Highway Research Program
O&M	Operations and Maintenance
RAM	Risk Assessment Methodology
SSI	Sensitive Security Information
SWAT	Special Weapons and Tactics
TSA	Transportation Security Administration

### **Executive Summary**

This technical report provides the findings of a preliminary security evaluation of the proposed Knik Arm Crossing project. The effect of the proposed project on the security of nearby public facilities and military bases is analyzed, in addition to the security requirements for the proposed bridge and approach roads. Included is a review of security standards and guidelines, as well as security assessment methods. Officials at the Port of Anchorage and Alaska Railroad were interviewed as part of this security evaluation and discussions were held with officials at the Department of Homeland Security. However, input from Elmendorf Air Force Base and Fort Richardson Military Base was not available at the time of publication.

This security evaluation is limited in scope and is not based on classified information or Sensitive Security Information (SSI). Security issues sometimes involve information that is sensitive and not available to the general public. However, confidential information has not been requested or reviewed. The purpose of this report is to evaluate security issues in the context of a report that may become part of an Environmental Impact Statement (EIS) and part of a public process for evaluation of route alternatives.

Extreme security issues such as terrorist attacks and weapons of mass destruction are generally beyond the scope of this limited security evaluation. Security measures considered are primarily related to maintaining restricted access and adequate setbacks to nearby sensitive properties, the proposed Knik Arm Crossing bridge and approach roads. Fencing is the primary recommended security measure. Security is assumed to be different from safety, although the requirements for each sometimes overlap.

## **1.0 INTRODUCTION**

This Technical Report provides documentation of security aviation findings, in the Matanuska-Susitna Borough (Mat-Su) and the Municipality of Anchorage (Anchorage) that would be affected by the proposed Knik Arm Crossing (KAC) project. The Federal Highway Administration (FHWA) is preparing a Draft Environmental Impact Statement (EIS) as part of the National Environmental Policy Act (NEPA) process to evaluate a Knik Arm crossing sponsored by the Knik Arm Bridge and Toll Authority (KABATA). This Technical Report is limited to the Study Area and to the alternatives further evaluated in the EIS. The Study Area, the proposed alternatives, and the projected impacts from their implementation are described below.

## **2.0 PROJECT DESCRIPTION**

More than 80 years of transportation, land use, and economic plans and studies for the Upper Cook Inlet region of Alaska have addressed the need for a Knik Arm crossing project to connect Anchorage with the Mat-Su.

In 2003, the Alaska State Legislature established the Knik Arm Bridge and Toll Authority (KABATA) as a public corporation and an instrumentality of the State of Alaska within the Alaska Department of Transportation and Public Facilities (ADOT&PF). The specific mission of KABATA is to "... develop, stimulate, and advance the economic welfare of the state and further the development of public transportation systems in the vicinity of the Upper Cook Inlet with construction of a bridge to span Knik Arm and connect the Municipality of Anchorage and the Matanuska-Susitna Borough." (Alaska Statutes chapter 19.75)

In accordance with this mission, the purpose of the proposed KAC project would be to provide improved access and connectivity between Anchorage and the Mat-Su through an efficient and financially feasible crossing of Knik Arm, including adequate connections to the committed roadway network on both sides of Knik Arm. A Knik Arm crossing would:

- improve regional transportation infrastructure to meet existing and projected population growth in Upper Cook Inlet
- enhance the movement of people, freight, and goods between Anchorage, the Mat-Su, and Interior Alaska
- offer safe, alternative connections between regional airports; ports; hospitals; and fire, police, and disaster relief services for emergency response and evacuation

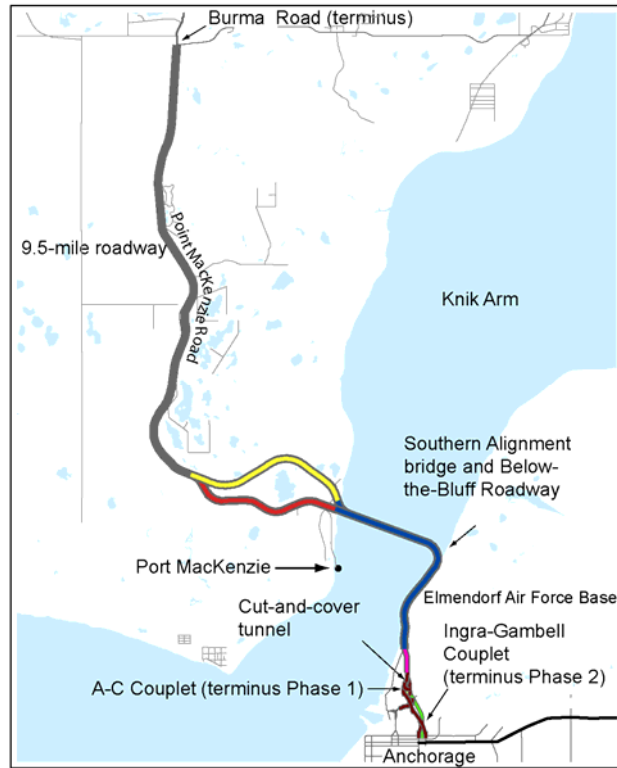
The proposed bridge crossing of Knik Arm would be located approximately 1.25 miles north of Cairn Point and would span approximately 2.5 miles (see Figure 2.1). The roadway connection on the Mat-Su side of Knik Arm would be Point MacKenzie Road near the Port MacKenzie District. The roadway connections on the Anchorage side of Knik Arm would be the A-C and Ingra-Gambell Couplets, generally in the Port of Anchorage (POA)/Government Hill/Ship Creek area. The total length of the project from

the intersection of Point MacKenzie and Burma Roads to the intersections of the A-C and Ingra-Gambell Couplets with Third Avenue would be approximately 19 miles.

Design and construction features of the proposed KAC project would include, among other details:

- a toll plaza
- a rural principal artery
- phased construction

The proposed project would be a controlled access toll facility with a toll plaza located in the Mat-Su near the western bluff of Knik Arm. The proposed project would be classified as a rural principal arterial in the Mat-Su and across Knik Arm, transitioning to an urban principal arterial in Anchorage in the vicinity of the POA. The proposed project would be phase-constructed as travel demand would warrant and would be anticipated to generally be an initial two-lane facility with expansion to a four-lane facility by the design year 2030. Initial construction would include a connection to the existing A-C Couplet on the Anchorage side and, by approximately 2022–2025, a connection to a new viaduct (elevated bridge) across the Ship Creek rail yard to connect with the Ingra-Gambell Couplet.



**Figure 2.1** shows that the proposed project begins at Burma Road and ends in Downtown Anchorage. Components common to all routes being considered are also identified.

Right-of-way (ROW) widths for the project would vary by specific design element. The proposed project ROW in the Mat-Su would be approximately 400 to 450 feet in width. In the Anchorage portion of the proposed project, the ROW would be approximately 260 feet along the east shore of Knik Arm down to the future expansion of the POA, then vary from 200 to 350 feet as it passed behind the port. As it climbed Government Hill, the ROW would expand to 985 or 585 feet wide to accommodate a cut-and-cover tunnel and access points along either a Degan Street- or Erickson Street-area alignment, respectively. Continuing southward it would cross the Ship Creek rail yard along an approximately 80-foot-wide, pier-supported viaduct ending at Third Avenue, the proposed project terminus.

