

Exhibit 9



*cc: [unclear]
[unclear]
[unclear]*

November 6, 2001

Mr. Tom Kinton
Acting Executive Director
Massachusetts Port Authority
One Harborside Drive, 200S
East Boston, 02128
(617)568-1600; 568-1603

Subject: Report - First Draft; November 6, 2001
"Physical Security Assessment: Boston Logan International Airport"

Reference: MPA #G-2711; Security Consulting Services

Dear Mr. Kinton:

Enclosed for your review is Subject Report - First Draft; November 6, 2001, "Physical Security Assessment: Boston Logan International Airport", per above Reference.

Counter Technology, Inc. (CTI), d/b/a CTI Consulting, stands ready to make whatever changes the Massachusetts Port Authority (Massport) requires regarding the Enclosed for development of the Report - Second Draft.

CTI appreciates this opportunity to support Massport.

Regards,

Michael R. Beirsto
Project Manager

Enclosure

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

Headquarters

4733 Bethesda Ave. Suite 200 Bethesda, MD 20814 Tel: (301) 907-0127 Fax: (301) 907-8997

Regional Offices

Chicago Los Angeles Austin Atlanta

MP100639

8709

Report

First Draft
November 6, 2001

"Physical Security Assessment: Boston Logan International Airport"

for



by

Counter Technology, Inc.
4733 Bethesda Ave. Suite 200
Bethesda, Maryland 20814
Phone (301) 907-0127
Fax (301) 907-6997

per

Massachusetts Port Authority Agreement (MPA) #G-2711
"Security Consulting Services"

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

MP100640

8709.001

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

TABLE OF CONTENTS

I. FORWARD	ii
II. PREFACE	iii
III. EXECUTIVE SUMMARY	1
A. Introduction	1
B. General Findings.....	1
C. General Conclusions.....	2
D. Specific Findings.....	4
E. Recommendations	5
IV. INTRODUCTION	9
A. Forward	9
B. General.....	9
C. Background.....	9
D. Purpose	11
E. Methodology	11
V. BOSTON LOGAN INTERNATIONAL AIRPORT FINDINGS, OBSERVATIONS AND RECOMMENDATIONS	14
A. General.....	14
B. Key Management Practices.....	18
C. General Description	19
D. General Safety and Security Concerns	19
E. Access Control and Alarm Monitoring System (ACAMS).....	21
F. Closed Circuit Television Systems (CCTV).....	24
G. Photo ID Badging System (Access Media/ID).....	28
H. Vehicle Identification and Control.....	33
I. Security Lock and Key Management and Control.....	34
J. Security Communications	35
K. Existing Security Rooms	38
L. Perimeter Barriers/Exterior Security/Accessways.....	38
M. Protective Lighting	43
N. Law Enforcement Officers (LEO)	43
O. Logan Guard Services	45
P. Airport Security Program (Plan) Manual [ASP]	46
Q. Airport Emergency Plan (AEP).....	47
R. Shipping and Receiving	48
S. Construction/Renovation	48
T. Parking	49
U. Visitor Control for FAA/Massport Tower	50
V. Security of Staff.....	51
W. Workplace Violence, Safety and Security.....	52
X. Utilities/Emergency Power	53
Y. Internal Security	54
Z. Fire Safety	55
AA. Safety and Security Planning	56
BB. Intelligence Sharing	57
CC. Training.....	57
VI. Conclusion	59

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

I. FORWARD

It is not the strongest of the species that survives, nor the most intelligent; it is the one that is the most adaptable to change. - Darwin

MP100642

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

#

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

II. PREFACE

Counter Technology, Inc. (CTI), Bethesda, Maryland, presents this First Draft Report: "Physical Security Assessment - Boston Logan International Airport" to the Massachusetts Port Authority (Massport). CTI wishes to thank each Massport staff person who provided information and assistance during this review for their candor, enthusiasm and keen interest in this Massport project.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100643

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

III. EXECUTIVE SUMMARY

A. Introduction

Work on the assessment of BOS Airport by CTI actually began in May, 2001, after CTI staff completed a survey of designated Massport administrative facilities and the First Draft Report of that assessment was submitted. On the afternoon of September 11, however, CTI was asked to postpone the airport study and assist Massport with their Disaster Recovery effort. Approximately five weeks later, on October 16, CTI resumed its assessment of BOS. Changes in the threat to U.S. aviation and recently implemented major security measures, obviously, affected areas of focus, findings, and resultant recommendations and development of this First Draft Report.

A factor used by the local news media to criticize BOS Airport's security program is that two of the four planes involved in the September 11 attacks departed from BOS. CTI staff firmly believes that this criticism is not justified. Obvious reasons for the selection of BOS by terrorists were relatively basic. First, BOS had planes flying transcontinental routes, carrying large loads of fuel. Second, BOS is located close to New York City.

Moreover, in assessing the vulnerabilities of BOS's security program, it is important to note that no security breaches at BOS allowed the hijacking of the planes to occur. The box cutters used by the terrorists were, at the time, lawful under Federal law. The terrorists possessed legitimate airline tickets; they successfully passed through the passenger security screening checkpoints, and underwent screening.

According to information to date, no BOS ID media was used, nor was unauthorized access onto BOS's secured area made. Aviation industry practice was based on acquiescence to hijacker demands and there were no security measures to prevent access to aircraft cockpits. Further, the potential for terrorists to take their own life makes all threats unacceptable. Therefore, a cognizant awareness of fear must now be considered a desired acceptable behavior.

Bearing these factors in mind, CTI's primary focus was directed at one key question as they carried out the vulnerability assessment effort in the aftermath of the events of September 11; "what is the vulnerability of BOS Airport based on the new threat and the new enhanced security measures that have been implemented?" Based on the security posture of BOS, the vulnerability assessment included the new threat and enhanced security measures recently implemented and are under serious consideration by the Federal government.

B. General Findings

The most obvious, yet significant, finding in this assessment is that the state of security at BOS, as is the case with every other airport in the country, has changed dramatically as the threat to US civil aviation has changed. Although Massport was moving forward in enhancing the security posture of BOS prior to the September 11 events, that progress was based on the previous perceived threat; the introduction of an explosive or incendiary device onto a passenger aircraft. The new security paradigm having become known on September 11 has caused CTI's staff to refocus a major part of their assessment effort.

To address the new threat, BOS and other American airports have had to consider new security concepts and measures while re-examining old attitudes such as limiting effective security due to limitations on security expenditures. These changes in attitudes and behavior

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

throughout the airport community include airports and airlines, but also pilots' associations, cargo companies, charter carriers, vendors and concessionaires, airport construction companies, and the traveling public.

CTI believes that the current changes to BOS' and other airports' security programs will most likely cause terrorist to abandon similar tactics in the future.

Just as the September 11 attacks exploited weakness in our aviation security system, future terrorists will look for different methodologies based on perceived vulnerabilities. These, for example, could include asymmetric threats, to include anthrax or other chemical/biological attacks, attacks on aircraft that are landing or taking off using shoulder fired surface to air missiles, attacks on the airport by sea, or the possibility of an insider threat. Just as the terrorists in the September 11 attacks developed unanticipated means of attack, so will airports have to be creative in anticipating future attacks. This, and other studies, must focus on these potential threats in addition to the more traditional threats and other security and law enforcement concerns.