## 2.1 Description of the Proposed KAC Project Study Area

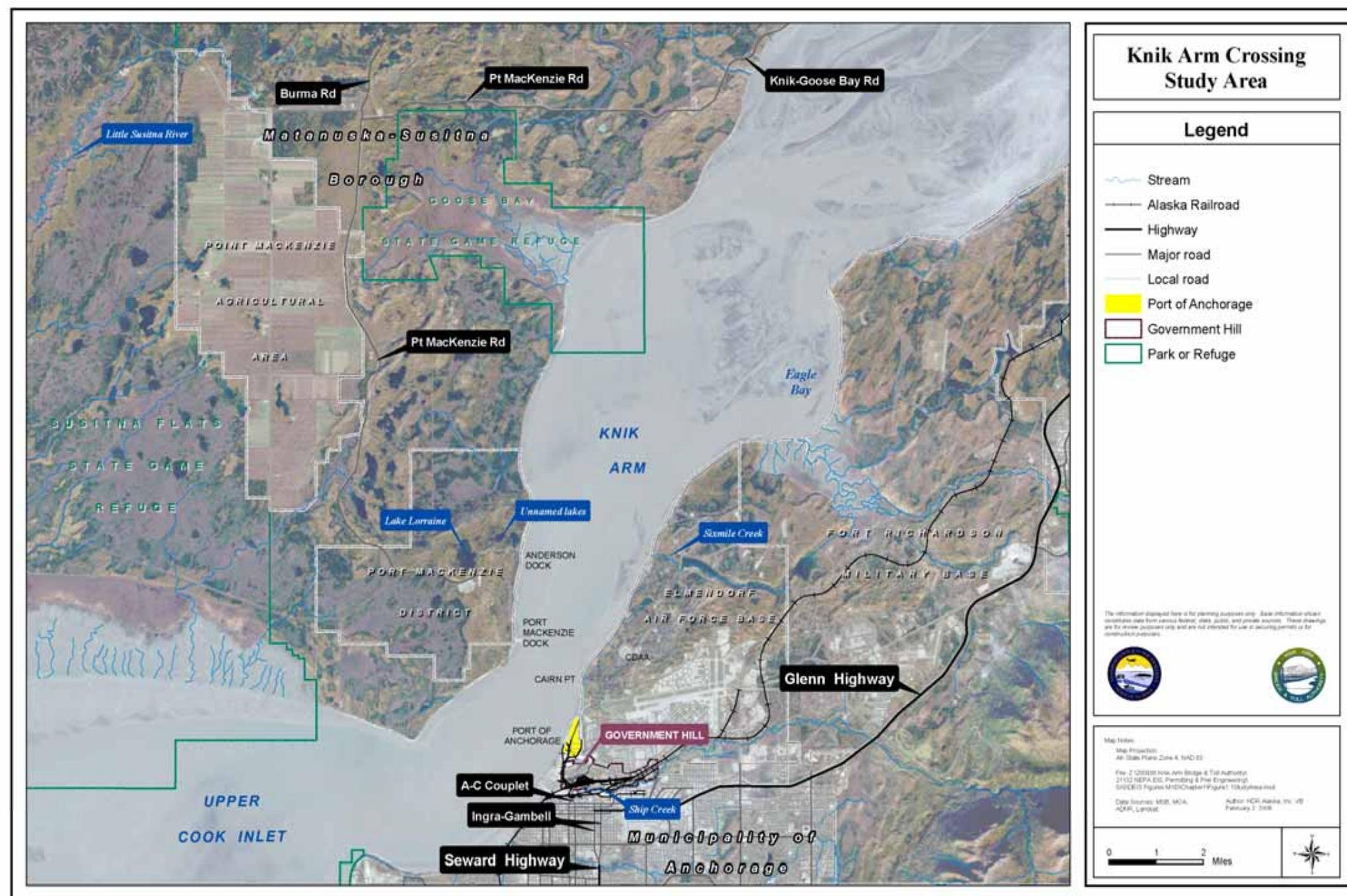
The Study Area for the proposed KAC project is located within the boundaries of Anchorage and the Mat-Su in the Upper Cook Inlet region of Southcentral Alaska

(Figure 2.2). The Study Area has a combined population of nearly 350,000, which represents over 50 percent of Alaska's total population. The Anchorage and Mat-Su portions of the Study Area are separated from one another by Knik Arm, a 30-mile-long waterway, which varies in width from 2 to 6 miles. Anchorage is located approximately 3 miles across Knik Arm from Port MacKenzie and the adjacent Port MacKenzie District.

Although the physical separation between these two areas consists of a short span of waterway, the only current surface transportation access between Anchorage and the Port MacKenzie District (Port District) is by 80 miles of existing roadway around the head of Knik Arm.

Located along the eastern shore of Knik Arm, Anchorage encompasses 1,961 square miles, 84 percent of which is occupied by National Forest, State Parklands, and tidelands, with an additional 6 percent occupied by military reservations. Only about 10 percent of the entire municipality is inhabited and available to accommodate existing and future growth. Most residents of Anchorage live in the Anchorage Bowl, the most urbanized portion of the municipality. The Anchorage Bowl occupies approximately 112 square miles and is bounded by Chugach State Park, Knik and Turnagain Arms, Elmendorf Air Force Base (Elmendorf), and Fort Richardson Military Base (Fort Richardson). Anchorage residents outside the Anchorage Bowl live either further north in the suburban communities of Chugiak-Eagle River or in small residential areas along the Glenn Highway and Turnagain Arm. Also located within this portion of the Study Area are the POA—a vital intermodal facility—and the adjacent Ship Creek industrial area.

On the western shore of Knik Arm, the Mat-Su consists of an area of 24,683 square miles, which encompasses approximately 23 percent of all private land in the state of Alaska. Because there is a substantial amount of undeveloped land available in the Mat-Su, the area provides an alternative to more costly and limited residential, commercial, and industrial lands within Anchorage. This availability has resulted in numerous changes that have recently occurred or will be occurring in the Mat-Su, including construction of Port MacKenzie in the late 1990s, existing and planned expansion of the connecting transportation network to and from Port MacKenzie, and planned development of the 9,000-acre Port District. The Mat-Su Borough is also developing a ferry link between Port MacKenzie and the POA; the ferry is projected to begin operation in 2008.



**Figure 2.2.** KAC Draft EIS Study Area. The Study Area has no specific, fixed boundaries because the Study Team has created a unique Study Area for each resource or issue assessed in the Draft EIS. The term *Study Area*, thus, has a context-specific meaning that shifts from one resource to another.

## **2.2 Alternatives**

The proposed KAC project would begin at the intersection of Point MacKenzie and Burma Roads and follow the existing roadway alignment south to the western boundary of the Port District. From here, there would be two alternative routes for getting to the proposed bridge crossing. The proposed Point MacKenzie Road Alternative would use the existing Point MacKenzie Road most of the way through the Port District before deviating from the established road and heading toward the proposed bridge crossing near the western bluff. The proposed Northern Access Alternative would skirt the core port area on the north side on a new alignment. With either proposed alternative, there would be a toll plaza and intersection/access road to allow access to and from Port MacKenzie.

The proposed bridge would be within the Southern Alignment, a corridor beginning approximately 1,500 feet south of Anderson Dock on the Mat-Su side and ending 1.25 miles north of Cairn Point on the Anchorage side. The crossing structure would be either 8,200 or 14,000 feet long. The Southern Alignment also includes the eastern bridge abutment, where the proposed Anchorage approach road would travel southwest on fill along the tidelands and below the bluff (termed the proposed “Below-the-Bluff Roadway”), toward Cairn Point, then turn southward, closely following the natural curve of the shoreline.

From this point the proposed roadway would parallel the eastern boundary of the POA, where the route would connect to the existing A-C Viaduct and the proposed Ingra-Gambell Viaduct by way of either of two routes: the Degan Alternative or the Erickson Alternative. The proposed Degan Alternative would follow the alignment of Degan Street through a cut-and-cover tunnel that would initially connect to East Loop Road with an at-grade, T-intersection (Phase 1). As travel demand would warrant, the route would continue on the proposed new Ingra-Gambell Viaduct over the Ship Creek rail yard before tying into the Ingra-Gambell Couplet at 3rd Avenue. At that time, Loop Road would be elevated over the proposed KAC route to provide access to Government Hill and Elmendorf. The proposed Erickson Alternative would be similar, but the cut-and-cover tunnel would align with Erickson Street and connect directly into Loop Road in Phase 1 (ramps would continue to provide access to Government Hill and Elmendorf). In Phase 2, when travel demand would warrant, the route would continue in a parallel cut-and-cover tunnel under Erickson Street onto the proposed Ingra-Gambell Viaduct, tying into the Ingra-Gambell Couplet at 3rd Avenue.

## **2.3 Preferred Alternative**

FHWA screened the range of alternatives against criteria for purpose and need and technical criteria to identify reasonable alternatives for detailed study in the Draft EIS. Based on these screening criteria and subsequent detailed evaluations, FHWA has identified a Preferred Alternative.