BOS is not a federal facility, however, the threats facing our nation today are no longer restricted to only US interests overseas or federal agencies and the facilities that house offices of those agencies. As was discovered on September 11, 2001, the aviation industry has clearly become a target for terrorist activities. Airport security was brought to the forefront with the realization that two of the aircraft used in the terrorist attacks departed from BOS. Consequently, it was those incidents that proved that BOS is indisputably susceptible to an asymmetric threat for the primary reasons of, but not limited to, its function, purpose, location and occupants.

C. General Conclusions

A major challenge facing Massport and BOS will be the understanding of why no action has apparently occurred on the many previous safety and security recommendations submitted from multiple sources, including its own Department of Public Safety, and what can be done to ensure constructive change move forward. The basic premise is that Massport should build its Public Safety operating processes around its assigned Directors, Deputy Directors, staff, and outside resources, empowering the Department of Public Safety to develop plans, to create and operate missions, providing them resources to succeed, and holding them accountable for the success and failure of these missions. For these individuals to succeed, they must have complete control of all resources required to realize and operate the mission.

Although extremely limited in such critical resources, as manpower (in number and competency), and formal training (beyond the two programs only recently developed), the Massport Public Safety Department has worked exceedingly well at keeping its security program efficient and compliant with all applicable laws, rules and regulations despite the hurdles presented to them and delineated in this First Draft Report. The positive results of their efforts have been skewed and outmatched by security and access control programs that have been expanding or are non-existent, and are being modified or created in patchwork fashion in an effort to meet the ever changing threats, concerns, and needs. This has been compounded by the events of September 11, 2001.

However, because of those events, and numerous continued security related matters, the Department of Public Safety has received much more response and cooperation from Massport senior staff not previously experienced.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100645

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Nevertheless, the Department of Public Safety's efforts are continuously mitigated by rogue attempts to address and solve safety and security matters by non-Public Safety Department personnel. It is this type of outside intervention by non-Public Safety personnel that has created a split in authority and division of responsibility that has effectively guaranteed inefficiency, encouraged rivalries and disrupted communication.

In light of the aggressive timeline of this study and First Draft Report, and the complexity of the issues examined, this First Draft Report, while comprehensive, is not an exhaustive examination of all issues facing Massport today and in the future. Hence, CTI's recommendations focus on actions that must be taken as a matter of urgency for the very survival and success of Massport and BOS. CTI's principal conclusion is that BOS must address several systemic elements just to begin to meet only minimum standards with regard to today's threats and risks. The principal recommendation is that Public Safety authority, responsibility, manpower and objectives must be clearly enhanced, delineated and expressed without ambiguity to all Massport entities in an effort to begin to bring BOS up to a level at minimum security standards as quickly as possible.

Because of BOS' security requirements, and the feasibility of enhancing existing conditions, CTI recommends that these security issues first be addressed with no less than Public Safety Department personnel. The resulting evaluations should then be brought to the attention of the Executive Director for forwarding to the Massport Executive Board - a clear and controlled line of creativity, development and implementation.

Indeed, implementation of many of the recommendations assumes and in most cases requires the availability of sufficient additional manpower, available time/schedule and funding. They also presume there will be no intervening Massport or City of Boston mandates, either on a local or state level, which would tend to establish competing priorities not in keeping with the Public Safety Department's immediate ability to respond.

CTI cannot yet offer an estimate of the resources required for each suggested recommendation or action, partly because it would depend not only on fully establishing the true existing conditions and anomalies at BOS beyond those identified in this First Draft Report, but also to the extent to which recommendations are implemented and accomplished. Indeed, retrofitting facilities and programs due to current and/or new safety and security demands that were earlier anticipated but ignored, could have been anticipated, or were known but were not effectively communicated and/or dealt with accordingly can be extremely costly. To this end, available Federal funds must be aggressively sought out.

Massport should be commended for seeking outside help in assessing and supporting its security systems as a first step in upgrading its security program at BOS. Such work requires the accomplishment of two things. First, as this project accomplished, the periodic step back and conducting of comprehensive assessments of one's security methods, systems and procedures to determine where such a program is, where it should be in view of current needs, developmental plans, and the measures and arrangements that will get it there.

Second, with the new impetus on security in the continental US, in direct response to the events of September 11, more commonly referred to as homeland security, and the newest threats, terrorism and others more commonly referred to as the asymmetric threat, security must become a full and continuous participant in the expansion and renovation of any business, especially one with the size and responsibilities of Massport.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100646

Page 9 of 50

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

D. Specific Findings

Following are the key findings contained in this First Draft Report:

- BOS is located in a target rich environment.
- Massport's philosophy regarding Public Safety has resulted in the creation of a split in authority and division of responsibility that has effectively and comprehensively guaranteed inefficiency, encouraged rivalries, and disrupted communication.
 - In fairness to Massport Senior officials, they have signaled their intentions for a wholesale overhaul of the fragmented Massport Aviation system, to include BOS security functions and responsibilities. The method and plan to accomplish such, however, is unknown to CTI and the Massport Public Safety Department.
- Massport support to the Department of Public Safety and governance activities, with specific regard to BOS, is replicated in numerous departments, with little if any relationship to one another.
- There is considerable duplication of technical and operational public safety activities across BOS.
- The overall risk identified at BOS is Critical.
- Before September 11, BOS severely lacked the majority of elements required to meet recommended minimum safety and security standards established by the FAA, the Department of Transportation, the U.S. Secret Service, the Federal Bureau of Investigation and the U.S. Department of Defense.
- There is no security CCTV surveillance system.
- The access control and alarm intrusion detection system is extremely slow and is not being used to its fullest capabilities.
- Poor perimeter access control measures have allowed several detected breaches that could have resulted in very serious incidents. One can only speculate as to the number of undetected breaches of security since BOS lacks both a perimeter access control system and a CCTV system.
- [REDACTED] accessible to attack from public areas.
- Before September 11, there was little to no LEO presence along the perimeter and the AOA.
- Unauthorized access to the property can be easily obtained via watercraft from the Boston Channel.
- The perimeter has several blind spots (areas that cannot be seen from the tower) that place key equipment at risk.
- International freight travels within close proximity of the property via the Boston Harbor Channel.
- Private and public marinas are located across from the perimeter road that make the property easily accessible.
- Despite language in the ASP, personnel (especially contractors) continue to park personal vehicles on airport property.
- Aircraft Operators are unwilling to effectively cooperate with BOS in their endeavor to increase the safety and security of BOS on behalf of the traveling public. For example:
 - The carriers are unwilling to incorporate 100% checked baggage screening and personal passenger bag matching
 - The carriers routinely fail to adhere to the provisions of recently issued FAA Security Directives, i.e., verification of passenger ID at the boarding gate and continuous passenger inspection at the boarding gate.
- [REDACTED]

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

- Before September 11, trees and foliage found along the perimeter fence hindered monitoring of the perimeter and facilitated undetected and easy access to the airside
- Even after September 11, it is clear that security is not a major concern among tenants and contractors as several large (fence level) and other smaller mobile ladders were found parked directly abutting the fence. Air carriers continuously fail to adhere to the provisions of the Security Directive.
- Before September 11, piggybacking appeared to be a common occurrence and challenging rarely occurred.
- Before September 11, several sections of the perimeter fence were in need of repair.
- Before September 11, several vehicles could be found parked in clearly marked fire lanes.
- Fuel trucks were routinely found unattended with the keys left in the ignition.
- There is blatant disregard for FAR guidelines involving the proper wear of airport media and proper escorting procedures.
- Gate guards assigned to control access to perimeter construction projects do not properly enforce BOS rules and regulations regarding proper SIDA access or proper escorting of personnel.
- Emergency doors, rooftop hatches, crawl spaces and utility tunnels are not integrated in the access control system.
- The time it takes to process an individual for an ID badge by far exceeds most other security Category X Airports.
- Massport Public Safety should strongly consider a consolidated alarm/CCTV monitoring and dispatch center.