The preferred approach route to the proposed Knik Arm Bridge from the Mat-Su side is the Northern Access Alternative: Point MacKenzie Road from its intersection with

Burma Road, south to the Port District, and connecting through to the Port District along the northern alignment. FHWA chose this route because it would avoid wetlands, would not impact Port MacKenzie operations, and is favored by Mat-Su Borough and Port MacKenzie officials.

The proposed Southern Alignment is the preferred route for the bridge to cross Knik Arm. The Southern Alignment, with its accompanying proposed Below-the-Bluff Roadway on the Anchorage approach, would be the most technically feasible and practical alignment that would avoid the Cairn Point Trench (a submarine trough), would not affect military mission and operations at Elmendorf, and would minimize potential impacts to beluga whales that congregate in areas of Knik Arm further to the north.

An 8,200-foot-long pier-supported bridge is preferred over a 14,000-foot-long pier-supported bridge because, in addition to lower construction costs, a shorter bridge would require fewer piers—meaning shorter in-water construction time and, therefore, less construction noise and pile-driving impacts that might adversely affect beluga whales and marine fishes.

The preferred Anchorage approach to the proposed bridge would be a cut-and-cover tunnel under Government Hill, using either the proposed Degan or Erickson Alternative to connect initially to the existing A-C Couplet and, in Phase 2, to the Ingra-Gambell Couplet.

All reasonable alternatives evaluated in the Draft EIS are under consideration and have been developed to a comparable level of detail. Final identification of a Preferred Alternative will not occur until the alternatives, impacts, written comments on the Draft EIS, and comments received at the public hearings have been fully evaluated and considered. The final Preferred Alternative will be provided in the Final EIS.

### **3.0 SECURITY DEFINITION AND GENERAL ISSUES**

Security is assumed to be different from safety, although the requirements for each may overlap. Security can be defined as measures taken to guard against illegal acts such as crime, attack, sabotage, espionage or trespass. Safety can be defined as measures taken to guard against accidents and natural hazards. Security measures may include fencing, signage, lighting, structure blast resistance, monitoring and patrols. Safety requirements such as minimum lane widths and guard rails are not directly considered in a security evaluation.

Security was reviewed in the context of maintaining restricted access to nearby properties and the proposed KAC bridge and approach roads. Extreme security issues such as terrorist attacks and weapons of mass destruction were not directly considered. In the aftermath of the terrorist attacks of September 11, 2001, issues relating to structural design and security are matters of increasing concern. However, clear policy has yet to develop regarding to what degree transportation structures/facilities are to be protected from and hardened against terrorist attack, compared to historic security measures

inherent to most major public works projects. The Department of Homeland Security, through the U.S. Coast Guard, has developed initial standards for protection of ports and facilities that represent an entry point into the United States.

The value of a particular structure, whether as a national icon or signature span, or its commercial value as a transportation link is an important determinant with regard to the level of necessary security. For the purposes of this security evaluation it is assumed that the proposed KAC facilities and structures would not be vital to national security, nor would they create a signature span structure. Construction of the project would provide a beginning point of future regional expansion and prosperity, not a loss against current levels of transportation activity.

While the proposed KAC bridge itself might not require exceptional security measures, nearby facilities and military bases do have important security concerns, specifically the POA, Elmendorf Air Force Base (Elmendorf) and Fort Richardson Military Base (Fort Richardson), which adjoin or are in the vicinity of proposed alignments for the bridge crossing. The POA is designated one of fifteen “Strategic Ports,” partly because of its location near Fort Richardson. Fort Richardson is planned as the home base for a rapidly deployable “Stryker” brigade.

The facilities below have been identified as being effected by one or more of the proposed alignments. While their security concerns may be partially addressed by current national codes and standards, a thorough security evaluation would require information about specific security standards and plans from the impacted properties and facilities:

- POA
- Port MacKenzie
- Elmendorf
- Fort Richardson
- Alaska Railroad

Table 3-1 lists some security issues relating to the proximity of the proposed project to adjacent sensitive facilities. Additional issues are discussed below in the relevant sections. In general, fencing would be anticipated as the primary method for providing security, although fencing would not necessarily be adequate by itself. Fencing would likely be provided along the at-grade and depressed road alignments and where the alignments would pass adjacent to or through military bases and secure areas.

**Table 3-1: Project Security Issues**

	Security Issue	Affected Facility
1	Access from right-of-way to Elmendorf	Elmendorf
2	Access from right-of-way to the POA	POA
3	Access from the right-of-way to the Alaska Railroad	Alaska Railroad
4	Access from the right-of-way to Fort Richardson	Fort Richardson
5	Secure access to the KABATA toll booth/conflict with main gate of Elmendorf	Municipality of Anchorage
		POA
		Elmendorf
6	Proximity to the POA tank farm	POA
7	Encroachment of the Cherry Hill military housing development	Elmendorf
8	Secured access at the port interchange/dedicated military port access	POA
		Elmendorf
9	Access from right-of-way to Port MacKenzie	Port MacKenzie and Mat-Su Borough

#### **4.0 REGULATIONS AND LITERATURE REVIEW**

Since the attacks of September 11, 2001, security has assumed increased importance. A number of new regulations, reports, studies and planning tools have been developed for ports, highways and transportation projects in the United States. However, areas of uncertainty exist. For example, it is not clear to what extent state departments of transportation (DOT) are responsible for security. Also, although methods exist for evaluating the security of existing structures, it is not clear what methods should be applied for projects in the planning and design phase. A well-established method for assessing risk has not been developed. Risk assessments are typically done by applying methods developed for seismic and other natural hazards.

A number of organizations have produced reports concerning transportation security, including the American Association of State Highway Transportation Officials (AASHTO), Federal Highway Administration (FHWA), Transportation Security Administration (TSA) and DOTs. However, laws, regulations and code requirements are not as extensive.

The “Guide to Highway Vulnerability Assessment for Critical Identification and Protection” (AASHTO, 2002) is commonly referenced and includes assessment methodologies to define threats, vulnerabilities and potential countermeasures. An ongoing research program aims to replace this with an expanded and enhanced guide applicable to multiple transportation modes. The National Cooperative Highway Research Program (NCHRP) is developing a “Guide to Risk Management of Multi-Modal Transportation Infrastructure” with a scheduled completion date of August 2006 (NCHRP, 2005).

The Maritime Transportation Security Act of 2002 resulted in a number of rules that affect transportation projects. Information is included in the Final Rules on Maritime Security (33 CFR 101). Federal regulations require that any facility or vessel that may be

involved in a transportation security incident conduct a vulnerability assessment and submit a security plan to the U.S. Coast Guard (Transportation Security Agency, 2003). A marine vulnerability self-assessment tool has been developed by the TSA to assist facility and vessel owners in complying with the regulations. Maritime security is not a focus of the proposed KAC project. However, TSA is developing similar tools for highway bridges and other transportation elements. These additional tools may be applied when they become available.

In addition to the marine vulnerability self-assessment, the U.S. Coast Guard provides a method for assessing facility security in Navigation and Inspection Circular No. 11-02, Change 1 (U.S. Coast Guard, 2004), attached as Appendix A. The document outlines a process called “Risk Assessment Methodology” (RAM). The RAM process has been applied as part of this preliminary security evaluation and the results are reported in the body of this document.

The TSA has relatively new security evaluation tools, TRAVEL and VISAT, which are oriented toward existing facilities. TRAVEL is a facilitated vulnerability assessment conducted by government-led teams. VISAT is a self-administered tool for identifying vulnerabilities. Inquiries about these programs were made as part of this security evaluation. However, no clear response was received from the TSA concerning how to request or obtain these tools. The programs are in their start-up phase and seem to have only been used once or twice by others. Use of these programs may be appropriate during design.

Further guidance regarding transportation security has been established by FHWA in the report “Recommendations for Bridge and Tunnel Security” (FHWA, 2003). The report is a product of the “Blue Ribbon Panel” of experts selected by FHWA from the fields of highway and tunnel design, heavy civil construction, and academia. The charter for the panel was to “develop short and long-term strategies for improving the safety and security of the nation’s bridge and tunnels ... and provide guidance to highway infrastructure owners/operators.”

The FHWA report includes specific recommendations for protection of structures and facilities that are vital to national security, represent a signature span, or provide a vital economic link. The report includes the following quote regarding security requirements:

Unlike the case of natural hazards we are in the dawn of an era in which asset owners feel overwhelmed by uncertainties about the occurrence and potential costs of terrorist attacks and about their legal responsibilities to protect the users of their facilities. (FHWA, 2003).

Many issues and recommendations in the FHWA report are relevant to large transportation projects, although not necessarily to the proposed KAC project. For the proposed KAC project, security evaluation follows security standards typical for most projects of this nature in the United States.

## **5.0 SECURITY ANALYSIS – PROPOSED KNIK ARM CROSSING PROJECT**

This section of the report analyzes the effect of the project on security of the proposed project elements: highway, bridge and pathway. A standard quantitative method does not exist for analyzing security risks. A common practice is to apply the techniques for analyzing natural hazards, such as seismic risk analysis and hurricane impact analysis, to security issues.

One process for assessing security risk is the RAM. RAM was applied to security risks for the U.S. Department of Energy in 2002 as part of a federal research and development project. It is used to evaluate the need for specific security measures or evaluate alternate measures. It has since been adopted by the U.S. Coast Guard, and is referred to in their recommended security guidelines for facilities (U.S. Coast Guard, 2004). In addition, RAM is at the core of tools developed for assessing risk at dams and transmission lines, called RAM-D and RAM-T, respectively. The systematic process is described in Appendix A and includes threat assessment, consequence assessment and vulnerability assessment. The results of the RAM analysis for the proposed KAC bridge are summarized in Table 5-1.

The RAM process is applied in this report as a preliminary analysis and to illustrate the method. A more thorough analysis would require meetings and discussions with a number of interested parties.

### **5.1 Bridge and Tunnel Security**

Bridge and tunnel security are an issue of increasing concern. In addition to the proposed bridge, the proposed KAC project would involve a tunnel under the Government Hill neighborhood. General security measures applicable to both bridges and tunnels would include fencing, signs, closed circuit television (CCTV) monitoring, intrusion detection devices, access control devices, lighting, emergency call boxes, and security patrols. Bridge security measures could include restricting access to structural support elements, and designing the bridge to have suitable structural redundancy and reserve load capacity. Tunnel security measures could include restricting certain types of cargo and vehicles types from tunnels.

In general, public access to proposed bridge and tunnel facilities and right-of-way should be controlled. Non-public areas should be securely fenced or provided with physical barriers to entry. The proposed alignment and structure type for the proposed KAC project would result in pedestrian traffic across the alignment, and beneath the overhang of the bridge deck. Note that a rigid application of security guidelines may conflict with other project objectives, such as public use of trails and pathways. Table 5-1 summarizes the risk assessment for the proposed KAC bridge structure. Table 5-2 summarizes the risk assessment for the proposed Government Hill tunnel. The method and terminology are described in Appendix A.

**Table 5-1: Risk Assessment Method (RAM) summary – proposed Knik Arm Crossing bridge**

Scenario/Description		Consequence Level	Vulnerability Score			Mitigate, Consider or Document
			Accessibility	Organic Security	Total Score	
1	Barge/ship collision with a bridge pier	3	2	2	4	Mitigate
2	Pedestrian tampering with bridge structural members	3	2	2	4	Mitigate
3	Criminal activity targeting pedestrians on the bridge	2	2	2	4	Consider
4	Unauthorized fishing or hunting from the bridge	1	2	1	3	Document

**Table 5-2: Risk Assessment Method (RAM) summary – proposed Government Hill tunnel**

Scenario/Description		Consequence Level	Vulnerability Score			Mitigate, Consider or Document
			Accessibility	Organic Security	Total Score	
1	Accident or malevolent act creating a hazardous pollution incident in the tunnel	2	2	2	4	Consider
2	Criminal activity targeting pedestrians	1	2	2	4	Document

## 5.2 Multi-use Pathway

Proposed multi-use pathways could be a security problem to users. In general, pathways should be well illuminated and designed to avoid dark or remote passageways, dead ends, regions with thick vegetation, and other areas that cannot be readily viewed or patrolled. The proposed pathways should promote public use and be visible from the roadway to discourage potential undesirable activity.

## 6.0 SECURITY ANALYSIS – NEARBY PROPERTIES AND FACILITIES

This section of the report analyzes the effect of the proposed project on security of nearby properties, public facilities, ports and military bases, and describes the civilian police forces.

Construction of the proposed KAC project would reduce travel time between areas of the Mat-Su and Anchorage, resulting in decreased response time for police and emergency vehicles when providing assistance to jurisdictions on the opposite side of Knik Arm. Thus, residents of some areas of the Mat-Su would have decreased travel time to hospitals in Anchorage.

### 6.1 Municipality of Anchorage

Anchorage has a population of approximately 260,000 people. The proposed KAC project is not expected to create increased security requirements for the Municipality.

Anchorage is served by a police force with 264 sworn officers and 522 employees. Specialized teams include Special Weapons and Tactics (SWAT), Hostage Negotiation and a Bomb Team (APD, 2005). Hospitals include Providence Alaska Medical Center, Alaska Native Medical Center, and Alaska Regional Hospital. Emergency medical response and helicopter “air ambulance” services are available.

## **6.2 Matanuska-Susitna Borough**

The Mat-Su Borough is on the western side of the Knik Arm Crossing. Police services are provided by Alaska State Troopers, although there has recently been discussion of forming a local police force. The Mat-Su Regional Medical Center is located in Palmer. A state correctional facility (minimum security work camp) is located approximately 10 miles north of Point MacKenzie.

The proposed KAC project would not be expected to create increased security requirements for the Mat-Su Borough government.

## **6.3 Private Properties**

A preliminary review of land use maps did not identify any private properties that would have special security requirements. The proposed KAC project would not be expected to create increased security requirements for private properties. Note, however, that tenants on POA land operate tank farms for the storage of petroleum products. Adequate security for these tank farms should be coordinated with the POA security plan.

## **6.4 Port MacKenzie**

Port MacKenzie is a port on the west side of Knik Arm that serves the Mat-Su. It includes a 500-foot-long wharf, and a deep draft dock with a mooring length of 1,200 feet. Figure 6.1 is an aerial photo of Port MacKenzie including a rendering of the deep draft dock (right side of figure), proposed upland improvements, and a proposed dock (left side of figure). Port MacKenzie includes approximately 9,000 acres of adjacent upland.

Port MacKenzie is required to maintain a Facilities Security Plan in accordance with the U.S. Coast Guard’s Navigation and Vessel Inspection Circular No. 11-02, including fence, lighting, vehicle barrier, and gate requirements to secure the port facilities. This plan is SSI and has not been reviewed. However, it is expected that the proposed KAC project would not create additional security issues for Port MacKenzie.



**Figure 6.1.** Port MacKenzie with a rendering of improvements (Mat-Su 2005).

## **6.5 Port of Anchorage**

The POA operates a five-berth terminal providing facilities for the movement of containerized freight, iron and steel products, bulk petroleum and cement. An estimated 5.0 million tons of various commodities moved across the POA's docks in 2005. A 129-acre industrial park adjoins the POA to the east. The POA is implementing an expansion plan that includes new docks, cranes and other facilities (Port of Anchorage 2005). Figure 6.2 is an aerial photo including the POA's expansion plans footprint. All POA properties are contiguous and are included in Figure 6.2. Table 6-1 summarizes a preliminary risk assessment for the POA.

Cruise ship visits are infrequent and usually consist of smaller sized "pocket" cruise ships. Cruise ships typically dock at one of the POA terminals. Most cruise ship visits in the region are to Whittier and Seward. The POA is planning to improve its cruise ship facilities, including providing a secure cruise ship terminal.

POA properties and roads have been closed to the general public since October 2001. All inbound traffic to the POA is monitored and drivers and individuals entering the POA must have proper identification and a port sponsor. Permit decals are issued to qualified individuals and businesses having a reason to enter POA property.