E. Recommendations

- In direct response to the current threats facing the airport and the aggressive security countermeasures recently implemented and under development and review, Massport should strongly consider developing a strategic plan for consolidating all safety and security related functions under the direct authority of the Department of Public Safety.
- Massport should re-define the Department of Public Safety position of responsibility and authority
- Massport should consider an in-depth assessment of the Department of Public Safety including staffing considerations and training and equipment needs analysis.
- Massport must establish and implement a continuous risk management program as it relates to security and addressing the terrorist threats.
- [REDACTED]
- Massport should consider the High Efficiency Particulate Air (HEPA) filters to facilitate the removal of airborne pathogens and other contaminants at fresh air intakes.
- Massport should research early warning devices that alarm after detecting the presence of nerve gas or other bioweapons.
- All glass should be treated with shatterproof material, such as Mylar, to minimize the danger of injuries and explosions due to flying glass.
- Massport should consider aesthetically pleasing, yet effective, bollards/planters to keep vehicles at a safe standoff distance to designated facilities.
- Establish internal and/or external annual security assessments.
- In direct response to the current threats facing the airport and the aggressive security countermeasures recently implemented and under review, Massport should strongly consider developing a strategic plan for consolidating all safety and security functions under the direct authority of Public Safety.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100648

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

- Massport should re-define the Department of Public Safety position of responsibility and authority
- Massport should consider an in-depth assessment of the Department of Public Safety including staffing considerations, training and equipment needs analysis.
- Massport should undertake aggressive steps to reduce the water boundary vulnerability through such measures as extension of the owner controlled area.
- Massport should develop and implement a passive intrusion detection and surveillance system at the water boundary perimeter.
- Massport should aggressively research the immediate prohibition of all hunting activity where firearms are used at or near BOS.
- Massport should establish a continuous and comprehensive waterway patrol program.
- Massport should consider the development and establishment of a revised portal identification system to entail consistent portal numbering scheme that would allow for expansion and other related changes, and address upkeep and revisions.
- Massport should develop procedures for the frequent review of existing conditions in comparison to current ACAMS data.
- Massport should ensure that all decisions (upgrades, new equipment, etc.) relating to the ACAMS must be coordinated with Public Safety personnel.
- All secured area/AOA doors should be installed with access control and alarm monitoring devices.
- All secured area/AOA doors should be monitored with CCTV monitoring devices.
- Massport should complete and maintain an ACAMS spare parts inventory.
- Massport should research and install single access control devices that include both the reader and the PINpad.
- BOS should consider greater use of ACAMS system capabilities closer to 100%, including automatic graphics call up with a corresponding alarm.
- Massport should ensure that alarms are not cleared until after an explanation has been entered into the system.
- Massport should establish regular printing of alarm reports to facilitate the tracking and analysis of trends and anomalies.
- Massport should consider an effective multi-year preventative maintenance contract with either Johnson Controls or another reputable ACAMS integrator.
- Massport should ensure that the [REDACTED] CCTV system is integrated with the ACAMS system.
- Massport should develop and implement a program for continuous inspection of FAR Part 107.14 and 107.13 security access portals [REDACTED]
- Massport should strongly consider simplifying FBI fingerprint recordkeeping procedures to only include the Results Sheets -- accomplished automatically and electronically, these sheets contain all necessary information needed to show proof of fingerprinting for an auditor.
- Massport should develop and maintain a comprehensive fingerprinting financial tracking system.
- Massport should extend the FBI fingerprint based criminal history records check hours of operation to five days a week (Monday through Friday), 8:30 AM to 4:30 PM each day.
- Massport must make every effort to ensure that individuals who are not applying for unescorted SIDA access are not being subjected to an FBI fingerprint based criminal history records check at this time.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

Page 6 of 59

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

MP100648A

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

- [Redacted]
- Massport should perform a comprehensive cost benefit needs analysis for a perimeter control intrusion detection system.
- Massport should establish and enforce a continuous and effective perimeter patrol program.
- Massport should perform a comprehensive assessment for the identification and installation of permanent security lighting structures along the perimeter fence and other vital areas.
- Massport should develop and establish recurrent civil aviation security and terrorism training and awareness for Massport LEO members.
- Massport should immediately and respectfully request an indefinite extension of 14 CFR FAR Part 107 provisions that become effective November 14, 2001; specifically, those concerning the Content of the Airport Security Program, as found in 14 CFR FAR Part 107.103, et al.
- Massport should begin to prepare materials and information for the updating of the ASP, to include the possibility of completely rewriting the document.
- Massport should begin to prepare materials and information for the updating of the AEP, to include the possibility of completely rewriting the document, in response to the official published date of the rewrite of 14 CFR FAR Part 139.
- Massport should perform a comprehensive assessment of all shipping and receiving procedures to ensure they are tightly controlled.
- [Redacted]
- Develop and establish a more comprehensive workplace violence program to include better documentation, clearer notification procedures, clearer after action activities, and a crisis management program that includes notification and communication procedures, incident response procedures and improved recurrent staff training.
- Enhance Massport new hire orientation sessions with workplace violence zero tolerance and personal security awareness.
- [Redacted]
- Develop and establish a comprehensive asset protection program to include property removal procedures, i.e., property pass functions, recurrent property inventory and Massport property identification tagging.
- Develop and implement a comprehensive information resources protection program to include document marking and destruction procedures, a "clean desk" policy, and the securing of electronic media such as personal computer terminals when such rooms are not occupied.
- Ensure that at least two State Police representatives apply for and receive DOD Secret clearances.
- Massport should develop recurrent SIDA Awareness training for all BOS and tenant personnel.
- Massport should develop and perform recurrent/annual airport-specific LEO training to include an intensive new-hire training program.
- [Redacted]

*D.P. for
FR/10/01*
Dove -
4

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

IV. INTRODUCTION

A. Forward

Since the September 11 events, BOS has implemented a vast number of significant and unprecedented changes in its security program. Many of these changes have been implemented as a result of numerous FAA Emergency Amendments, but include measures instituted by Massport's own initiative to go above and beyond federal requirements and recommendations.

B. General

Massport and its Department of Public Safety have come together at a significant crossroads and have begun to put in place numerous initiatives to meet the security needs and demands of the 21st century. In their continuing effort to ensure and maintain the safety and security of Massport personnel, facilities, and operations, the Massport Department of Public Safety tasked CTI to perform a comprehensive physical security assessment of Boston Logan International Airport for the development of potential advancements and solutions to current and future safety and security needs.

On May 8, 2001, senior CTI staff met with Joseph M. Lawless, Director of Public Safety, and Delcine Gibbs, Deputy Director of Public Safety, to provide the initial client in-briefing. Subsequent to that meeting, CTI invited additional senior staff to the Airport, where, over the course of the next several weeks, various and extensive field observations, studies, interviews, evaluations, and document reviews were performed. CTI attached this assessment from diverse perspectives and approaches; nationally, internationally, and locally.

Because of the events of September 11, 2001, Massport was forced to forego normal operations and incorporate emergency measures, both Massport initiated and federally mandated. Senior CTI staff responded to Massport, at the request of the Director of Public Safety, to assist Massport in their recovery efforts, which included complying with FAA Emergency Amendments (EA).