**Figure 6.2.** 2002 aerial photo with POA Expansion Plan footprint (Port of Anchorage 2005).

**Table 6-1:** Risk Assessment Method (RAM) summary – Port of Anchorage

Scenario/Description	Consequence Level	Vulnerability Score			Mitigate, Consider or Document
		Accessibility	Organic Security	Total Score	
1 External attack from the right-of-way using a weapon to damage oil tank farm	3	2	2	4	Mitigate
2 Gain unauthorized access to the port facilities via the Elmendorf/POA access road	3	2	2	4	Mitigate
3 Unauthorized access from waterways	3	2	2	4	Mitigate
4 Transport people into/out of country through the port	2	2	2	4	Consider
5 Transport contraband/cash into/out of country through the POA	2	2	2	4	Consider

A site visit was made to the POA in August and security issues were discussed with the Port Operations Manager. The POA adjoins Elmendorf, which has security patrols and fencing that also benefit security for the POA. Security on the water side of the POA is provided by the U.S. Coast Guard.

The proposed Anchorage-side alignment alternatives would encroach on POA property on its northern end. There would likely be no adverse impact on security at the POA’s southern end including tenant-occupied lands.

The Captain of the Port makes the final decision on security-related issues. The security program is managed by the Port Operations Manager. The POA is in the process of upgrading security, including installing video monitoring cameras and improving fencing. A number of government agencies and groups have studied the POA's security and done vulnerability assessments. The results of these studies have not been reviewed for this security evaluation. The POA is currently in compliance with federal regulations concerning security.

The POA has not expressed an opinion on which alignment alternative would be preferable. The POA has identified facilities that are sensitive, however, this information is restricted. The petroleum storage tanks at the southeast corner of the POA are a security concern. In general, POA security is improved by providing a standoff distance and physical barrier such as a fence between POA facilities and areas open to the public, and lighting is desirable.

Note that a 129-acre industrial park is located east of the POA. Eighty-one acres of the park are leased to tenants, each of which has its own security plan. However, the port and its tenants cooperate in developing security plans. There is only one access point into the POA and tenant occupied lands, and access to all leased land is through the main POA access.

The POA is required to maintain a Facilities Security Plan as required by the U.S. Coast Guard's Navigation and Vessel Inspection Circular No. 11-02, including fence, lighting, vehicle barrier, and gate requirements to secure the POA facilities. This plan is SSI and has not been reviewed. A confidential security evaluation based on SSI may be appropriate.

## **6.6 Airfield and Flight Paths**

Four airfields are located in Anchorage, and a number of private airstrips in Mat-Su are near the proposed KAC project. The Elmendorf runways are a constraint in locating the proposed project alignment alternatives. Bryant Airfield at Fort Richardson is east of Elmendorf. Security issues concerning these military runways are discussed in the next section.

Two civilian airfields are located south of the proposed KAC project. Ted Stevens Anchorage International Airport is 3 miles southwest of Downtown Anchorage. Merrill Field is approximately one-half mile south of Elmendorf, near Downtown Anchorage.

Detailed analysis of airport and flight clearance requirements is not included in this security evaluation. If the proposed project would involve intrusion into airfield clear zones, then a separate airport operations impact analysis would be recommended. Federal Aviation Regulations (FAR) and special rules specific to the Anchorage area should be reviewed and their effect on the proposed KAC project evaluated. FAR Part 77 "Objects Affecting Navigable Airspace" is a regulation controlling the height of objects

in the vicinity of airfields. Airfields are also discussed below in the section on military bases.

Airports are sensitive facilities and subject to federal security regulations and planning requirements. A confidential security evaluation based on SSI may be appropriate for the region’s civilian and military airfields. Table 6-2 summarizes a preliminary risk assessment for civilian airports in the region.

**Table 6-2: Risk Assessment Method (RAM) summary – Civilian Airports**

Scenario/Description	Consequence Level	Vulnerability Score			Mitigate, Consider or Document
		Accessibility	Organic Security	Total Score	
1 Damage/destroy airfield facilities or aircraft	3	2	1	3	Mitigate
2 Hijack airplane and take passengers hostage	3	2	1	3	Mitigate
3 Launch or shoot weapons from a distance	2	2	1	3	Consider
4 Move people into/out of country	2	2	1	3	Consider
5 Move contraband/cash into/out of country	2	2	1	3	Consider

## 6.7 Military Bases

There are two active military bases in the area. Elmendorf is a strategic air base. Fort Richardson is a base for the 172nd Stryker Brigade. Both bases have increased security needs and a heightened military mission, partly as a result of the attacks of September 11, 2001. Military bases are sensitive facilities and have a range of security requirements. New security measures may constrain the route alternatives. The Circularly Disposed Antenna Array (CDAA) at Elmendorf is a significant constraint because of the requirement for a one-mile clear zone around the CDAA. In addition to the one-mile clear zone, a three-mile restriction zone is in effect for some activities. The zones are required in part to avoid adverse impacts to the Electro-Magnetic Compatibility (EMC) of the base (ADOT, 2003). EMC is required to avoid interference with electronic equipment including communications, surveillance and navigation systems. The CDAA is operated by the National Security Agency. Although the proposed Southern Alignment and Below-the-Bluff Roadway are within the one-mile CDAA clear zone, they would be shielded from the CDAA by the bluff, eliminating the interference concern.

The proposed KAC alignments would need to comply with the 3,000 foot air-clearance zone at the end of the runways. However, the proposed pile-supported bridge that has a low profile and does not use towers would make interference with runway approach paths unlikely.

Lighting for the proposed crossing and/or security has the potential to impact Elmendorf. Lighting could interfere with runway lighting and could potentially affect the EMC.

An eroding bluff area north of Cairn Point is an old military landfill and could be a security concern if materials were to become exposed. This should not be an issue, however, as the proposed alignment alternatives avoid the landfill.

Fort Richardson may be consolidated with Elmendorf in accordance with the recommendations of the 2005 Base Realignment Commission (BRAC). However, it is likely that the overall boundaries or land uses on the military bases will not change. Detailed land use plans for the military bases are not currently available.

**Table 6-3: Risk Assessment Method (RAM) summary – Military Bases**

Scenario/Description		Consequence Level	Vulnerability Score			Mitigate, Consider or Document
			Accessibility	Organic Security	Total Score	
1	Gain unauthorized entry into the facility due to right-of-way proximity to Elmendorf main gate	3	1	1	2	Consider
2	External attack on Cherry Hill housing with a firearm	3	2	1	3	Mitigate
3	Gain unauthorized entry into Elmendorf via the Elmendorf/POA access road	3	2	1	3	Mitigate
4	Espionage	2	2	1	3	Consider
5	Damage to equipment	2	2	1	3	Consider
6	Theft of equipment or weapons	3	1	1	2	Consider
7	Trespass/access to the Elmendorf runway	2	2	1	3	Consider

Information has been requested from the military bases, but a response was not received during the study period. A confidential security evaluation based on SSI may be appropriate for Elmendorf and Fort Richardson. Specific requirements for security fencing, lighting, vehicle barriers, gates and other security measures have not been obtained. Table 6-3 summarizes a preliminary risk assessment for the military bases in the region.

## **6.8 Alaska Railroad**

Anchorage is served by the Alaska Railroad. The Alaska Railroad has lines connecting Anchorage to Seward and Whittier to the south, and Fairbanks to the north. In addition, the railroad owns approximately 963 acres of land in Anchorage. The railroad’s northbound line runs from the POA northwest through Elmendorf. A railroad and highway tunnel connects Whittier to Anchorage (described in the next section). However, the proposed KAC project would not affect this tunnel.

A site visit was made to the Alaska Railroad offices near the POA, and security issues were discussed with the Chief of Security. Security issues for the railroad are closely related to the POA and their tenants, which are crossed by the railroad and include rail yards.

## **6.9 Roads and Highways**

The current highway route connecting the Mat-Su and Anchorage is along Glenn Highway from Anchorage to the end of Knik Arm, then connecting to the Parks Highway to travel to Wasilla and Houston in the Mat-Su. The Glenn Highway passes through Fort Richardson. The Glenn and Parks Highways are part of the National Highway System. The proposed KAC project would provide a more direct route between Anchorage and areas of the Mat-Su.

The Whittier tunnel is the only major tunnel in the region, approximately 40 miles from the proposed KAC project. The proposed KAC project would not affect tunnel security or adversely impact the security of other roads and highways in the region.