As a result of these efforts, the assessment of BOS was temporarily delayed. On October 16, 2001, CTI was informed by Massport that the physical security assessment of BOS was to continue with a First Draft due November 5, 2001. As directed, CTI recommended the assessment that was temporarily sidetracked because of the Disaster Recovery efforts. This First Draft Report is the result of the merging of the initial information gathered prior to September 11, and the additional information obtained post to September 11.

Further, the evolution of technology is dictating change within the United States and more specifically, Massport, with the impetus for self-examination and introspection. Most importantly, Massport customers, including BOS, along with other external entities, have been pointing to much inefficiency in the way they manage their assets, their leadership, their communication and cooperation with one another, and their approach to technology.

C. Background

The threat of terrorist attacks against U.S. citizens and U.S. interests around the world has become the Nation's most pressing national security issue. Currently, the United States is retaliating to the horrific terrorist attacks that took place on the morning of September 11, 2001. The campaign, if carried to the lengths necessary to eradicate the terrorist organization(s) responsible, will be fierce, protracted, and bloody. This is particularly true if

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100651

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

the U.S. government follows through on its determination to go after all nations that harbor, support, and fund terrorist activities and individuals.

Consequently, American and coalition military strikes are likely to lead to further terrorist strikes against American and allied citizens and interests, both in the U.S. and abroad. This aggression will likely take a variety of forms as stated by the National Security Council that may include infrastructure assets, particularly transmission lines, and other modes of transportation.

Even more likely, are cyber attacks by sympathizers of the terrorists, hackers with general anti-U.S. or anti-coalition sentiments, and thrill seekers lacking any particular political motivation. During the past five years, the world has witnessed a clear escalation in the number of politically motivated cyber attacks, often embroiling hackers from around the world in regional disputes. Prevention of cyber attacks in the near future will be no different than in the past.

Best practices for maintaining systems should be followed as a tenet of any organization's standard operating procedures:

- Operating systems and software should be updated regularly
- Strong password policies should be enforced
- Systems should be 'locked down'
- All unnecessary services should be disabled
- Anti-virus software should be installed and kept up to date
- High fidelity intrusion detection systems (IDS) and firewalls should be employed

Security measures, which were previously considered excessive, should now be considered a minimum effort. System administrators must recognize that this new war on terrorism will require increased vigilance from everyone, particularly those who are entrusted with maintaining critical information assets. These basic steps will go a long way toward preventing successful attacks.

In addition to the very real possibility of cyber attacks, the nation is currently facing an ongoing anthrax situation. Anthrax spores have been discovered at several different locations, mostly mail facilities. With the government currently having no reliable leads, the next anthrax attack could occur anywhere, including Massport, specifically BOS. There are three different types of infection: Cutaneous, Gastrointestinal, and Inhalation. Further, terrorists may attempt to use anthrax in an attack via the water supply, or aerosolize it and use it in an attack via the ventilation system. With all these facts in mind, it is obvious that all Massport facilities, not just BOS, should be properly secured and monitored.

Nevertheless, combating terrorist attacks is extremely difficult. The FBI is the lead law enforcement agency dealing with the threat of weapons of mass destruction, under which anthrax is included. The FBI's National Domestic Preparedness Office is designated as the office to provide guidance to heads of fire departments relative to response for threats of anthrax and other agents of weapons of mass destruction. It is with the FBI's guidance, assistance, and the cumulative effort of Massport and other local, state and federal agencies that will help ensure BOS emergency personnel are prepared to respond to a bio-terrorism attack.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100652

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

In addition to terrorist activities, Massport faces other challenges. The Bureau of Labor Statistics identifies homicide as the number two cause of death in the workplace; number one for women. Just as alarming, recent studies show that in the last year alone, one out of every four employees was attacked, threatened, or harassed at work. Further, signs point to exceptional vulnerability on the part of professionals in their offices and out-reach programs.

With all these issues facing Massport, it is imperative that Massport officials stay a step ahead. To contend with these issues, Massport must commit to the development of policies and procedures, establish a threat response system, conduct violence risk analysis, and train managers, supervisors, and employees in violence awareness, emergency preparedness and prevention issues.

D. Purpose

The Massachusetts Port Authority (Massport) contracted Counter Technology, Inc. (CTI), Bethesda, Maryland, to perform comprehensive physical security assessments of:

- 1) Boston Logan International (BOS) Airport
- 2) Hanscom Air Field
- 3) Port of Boston
- 4) Tobin Memorial Bridge

The primary purpose of this assessment is to identify the need for safety and security countermeasures, identify the countermeasures, and develop recommendations to employ such countermeasures to further strengthen Massport's safety and security program for its employees and facilities specific to BOS.

The goals met in achieving this objective include, but are not limited to, the following:

- 1) Identify and describe the specific mission, authorities, and responsibilities of Massport, local, state and/or federal agencies.
- 2) Identify the roles played in security by each of the aforementioned, including the private sector, where applicable, for BOS.
- 3) Analyze the nature and extent of threat, vulnerability, risk, and crime with a nexus towards the operating context for BOS.
- 4) Assess the readiness of Massport to respond to terrorist and/or criminal acts (by internal and external forces) and/or threats regarding BOS.
- 5) Evaluate the state of safety and security at BOS.
- 6) Assess the nature and effectiveness of ongoing coordination between Massport, local, federal, and/or other state government and law enforcement agencies for BOS.
- 7) Solicit input from Massport and other interests regarding the safety and security posture as perceived by them regarding BOS.
- 8) Identify specific recommendations on system, policy and program issues.

E. Methodology

This First Draft Report by CTI addresses Boston Logan International (BOS) Airport. For this First Draft Report, CTI's methodology for assessment employed the same methods and standards as those developed by the federal government for the assessment of military facilities and airports.

MP100653

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

- As to the safety and security of BOS, Massport requested CTI accomplish the following:
- 1) Identify and describe the specific mission, authorities, and responsibilities of Massport, local, state and federal agencies and identify the roles played in security by each, including the private sector, where applicable.
 - 2) Analyze the nature and extent of threat, vulnerability, risk, and crime with a nexus towards the business context.
 - 3) Assess the readiness of Massport to respond to retaliatory, terrorist and/or criminal acts and/or threats.
 - 4) Evaluate the state of security.
 - 5) Evaluate the state of personal safety in the context of workplace violence.
 - 6) Assess the nature and effectiveness of ongoing coordination between Massport, local, federal, and other state, government, and law enforcement agencies.
 - 7) Solicit input from various Massport staff and other interests regarding the safety and security operations and posture as perceived by them.

CTI conducted this comprehensive Physical Security Assessment of Boston Logan International (BOS) Airport, with senior staff extensively familiar with, trained and well experienced on the subjects of, but not limited to:

- Continuous Risk Management
- Safety and Security Vulnerability and Threat Assessment
- Counterterrorism and Force Protection
- Workplace Violence and Crisis Management
- Security Systems Design and Integration
- NARCO Terrorism/Executive Witness Protection

Consequently, CTI accomplished the assessment of BOS utilizing and employing, as a base line, the same type methods, standards and techniques as those developed, taught, recommended and currently employed by, in no particular order:

- The Federal Bureau of Investigation
- The Drug Enforcement Administration
- The US Department of Justice
- The Central Intelligence Agency
- The US Marshals Service
- The US Department of Transportation
- The US Secret Service
- The US Department of State
- The Federal Aviation Administration
- Military Special Ops and Reactionary Units
- National Institute for Occupational Safety and Health
- Occupational Safety and Health Administration

CTI staff surveyed all areas of each BOS facility, including their location, design, operations, security programs, security systems, and certain known areas of concern as previously identified by the Director and Deputy Director of Public Safety. CTI performed this assessment during and outside normal business hours over the course of several weeks.