## **6.10 Pedestrian Pathways**

A number of trails and pathways exist in the region. A new pathway is proposed as part of the proposed KAC project. A pathway could be a potential security concern as it would provide a potential means for the public to access adjoining properties. A pathway may require patrols, lighting and other measures to discourage undesirable activity.

## **6.11 Easements and Public Rights-of-Way**

Existing easements and rights-of-way have not been analyzed separately. It is assumed that the public has the right to use the existing roads and trails in the region. Additional easements may exist along routes that have not been developed and where no road or trail exists. Construction of new roads and trails as part of the proposed KAC project could conceivably make previously unused easements available to the public. A title search is recommended to identify easements that may not be currently in use, but which may create a security issue should they become accessible to the public.

## **6.12 Parks and Open Spaces**

Chugach State Park, immediately east of Anchorage, is the largest public park in the area. Other large public parks on the Anchorage side of Knik Arm include Kincaid Park, Russian Jack Park and the Far North Bicentennial Park. Public parks and open spaces on the Mat-Su side of Knik Arm include Nancy Lake State Recreation Area, Susitna Flats State Game Refuge, Goose Bay State Game Refuge, and Palmer Hay Flats State Game Refuge. The proposed KAC project is unlikely to adversely affect security at these existing parks and open spaces.

### **6.13 Utilities and Pipelines**

Numerous utilities either cross the proposed alignment alternatives or are in their vicinity. The utilities include water, sewer, electrical and gas lines. Utilities are analyzed in the “Utilities Impacts Technical Report” which concludes that impacts of the proposed KAC project to utilities would not be significant. Burial of utilities usually provides sufficient security. Utilities exposed on the surface may require security measures. The Municipality of Anchorage owns the local water, wastewater, refuse and one of the electrical power utilities.

The Anchorage Water and Wastewater Utility (AWWU) is the largest provider of water and sewer services in Alaska, and serves Anchorage and nearby communities. AWWU collects water from two major surface watersheds, Eklutna Lake and Ship Creek, and several deep underground wells (AWWU 2005). AWWU also provides sewer services to Anchorage and the surrounding region. Treated wastewater is discharged to Cook Inlet, Eagle River and Glacier Creek.

Municipal Light and Power provides electrical power service to parts of Anchorage. Chugach Electric Association supplies power to the region via above-ground powerlines and also supplies power to parts of Anchorage.

Local telephone service is available from General Communications Inc. (GCI) and Alaska Communication Systems (ACS), as well as Matanuska Telephone Association. These and other companies also provide long-distance phone and other telecommunications services.

Natural gas is provided by Enstar Natural Gas Company. Gas mains are near the proposed alignment alternatives, including a 4-inch line crossing Degan Street between E. Manor Avenue and E. Harvard Avenue.

## **7.0 RECOMMENDATIONS**

A number of security measures are available for public transportation projects. Security measures can include fencing, signs, closed circuit television (CCTV) monitoring, intrusion detection devices, access control devices, lighting, emergency call boxes, security patrols, and restricted access for certain types of cargo and vehicles. Security can also be improved by policies such as keeping an area clean and free of graffiti, debris and other conditions that can create a sense of insecurity.

As shown in Table 7-1, the primary recommended security measure for the proposed KAC project is fencing that meets Department of Defense standards. Fencing could be constructed along the at-grade and depressed road alignments and where the alignments passed through military bases and secured areas. Secondary to fencing and physical barriers the following measures would also increase security and should be considered during design:

- Establish a secure perimeter or corridors to control access by pedestrians or vehicles
- Eliminate vegetation that provides cover for people or equipment
- Provide inspection surveillance either remotely or via security forces
- Ensure that items are prominent and visible
- Provide lighting
- Minimize loitering time for vehicles and/or people in sensitive areas

Coordination with nearby military bases, ports and other facilities would be required during planning and design to determine specific security requirements and ensure they are addressed. The primary security measure that would be needed is fencing. Fencing, lighting and other security measures should be included in the design and described in a project manual.

Additional security evaluation work should be considered using the relatively new TRAVEL and VISAT programs offered by the TSA. TRAVEL is a facilitated vulnerability assessment conducted by government-led teams. VISAT is a self-administered tool for identifying vulnerabilities.

Security would require regular inspection of facilities and operations and maintenance measures (O&M). Security lighting would require replacement of light bulbs. Fencing could be damaged by large animal migration (moose) and by poor soils and slope movement. O&M and inspection requirements could be described in a project manual.

**Table 7-1: Security recommendations**

	Security issue	Recommendations
1	Access from right-of-way to Elmendorf	Security fencing
2	Access from right-of-way to POA	Security fencing and lighting
3	Access from the right-of-way across Alaska Railroad line	Security fencing
4	Access from the right-of-way to Fort Richardson	Security fencing
5	Secure access to the KABATA toll booth/conflict with main gate of Elmendorf	Fencing, lighting, video monitoring and vehicle barrier
6	Relocation of the main gate to Elmendorf	Fencing and vehicle barrier
7	Proximity to the POA tank farm	Security fencing
8	Encroachment of the Cherry Hill military housing development	Security fencing
9	Secured access at the POA interchange/dedicated military POA access	Security fencing
10	Access from right-of-way to Port MacKenzie	Security fencing

## **8.0 References**

- Alaska DOT. 2004. Knik Arm Crossing Engineering Feasibility and Cost Estimate Update, 2004. Project Estimate Update Technical Memorandum, State Project No. 56047, Volumes 1-3.
- AASHTO. 2002. A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection. Prepared by SAIC, Washington, D.C.
- Alaska Water and Wastewater Utility. 2005. Overview of Anchorage Water and Wastewater Utility. <<http://www.awwu.biz/website/AboutAWWU/aboutawwu.htm>> Viewed July 15, 2005.
- Anchorage Municipal Light and Power. 2005. Service Area Map. <[http://www.mlandp.com/new%20paint/map\\_page.htm](http://www.mlandp.com/new%20paint/map_page.htm)> Viewed July 15, 2005.
- APD. 2005 “Anchorage Police Department” <<http://www.muni.org/apd2/askapdanswers.cfm>> Viewed September 8, 2005.
- Federal Aviation Regulation, Part 77. 2006. Objects Affecting Navigable Airspace.
- Federal Highway Administration. 2003. Recommendations for Bridge and Tunnel Security. Prepared by the AASHTO/FHWA Blue Ribbon Panel on Bridge and Tunnel Security, FHWA-IF-03-036.
- Final Rules on Maritime Security. 2002. U.S. Code of Federal Regulations, 33 CFR, Subchapter H, Parts 101-106.
- KABATA. 2005. Knik Arm Crossing Area Basemap. <[http://www.knikarmbridge.com/project\\_docs.html](http://www.knikarmbridge.com/project_docs.html)> Viewed July 15, 2005.
- KABATA. 2004. Aerial photo – Port of Anchorage, Knik Arm Bridge and Toll Authority 2004 Annual Report. <<http://www.knikarmbridge.com/documents/KABATAANNUALREPORT2004-1.pdf>> Viewed July 15, 2005.
- Matanuska-Susitna Borough. 2005. Port MacKenzie Project Update. <<http://www.matsugov.us/Port/portprojectinfo.cfm>> Viewed October 5, 2005.
- Municipality of Anchorage: Municipal Traffic Department. 2003. Municipality of Anchorage Park and Major Trails Map, August 2003.
- NCHRP. 2005. Guide to Risk Management of Multimodal Transportation Infrastructure: National Cooperative Highway Research Program Project 20-59(17). <<http://www4.trb.org/trb/crp.nsf/0/4f66b8813755221c85256fbf00521f7f?OpenDocument>> Viewed July 15, 2005.

Port of Anchorage. 2005. Port of Anchorage – Background. <<http://www.muni.org/port/>> Viewed July 15, 2005.

Texas DOT. 2002. Design of Bridges for Security: The National Pooled Fund Project TPF-5(056), TxDOT Project No. 0-4569. <[www.pooledfund.org/orgdetails.asp?id=139](http://www.pooledfund.org/orgdetails.asp?id=139)> Viewed May 1, 2006.

Transportation Security Administration. 2003. TSA Maritime Vulnerability Self-Assessment Tool: Federal Register, 68 FR No. 234, 68096-68097; 05 December 2003.

U.S. Coast Guard. 2004. Guidelines on Assessing Facility Security Measures: Enclosure 1 to Navigation and Vessel Inspection Circular No. 11-02, Change 1, CH-1 to NVIC 11-02, Recommended Security Guidelines For Facilities.

U.S. Department of Defense. 1994. Security Engineering Project Development. TM 5-853-1.

U.S. Department of Defense. 1994. Security Engineering Concept Design. TM 5-853-2.

U.S. Department of Defense. 1994. Security Engineering Final Design. TM 5-853-3.

**Appendix A**  
**Guidance on Assessing Facility Security Measures**  
**(8 pages)**

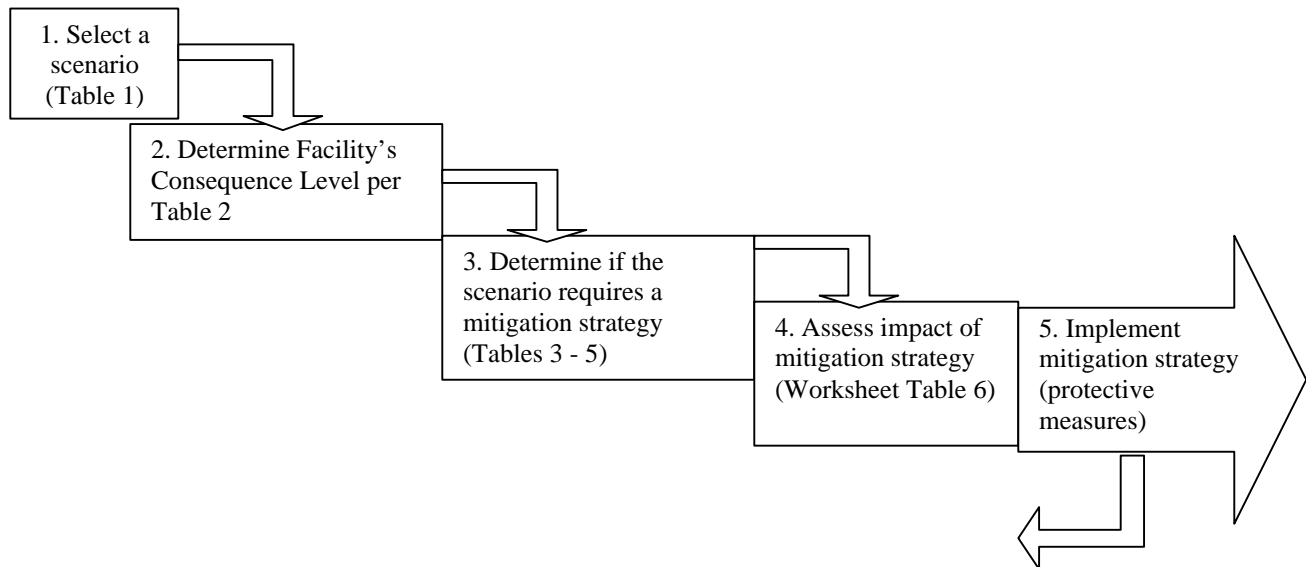
**Guidance on Assessing Facility Security Measures**

A security assessment performed in accordance with this enclosure may be used to evaluate the need for specific measures or evaluate alternate measures.

Risk-based decision-making is one of the best tools to perform a security assessment and to determine appropriate security measures for a facility. Risk-based decision-making is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function and to identify actions that will reduce the vulnerability to and mitigate the consequences of a security breach.

A security assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses. For example, a security assessment might reveal weaknesses in an organization’s security systems or unprotected access points such as the facility’s perimeter not being lighted or gates not being secured or monitored after hours. To mitigate this vulnerability, a facility would implement procedures to ensure that such access points are secured and verified by some means. Another security enhancement might be to place locking mechanisms and/or wire mesh on doors and windows that provide access to *restricted areas* to prevent unauthorized personnel from entering such spaces. Such assessments can identify vulnerabilities in facility operations, personnel security, and physical and technical security.

The following is a simplified risk-based security assessment, outlined in the following flow chart, which can be further refined and tailored to specific *facilities*. The process and results should be documented, (example provided in Table 5), when performing the assessment.



Note: Repeat process until all unique scenarios have been evaluated.

**STEP 1: POTENTIAL THREATS**

To begin an assessment, a facility or company needs to consider attack scenario(s) that consist of a potential threat to the facility under specific circumstances. It is important that the scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents as given by a threat assessment. They should also be consistent with scenarios used to develop the Port Security Plan. For example, a bomb threat at a major petrochemical facility is one credible scenario. Table 1 provides a notional list of scenarios that may be combined with specific critical targets to develop the scenarios to be evaluated in the Facility Security Assessment.

The number of scenarios is left to the judgment of the facility or company. An initial evaluation should at least consider those scenarios provided in Table 1. Care should be taken to avoid unnecessarily evaluating an excessive number of scenarios that result in low consequences. Minor variations of the same scenario also do not need to be evaluated separately unless there are measurable differences in consequences.

**Table 1: Notional List of Scenarios**

<b>Typical Types of Scenarios</b>		<b>Application Example</b>
<b>Intrude and/or take control of the target and ...</b>	Damage/destroy the target with explosives	Intruder plants explosives.
	Damage/destroy the target through malicious operations/acts	Intruder takes control of a facility intentionally opens valves to release oil or hazmat that may then be ignited.
	Create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release oil or toxic materials or releases toxic material brought along.
	Take hostages/kills people	Goal of the intruder is to kill people.
<b>Externally attack the facility by ...</b>	Launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc to damage or destroy bulk storage tanks, dangerous cargo, etc.
<b>Use the facility as a means of transferring ...</b>	Materials, contraband, and/or cash into/out of the country	Facility is used as a conduit for <i>Transportation security incidents</i>
	People into/out of the country	

**STEP 2: CONSEQUENCE ASSESSMENT**

For this step a *Facility Security Officer* or company official should determine the appropriate consequence level (3, 2, or 1) determined from Table 2. The appropriate consequence level should be based on the “Description” of the facility (i.e., one that transfers, stores, or otherwise contains *certain dangerous cargoes* would have a “3” consequence level).

**Table 2: Consequence Level**

<b>Consequence Level</b>	<b>Description</b>
<b>3</b>	<i>Facilities that transfer, store, or otherwise handle a certain dangerous cargoes</i>
<b>2</b>	<i>Facilities that</i> (1) <b>Are subject to 33 CFR Parts 126 and 154 (other than certain dangerous cargoes);</b> (2) <b>Receive vessel(s) that are certificated to carry more than 150 passengers (other than those required to comply with 33 CFR 128); or</b> (3) <b>Receive vessels on international voyages including vessels solely navigating the Great Lakes</b>
<b>1</b>	<i>Facilities, other than those above.</i>

**STEP 3: VULNERABILITY ASSESSMENT**

Each scenario should be evaluated in terms of the facility’s vulnerability to an attack. Four elements of vulnerability could be considered in the vulnerability score: availability, accessibility, organic security, and facility hardness, described as follows:

<b>AVAILABILITY</b>	The facility’s presence and predictability as it relates to the ability to plan an attack.
<b>ACCESSIBILITY</b>	Accessibility of the facility to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
<b>ORGANIC SECURITY</b>	The ability of security personnel to deter the attack. It includes security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.
<b>FACILITY HARDNESS</b>	The ability of the facility to withstand the specific attack based on the complexity of facility design and material construction characteristics.

The *Facility Security Officer* or company official should discuss each vulnerability element for a given scenario. The initial evaluation of vulnerability should be viewed with only existing strategies and protective measures, designed to lessen vulnerabilities, which are already in place. After the initial evaluation has been performed, a comparison evaluation can be made with new strategies and protective measures considered. Assessing the vulnerability with only the existing strategies and protective measures will provide a better understanding of the overall risk associated with the scenario and how new strategies and protective measures will mitigate the risk.