MP100654

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

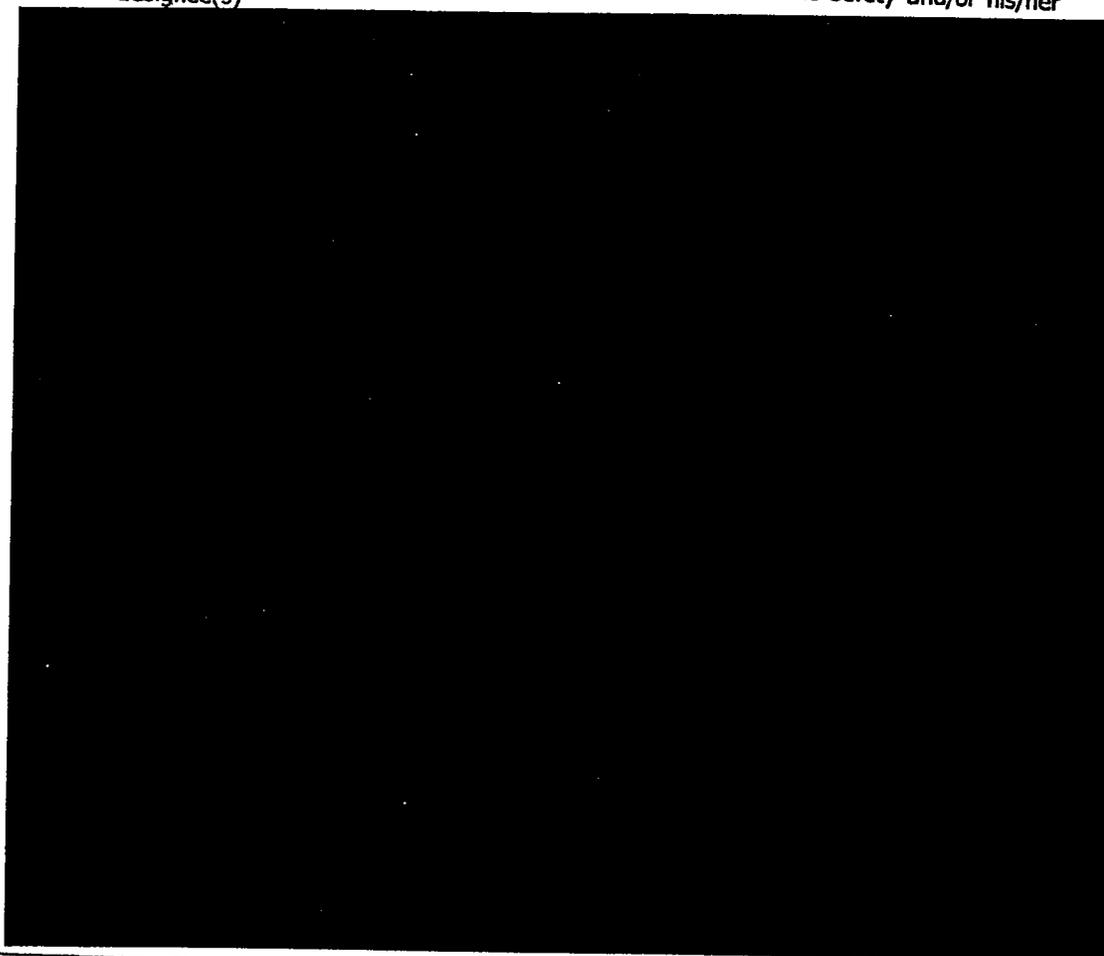
CTI staff met with and/or interviewed numerous individuals, including, but not limited to, the following key Massport personnel:

- The Director of Public Safety
- The Deputy Director of Public Safety
- The Deputy Director, Facilities
- The Deputy Director, Operations
- The Manager of Systems Development
- The Director of Information Systems and Telecommunications
- Various Massport Security Services Unit staff

CTI staff collected, studied and reviewed documentation that included the Airport Security Program (ASP), the Airport Emergency Plan (AEP), the Massport Workplace Violence Program, and other safety and security policies, directives, procedures, drawings, and maps.

Moreover, CTI employed a work-plan, including, but not limited to the following:

- Perform an initial in briefing with the Massport Director of Public Safety and/or his/her designee(s)



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100655

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

V. BOSTON LOGAN INTERNATIONAL AIRPORT FINDINGS, OBSERVATIONS AND RECOMMENDATIONS

A. General

During the course of the assessment of BOS, CTI met or spoke with and interviewed the following key Massport and non-Massport personnel:

Massport Personnel

Director of Public Safety	Joseph M. Lawless
Deputy Director of Public Safety	Delcine Gibbs
Deputy Director of Public Safety	Chuck Monahan
Special Assistant to the Director of Public Safety	Bill Christiansen
Assistant Chief, Fire/Rescue	Jim McGinty
Major, Massachusetts State Police	John Kelly
Deputy Director, Aviation Operations	John Duval
Deputy Director, Airport Facilities	Gary Tobin

Non-Massport Personnel

FAA FSM	Steve Luongo
FAA CASFO Special Agent	Sherry Moran

- BOS resources (assets), identified through this comprehensive security assessment, include the following:
 - Numerous mission critical/sensitive BOS operations
 - BOS Director of Aviation
 - Massachusetts State Police Troop F
 - Aircraft supporting equipment
 - The public terminals
 - Numerous mission critical/sensitive security US federal agency operations
 - Federal Aviation Administration
 - US Customs Service
 - Immigration and Naturalization Service
 - US Department of Agriculture
- Vulnerabilities at BOS, identified through this comprehensive security assessment include, but are not limited to, the following areas/operations:
 - Insufficient security/access control systems, methods, and procedures. Including:



- Ineffective workplace violence and personal security awareness programs
- Substandard Information resources management:
 - Required and best type document/asset destruction procedures/methods not completely known, hence not properly executed
- The threats at BOS; identified through this comprehensive security assessment, include, but are not limited to, in no particular order, the following entities:
 - Terrorist organizations, sects, cells, or sympathizers
 - Organized and non-organized criminal activities

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

- o Disgruntled employee(s)
- o Disgruntled contractor(s) or contract employee(s)
- o Domestic violence
- o Community activists upset with Massport Runway Expansion and/or Regionalization Plans
- o Other physical and environmental type threats

The Threat

The events of September 11 were the unthinkable expansion of terrorists attacks. That being said, terrorist groups have looked at and are allegedly mixing new, or asymmetrical, techniques into traditional attacks as a force multiplier of sorts – the Asymmetrical Threat. This includes, for example, mixing chemical agents in with an explosive or using radioactive material in traditional explosive devices to create a "dirty device." In addition, and in light of current biological attacks within the US, if a biological agent is used, and this holds true for a radiological component as well, you cannot see what you cannot see. In other words, without the appropriate detection equipment, no one can tell if there is anything else to be concerned about until it is almost too late.

The obvious and clear as day technique, large vehicle bombs, does not preclude a more covert technique from being used in conjunction. The majority of Muslim extremist groups are seeking the creation of Khilafah, or Islamic state. As such, there are efforts currently underway to establish this in Chechnya, Pakistan, Afghanistan and other places around the world. This is nothing short of a holy struggle in the extremist's eyes and, as further evidenced by the events of September 11, 2001, they will not stop until all of the kufr, the infidels, have been beaten down and destroyed. This is not a group fighting for a few political demands.