With the understanding that the facility has the greatest control over the accessibility and organic security elements, this tool only takes into consideration these elements (not addressing availability or facility hardness) in assessing each scenario. The vulnerability score and criteria with benchmark examples are provided in the following table. Each scenario should be evaluated to get an accessibility and organic security score. Then sum these elements to get the total vulnerability score (step 3 in Table 5). This score should be used as the vulnerability score when evaluating each scenario in the next step.

**Table 3: Vulnerability Score**

<b>Score</b>	<b>Accessibility</b>	<b>Organic Security</b>
<b>3</b>	No deterrence (e.g. unrestricted access to facility and unrestricted internal movement)	No deterrence capability (e.g. no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability)
<b>2</b>	Fair deterrence (e.g. single substantial barrier; unrestricted access to within 100 yards of bulk storage tanks)	Fair deterrence capability (e.g. minimal security plan, some communications, security force of limited size relative to the facility; outside law enforcement with limited availability for timely prevention, limited detection systems)
<b>1</b>	Good deterrence (expected to deter attack; access restricted to within 500 yards of bulk storage tanks; multiple physical/geographical barriers)	Good deterrence capability expected to deter attack (e.g., detailed security plan, effective emergency communications, well trained and equipped security personnel; multiple detection systems [camera, x-ray, etc.], timely outside law enforcement for prevention).

**STEP 4: MITIGATION**

The facility or company should next determine which scenarios should have mitigation strategies (protective measures) implemented. This is accomplished by determining where the scenario falls in Table 4 based on the consequence level and vulnerability assessment score. Table 4 is intended as a broad, relative tool to assist in the development of the *Facility Security Plan*. “Results” are not intended to be the sole basis to trigger or waive the need for specific measures, but are one tool in identifying potential vulnerabilities and evaluating prospective methods to address them.

The following terms are used in Table 4 as mitigation categories:

**“Mitigate”** means that mitigation strategies, such as security protective measures and/or procedures, should be developed to reduce risk for that scenario. An appendix to the *Facility Security Plan* should contain the scenario(s) evaluated, the results of the evaluation, and the mitigation measures chosen.

**“Consider,”** means that mitigation strategies should be developed on a case-by-case basis. The *Facility Security Plan* should contain the scenario(s) evaluated, the results of the evaluation, and the reasons mitigation measures were or were not chosen.

**“Document”** means that the scenario may not need a mitigation measure and therefore needs only to be documented. However, measures having little cost may still merit consideration. The security plan should contain the scenario evaluated and the results of the evaluation. This will be beneficial in further revisions of the security plan, in order to know if the underlying assumptions have changed since the last security assessment.

**Table 4: Vulnerability & Consequence Matrix**

		Total Vulnerability Score (Table 3)		
		2	3-4	5-6
Consequence Level (Table 2)	3	Consider	Mitigate	Mitigate
	2	Document	Consider	Mitigate
	1	Document	Document	Consider

**STEP 5: IMPLEMENTATION METHODS**

To determine which scenarios require mitigation methods, the *Facility Security Officer* or company official may find it beneficial to use the Table 5 provided below. The facility or company can record the scenarios considered, the consequence level (Table 2), the score for each element of vulnerability (Table 3), the total vulnerability score, and the mitigation category (Table 4). The desire is to reduce the overall risk associated with the identified scenario. Note that generally, it is easier to reduce vulnerabilities than to reduce consequences or threats.

**Table 5**

MITIGATION DETERMINATION WORKSHEET					
Step 1	Step 2	Step 3			Step 4
Scenario/Description	Consequence Level (Table 2)	Vulnerability Score (Table 3)			Mitigate, Consider, or Document (Table 4)
		Accessibility +	Organic =	Total Security Score	
	Once a facility is categorized, the consequence level remains the same.				

To assist the *Facility Security Officer* or company official evaluate specific mitigation strategies (protective measures), it may be beneficial to use Table 6 provided below.

**Table 6**

MITIGATION IMPLEMENTATION WORKSHEET						
1	2	3	4			5
Mitigation Strategy (Protective Measure)	Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)	Consequence Level (Table 2)	New Vulnerability Score (Table 3)			New Mitigation Results (Table 4)
			Accessibility +	Organic =	Total Security Score	
1.	1.					
	2.					
	...					
2.	...					

The following steps correspond to each column in Table 6.

1. For those scenarios that scored as **consider** or **mitigate**, the facility or company should brainstorm mitigation strategies (protective measures) and record them in the first column of Table 6.
2. Using the scenario(s) from Table 5, list all of the scenario(s) that would be affected by the selected mitigation strategy.
3. The consequence level remains the same as was determined in Table 2 for each scenario.
4. Re-evaluate the accessibility and organic security scores (Table 3) to see if the new mitigation strategy reduces the total vulnerability score for each scenario.
5. With the consequence level and new total vulnerability score, use Table 4 to determine the new mitigation categories.

A strategy may be deemed as effective if its implementation lowers the mitigation category (e.g. from **mitigate** to **consider** in Table 4). A strategy may be deemed as effective if the strategy will lower the overall vulnerability score when implemented by itself or with one or more other strategies. For example, for a facility with a consequence level of “2”, if a mitigation strategy lowers the vulnerability score from “5-6” to “3-4”, the mitigation category changes from **mitigate** to **consider** and the mitigation strategy is effective. For a facility with a consequence level of “3”, the mitigation category would remain the same (**mitigate**) for a similar reduction in vulnerability score from “5-6” to “3-4”.

It should be noted that if a mitigation strategy, when considered individually, does not reduce the vulnerability, then multiple strategies may be considered in combination. Considering mitigation strategies as a whole may reduce the vulnerability to an acceptable level.

As an example of a possible vulnerability mitigation measure, a facility or company may contract for additional security personnel to prevent unauthorized access during times of elevated threat levels. This measure would improve physical security and may reduce the total vulnerability score from a “3-4” to a “2”. However this option is specific for this scenario and also carries a certain cost.

A strategy may be deemed feasible if it can be implemented with little operational impact or funding relative to the prospective reduction in vulnerability. A strategy may be deemed partially feasible if its implementation requires significant changes or funding relative to the prospective reduction in vulnerability. A strategy may be deemed not feasible if its implementation is extremely problematic or is cost prohibitive.

Feasibility of a mitigation strategy may vary based on the *MARSEC level*. Therefore, some strategies may not be warranted at *MARSEC Level 1*, but may be at *MARSEC Levels 2 or 3*. For example, using divers to inspect the underwater pier structures and vessel may not be necessary at *MARSEC Level 1*, but may be appropriate if there is a specific threat and/or an increase in *MARSEC level*. Mitigation strategies should ensure that the overall level of risk to the facility remains constant relative to the increase in threat.

Tables 7 and 8 provide an abbreviated example of how Tables 5 and 6 would be filled out for a bulk oil facility that is subject to 33 CFR 154 and receives vessels on international voyages. This example assumes that the facility has a fair deterrence capability with respect to organic security, however does not have a fenced perimeter to restrict access to the facility.

**Table 7**

MITIGATION DETERMINATION WORKSHEET					
Step 1	Step 2	Step 3			Step 4
Scenario/Description	Consequence Level (Table 2)	Vulnerability Score (Table 3)			Mitigate, Consider, or Document (Table 4)
		Accessibility + Organic = Total Security Score			
1. Gain unauthorized entry into the facility.	2	3	2	5	Mitigate
2. Externally attack the facility with a firearm.		3	2	5	Mitigate
3. Use the facility as a means of transferring people from a ship to a vehicle to illegally enter the U.S.		3	2	5	Mitigate
...		...	...	...	...

**Table 8**

MITIGATION IMPLEMENTATION WORKSHEET						
1	2	3	4			5
Mitigation Strategy (Protective Measure)	Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)	Consequence Level (Table 2)	New Vulnerability Score (Table 3)			New Mitigation Results (Table 4)
			Accessibility +	Organic =	Total Security Score	
1. Perimeter Fence that Restricts Access to the facility (meeting ASIS standards)	1. Intrude to the facility.	2	2	2	4	Consider
	2. Use the facility as a means of transferring people from a ship to a vehicle to illegally enter the U.S.		2	2	4	Consider
	...		...	...	...	...
2...	...	...	...	...	...	...