Osama bin Laden, a 44 year old Israeli who has lived in Afghanistan since 1996 and who, since 1990, has been ever escalating his war from a small bombing in a hotel overseas in 1990 to the events of September 11, 2001, sees civilians as legitimate targets. His logic behind this is that in order to participate in jihad, you do not only take part by taking up arms. People donating money and other support are taking part in jihad just as the frontline fighters are. According to this logic, bin Laden sees American taxpayers as participants, much as the frontline fighters are.

Sheikh Omar Bakri Muhammad, another key terrorist figure, has in the past five years issued numerous fatwas, creating a religious justification for the use of nuclear and biological weapons in a "defensive jihad." Unfortunately, he and other terrorists only have to be successful once; those fighting terrorism must be successful every time. One simply cannot believe that he/she can prevent every attack of terrorism from occurring. Therefore, Massport must do all that they can to stack the odds in their favor, on a continuous and indefinite basis.

Much like we learned that drug dealers are not just a bunch of thugs standing on a street corner, Massport, on behalf of BOS, must clearly understand that Muslim extremists are not just a group of mindless fanatics running around with explosives. The image of an Afghan mujahideen fighter standing with a Kalishnikov slung over his shoulder in a barren Afghan desert, and all the stereotypes that go with it, will forever skew our understanding of the threat. Only now are we beginning to come to grips with the fact that terrorist individuals can fly planes, send secure communications, conduct complicated intelligence operations, run

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100657

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

a high-profile business, hack into computer systems, and otherwise blend into every level of our society. As such, only now do we stand a chance at maneuvering our opponent; when one does not understand the enemy, so too will that one forever underestimate the terrorists ability.

- You do not know what you do not know; if there are other operational cells, and there is more reason to believe there are than there are not, we won't necessarily know who or where they are. They could launch an action tomorrow or next year. For example, the terrorist group Al-Qaeda currently has at least 50 cells located around the world.
- Just because the four attacks of September 11, 2001, and surrounding individuals all seemed to be focused on flying planes, it does not mean the next attack will have anything to do with planes. Anything and everything is fair game, from target to method.
- When attacks occur overseas, all of our attention is focused on overseas exposure, when an attack occurs in the States all we think about is additional possible attacks within CONUS (the Continental United States). Massport has a great many exposed interests that are clearly facing a significantly high threat from Osama bin Laden associates and others.
- Terrorist groups have shown a great interest in chemical, biological, radiological, nuclear and cyber type attacks. Notwithstanding the events of September 11, 2001, and while experiments and researching of these techniques is occurring at present, Muslim extremist groups and other terrorists do continue to use traditional techniques (i.e. car bombings, assassination, suicide bombings). These techniques are what that they know how to do well, albeit on a scale never before seen.

Nevertheless, to date there have been 32 known anthrax exposures since September 11. Of those exposures, 17 victims have been confirmed to be infected with the virus: 10 have been confirmed with the inhalation form of anthrax (at the writing of this report, 6 are seriously ill and 4 have perished), and 7 have contracted the cutaneous form of anthrax.

Other chemical and biological threats that must now be contended with include botulism, pneumonic plague, and smallpox. Further, while smallpox was eradicated from the world in 1977, the US and the CDC are currently assessing smallpox vaccine stock due to the current threat of its possible exposure. There is no proven treatment for smallpox, but research to evaluate new anti-viral agents is aggressively ongoing.

Recommendation # 1

For suspicious unopened letters or packages marked with threatening messages:
Do not shake or empty the contents of any suspicious envelope or package.
Place the envelope or package in a plastic bag or some other type of container to prevent leakage of contents.
If you do not have any container, then COVER the envelope or package with anything (e.g., clothing, paper, trash can, etc.) and do not remove this cover.
Then LEAVE the room and CLOSE the door, or section off the area to prevent others from entering (i.e., keep others away).
WASH your hands with soap and water to prevent spreading any powder to your face.
Report the incident to Massport LEOs and notify your supervisor.
List all people who were in the room or area when this suspicious letter or package was recognized. Give this list to the responding emergency personnel.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100658

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Recommendation #2

If contamination is due to possible powder substance:
Do not try to clean up any powdery substance that may spill out of an envelope onto a surface. Instead, immediately cover the spilled contents with anything (e.g., clothing, paper, trash, etc.) and do not remove this cover. Once the item has been covered, leave the room and close the door, or section off the area to prevent others from entering – keep others away.

Once the room has been left, individuals must wash their hands with soap and water to help prevent spreading any powder to your face. Immediately report the incident to an LEO, and notify the department/office supervisor.

Remove heavily contaminated clothing as soon as possible and place such clothing in a plastic bag or other container that can be sealed. This clothing bag should be given to the emergency responders for proper handling and testing. Shower with soap and water as soon as possible – Do not use bleach or other disinfectant on the skin. If possible, list all people who were in the room or area, especially those who had actual contact with the suspect powder. Provide this to the responding LEO and/or responding public health authorities so that proper instructions and procedures can be given and followed for medical follow-up and further investigation, respectively.

Some characteristics of suspicious packages and letters include the following:

- Excessive postage
- Handwritten or poorly typed addresses
- Incorrect titles
- Title, but no name
- Misspellings of common words
- Oily stains, discolorations or odor
- No return address
- Excessive weight
- Lopsided or uneven envelope
- Protruding wires or aluminum foil
- Excessive security material such as masking tape, string, etc.
- Visual distractions
- Ticking sounds
- Marked with restrictive endorsements, such as "Personal" or "Confidential"
- Shows a city or state in the postmark that does not match the return address

Recommendation #3

If contamination is due to possible aerosolization:

Turn off all local fans and/or ventilation units in the area and leave the area immediately. Close the door or section off the area to prevent others from entering. Immediately notify an LEO and the local FBI field office, and notify the department/office supervisor.

Immediately shut down the air handling system in the building, if possible. List the names of all people who were in the room and in the area. Provide the list to both the LEOs (Includes the FBI) and the responding public health authorities so that proper instructions and procedures can be given and followed for medical follow-up and further investigation, respectively.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100659

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Recommendation #4

Massport must establish and implement a continuous risk management program as it relates to security and addressing the terrorist threats.

Recommendation #5

Recommendation #6

Massport should consider the High Efficiency Particulate Air (HEPA) filters to facilitate the removal of airborne pathogens and other contaminants at fresh air intakes.

Recommendation #7

Recommendation #8

Massport should ensure clear evacuation plans are well defined.

Recommendation #9

Recommendation #10

Massport should consider aesthetically pleasing, yet effective, bollards/planter to keep vehicles at a safe standoff distance to designated facilities.

Recommendation #11

Establish internal and/or external annual security assessments.

B. Key Management Practices

CTI evaluated current Massport Department of Public Safety management practices, internally, and how it relates to Massport management practices on a whole, to determine legacy patterns that should be changed to make the Department of Public Safety most effective. CTI determined that, unlike most other government agencies, state, federal or otherwise, Massport's culture is to do work internally yet fragmented and disjointed. This philosophy apparently has evolved over the years based on an "old school" philosophy.

Indeed, when interviewing key Massport Senior personnel, the response given to the aforementioned description of Massport's philosophy was, "... it has been that way since I've been here". The result of this philosophy is the creation of a split in authority and division of responsibility that has guaranteed inefficiency, encouraged rivalries, and disrupted communication.

Because of this philosophy, Massport can no longer expect its Department of Public Safety to lead and present management practices within the Agency that will accommodate today's new threats unless a drastic and immediate change occurs to reverse this epidemic like effect.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

FIRST DRAFT REPORT
 "Physical Security Assessment:
 Massachusetts Port Authority
 Boston Logan International Airport"

November 6, 2001

Recommendation #12

In direct response to the current threats facing the airport and the aggressive security countermeasures recently implemented and under review, Massport should strongly consider developing a strategic plan for consolidating all safety and security functions under the direct authority of Public Safety.

Recommendation #13

Massport should re-define the Department of Public Safety position of responsibility and authority

Recommendation #14

Massport should consider an in-depth assessment of the Department of Public Safety including staffing considerations and training and equipment needs analysis.

C. General Description

Boston Logan International (BOS) Airport comprises approximately 2,400 acres in the City of Boston. The property on which the Airport is located is owned and operated by the Massachusetts Port Authority (Massport).

The Airport currently has five terminals; Terminals A, B, C, D and E. The Amelia Earhart Terminal is currently used as a secure hold room for pre-screened commuter passengers. Terminal A currently has seventeen gate positions with security checkpoints at the entrances to the east and west ends of the terminal. Terminal B consists of two terminals separated by a parking garage. Each terminal is equipped at midpoint with piers running perpendicular to the terminal building. The terminal currently has thirty-eight possible gate positions with seven security checkpoints in operation.

Terminal C possesses twenty-five gate positions, three security checkpoints, and three piers; piers A, B, and C. One checkpoint serves all three piers, while piers C and D have an additional checkpoint each. Terminal D has three gate positions and one ground-level security checkpoint. Terminal E has four levels. The fourth floor houses two mechanical rooms to which there is no public access. Passenger screening is conducted at two checkpoints on the third floor and one checkpoint on the second floor. The second floor housed the United States Immigration inspection area, VIP rooms, and office space for air carriers and government agencies. The first floor houses the United States Customs Hall.

D. General Safety and Security Concerns

BOS is bordered by the Boston Channel, residential areas, major roadways and business entities. Ultimate responsibility for safety and security of BOS is supposed to reside with the Director of Public Safety, however, currently it is handled by the Airport Director, the Deputy Director, Operations, Deputy Director, Facilities, and temporarily assigned Airport Security individual and numerous other department heads, individually and/ or collectively. The Public Safety Department consists of two Deputy Directors of Public Safety, one Public Safety and Security Manager and one Massachusetts State Police Sergeant who directly assists the Director of Public Safety.

At the writing of this report, the position of Director of Public Safety was vacant. The head of the Massachusetts State Police, Col. John DiFava, was appointed temporary Head of Airport Security. Because of this, a new position was created; the Director of Public Safety for the Port.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

Page 19 of 59

Subject to Confidentiality Protective Order
 In re September 11 Litigation
 21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
 Do Not Copy or Disclose

MP100660A

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

The current concerns dealing with airport security are overwhelmingly related to the terrorist attacks on September 11, 2001. BOS has had to deal with ever changing FAA guidance and with coordinating the efforts of different law enforcement agencies assigned to the airport, including US Marshals, US Customs, US Border Patrol, and the National Guard.

It is important to remember that, even though the immediate response to the terrorist attacks is warranted, there remain other issues of security concern. Because of its proximity to the Boston Channel BOS' perimeter is easily accessible via watercraft. International freight passes along this route, [REDACTED] this area is still of concern.

Another concern is the proximity of personal watercraft to BOS property. Civilians were observed fishing close to the perimeter on several occasions; one individual even docks his houseboat in the bay, extremely close to the perimeter of the airport near the International Terminal. Another concern is the activity of local clam diggers. Several individuals were observed docking their boats and literally walking up to the perimeter boundary to engage in digging for clams, in immediate proximity to active runways, no less. Along with this concern is the arrival of duck hunting season, which has on occasion, brought with it duck hunters to BOS property, also on the side of the airport's new International Terminal and active runways. Obviously, the proximity of unauthorized and unscreened individuals to active runways should be of particular concern.

Much has been reported recently in the media regarding the aviation security programs overseas vs the US, specifically Israel. Unfortunately, however, there is no comparison. Israel unlike any other country has approximately 1000 government security personnel at their disposal to perform individual one-on-one passenger profiling for all passengers attempting to fly El Al Airlines. These interviews last, on average, approximately ninety to 150 minutes. Further, El Al Airlines has installed reinforced cockpit doors and multiple (average four) armed persons on each El Al flight, of which only twenty thousand flight operations per year occur.

The US, on the other hand, is the only country to incorporate approximately 98% of the security guideline provisions currently found in the International Civil Aviation Organization (ICAO) standards, as found in ICAO Annex 17. Additionally, the US civil aviation industry has incorporated numerous security measures beyond those found and required by FARs and/or Legislative Acts. Further, the US operates more than 40,000 flight operations per day, with passenger enplanements in the millions!

Recommendation #15

[REDACTED]

Recommendation #16

Consider utilization of a passive intrusion detection and surveillance systems

Recommendation #17

Consider greater signage distribution prohibiting intrusion into owner controlled area

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100661

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Recommendation #18

Massport should aggressively research the immediate prohibition of all hunting activity where firearms are used at or near BOS.

Recommendation #19

Consider the use of a waterway patrol unit.

E. Access Control and Alarm Monitoring System (ACAMS)

The system administrator has the overall responsibility for the performance of the ACAMS. The system administrator is currently an IS department position and is located in Terminal C, Room 1037. Massport electricians handle the day-to-day maintenance and upkeep of the system with overall responsibility of the system charged to a former Massport electrician. This individual was, until recently, performing dual roles; electrician and system maintenance technician. He has been given verbal instructions by the Deputy Director, Facilities as to his responsibilities. He is no longer to perform electrician functions and is to devote 100 percent of his time to access control system maintenance. This is understood to be a permanent position change, a title change more indicative of his responsibilities has not yet occurred.

All airport electricians are currently Massport Facilities positions. This individual is currently located in temporary space in one of the Massport Facilities buildings while he awaits permanent office space. Massport recently hired a Systems Specialist to train on the upkeep of the system and to assist the electrician as necessary; his eventual specific duties will include system maintenance. Massport currently requires that two electricians be on site at all times to ensure that there is a response to system issues. According to the Deputy Director, Facilities, the eventual goal is for all Massport electricians to be trained in the proper maintenance of both the software and hardware of the access control system.

Massport decided against renewing the access control maintenance contract with Johnson Controls Inc. (JCI) because they believe it would be more cost efficient to have proprietary staff receive training and perform the required duties rather than contracting the duties out. However, JCI is still contracted to perform certain functions on a Purchase Order (PO) basis. The PO agreement includes a not to exceed (NTE) amount of \$50,000 annually, with Massport Facilities personnel as the primary points of contact.

The ACAMS consists of several workstations, remote access panels and door hardware. The ACS workstations software is made by Surveillant (formerly MIC) Access NT and runs on Microsoft Windows NT Server Version 4.0 and uses Microsoft SQL Server Version 7.0 to store data, which is running on Compaq ProLiant redundant servers. Each server contains dual Pentium II 450 MHz processors, 512 MB of RAM and six 9.1 GB drives arranged in a RAID 0+1 array for a total of approximately 25 GB of disk storage. Each processor is attached to a heavy duty UPS capable of providing backup power to the units for up to 30 minutes. The servers communicate via Ethernet with two Digiboard 32 serial port devices, which are connected to the forward and reverse channels of the remote access panels (18) located throughout the phone and electrical closets of the airport. The access control system was installed approximately two and one-half years ago, and has a warranty period of three years.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100662

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

The ACAMS uses additional hardware at each portal such as reader's, keypads, electric strikes, magnetic locks, door contacts, audible alarms and strobe lights. These devices are not covered under service contract, but are repaired as needed by the facilities department. The facilities department has not purchased any new equipment for the system in over one and one-half years. The overall system is lacking a periodic maintenance contract and system-testing program.

JCI or a Massport electrician repairs the system remote access panels or nodes on a T&M basis. CTI performed a functional test on [redacted] (greater than [redacted] of the current system) FAR 107 doors, finding [redacted] that failed the testing. The doors failed for several different reasons, including, but not limited to, the following examples.

Two doors, while they alarmed locally, did not alarm at the communications center, two doors that did not alarm locally were found to have paper stuffed into the alarm casing, tamper alarms at nodes failed to generate an alarm at keybase and had to be replaced, and several strobe lights were found to be inoperable. In addition, several maintenance issues were discovered, which led to on the spot maintenance. The results of the functional test produced a failure rate of approximately [redacted] which underscores a far greater problem when applied to the entire system of approximately [redacted] portals.

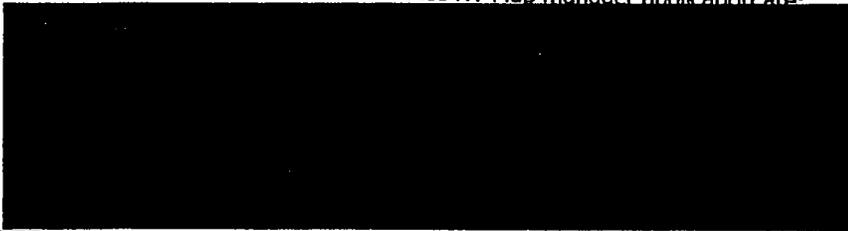
The access control system is also capable of monitoring alarms. The alarm manager displays the real-time status of interface panels in the access control system. Alarms are displayed on alarm page windows that have been defined for the operator monitoring the alarms in real time.

The major functions of the alarm manager application are:



The ACS Map Manager uses a graphical interface to represent the state and condition of Alarm points defined in the MIC-Access NT system. The MIC-Access NT Map manager uses a series of icons to represent the current states of these alarm points.

Some of the features of the MIC-Access NT Map manager application are:



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100663

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

The MIC-Access NT Loop Monitor provides real-time information about the status of the hardware of the ACS. It is a view only application, and may be accessed through the main MIC-Access NT menu system, or by logging into the Loop Monitor application from the start menu. The Event Monitor is a real time log of events occurring in the system. There are ten ACAMS remote terminals located throughout the airport.



System backup is accomplished daily and is stored on site in the same room as both the primary and the redundant server and the fiber optic connections. All are located in a dedicated room in the system administrator's office area. The room is secured via lock and key and only the head electrician, the system administrator, certain Facilities personnel and certain Massport senior staff have access.

Recommendation #20

Massport should consider the development and establishment of a revised portal identification system to entail consistent portal numbering scheme that would allow for expansion and other related changes, and address upkeep and revisions.

Recommendation #21

Massport should develop procedures for the frequent review of existing conditions in comparison to current ACAMS data.

Recommendation #22

Massport should ensure that all decisions (upgrades, new equipment, etc.) relating to the ACAMS must be coordinated with Public Safety personnel.

Recommendation #23

All secured area/AOA doors should be installed with access control and alarm monitoring devices.

Recommendation #24

All secured area/AOA doors should be monitored with CCTV monitoring devices.

Recommendation #25



Recommendation #26

Massport should complete and maintain a spare parts inventory.

Recommendation #27

Consider installing single access control devices that include both the reader and the pinpad.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100664

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Recommendation #28

Recommendation #29

Recommendation #30

Strongly recommend regular printing of alarm reports to facilitate tracking analysis of trends and anomalies.

Recommendation #31

Massport should consider an effective multi-year preventative maintenance contract with either Johnson Controls or another reputable ACAMS integrator.

Recommendation #32

Recommendation #33

Coordinate with Public Safety on a Key Card return policy for better control of the Key Cards and perform regular audits for proper record keeping.

Recommendation #34

Massport should develop and implement a program for continuous inspection of FAR Part 107.14 and 107.13 security access portals to identify and address concerns quickly, and to facilitate up to date accuracy of security portal data.

F. Closed Circuit Television Systems (CCTV)

BOS currently has no CCTV system in place. Nevertheless, senior technical security personnel from CTI accomplished an initial CCTV system assessment on Saturday, September 29, 2001 and Sunday, September 30, 2001, on behalf of Massport. In accordance with the provisions of the assessment, the following information and recommendations are a result of that assessment.

The average cost of a digital recording CCTV system for installment at screening checkpoints within BOS is estimated to cost approximately \$40,000.00 per checkpoint. This cost allows for fixed cameras aimed directly at each walkthrough magnetometer (metal detector), as well as Pan Tilt & Zoom (PTZ) cameras directed at the entire screening area. The fixed cameras would allow for identification of all individuals that pass through the walkthrough magnetometer while PTZ cameras would provide an image of all activity and present an additional resource for capturing any individuals trying to bypass screening. A second PTZ camera could be installed to face the exit lane from the sterile side and thus capture a full-face picture of anyone using that area to bypass screening.

Using a video monitor would also allow for video playback of the digital picture almost instantaneously. If necessary, a picture of the suspect (when identified) can be printed out and provided to the LEOs for their use during an immediate search throughout the terminals. The digital video player would need no more than one hour of recording time before rewriting the disk in a first-in-first-out (FIFO) style to be effective. The network controller

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100665

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

can send a second feed of the picture to the central monitoring station where it could be recorded on the main digital recorder for longer storage. This would also allow the system to be used integrated a facial recognition system.

Facial recognition software is currently available for use; however, the technology is continuously undergoing development. Facial recognition system databases work to recognize individuals that are known criminals or are being sought by various federal state and local law enforcement agencies. Such databases, however, are the difficult part within any facial recognition system. As we have learned, known leaders of most terrorist groups do not conduct most terrorist acts, but rather individuals from their groups that may not be so readily known. Furthermore, the FBI and the CIA are very reluctant to include the face of an individual whom they are tracking into a database where non law enforcement personnel would have the ability to view them.

Furthermore, biometrics cannot identify terrorists, biometrics only identifies individuals, and then only when an individual's template already resides in the biometric database. If the image for producing the biometric template is of poor quality and/or the image received for verification/identification is of poor quality, the results will not be very satisfactory. Those biometric technologies that are producing superior verification/identification results depend on one or more of the following: user participation, environment, ethnic background, the quality of the biometric hardware and software used. In short, biometrics technology still has serious deficiencies and much room to evolve. Additionally, there exists the possibility that a full scale use of biometrics within an airport environment might result in extremely long lines and an exorbitant amount of mismatches of false-negatives, or worse, false-positives.

There also exist liability issues because of obvious legal ramifications of placing an individual on any type of watch list before that individual has been convicted of a criminal act. Thus, these lists would be limited to known individuals that have been convicted of a law in the US or is being sought out for criminal activities during the course of an official investigation, and their face has been entered into a facial recognition system's database. Such a system, however, can also be used to watch for individuals terminated under adverse conditions and who pose a legitimate threat.

Systems currently available and under development on the market allegedly have the ability to allow the user to decide the level of certainty that would trigger an alarm. Unfortunately, however, when the level is set very high, then an individual tilting his/her head could be missed by the system. Consequently, when the level is set too low, then many people who look somewhat similar to the subject could trigger an alarm. In fact, if set low enough the system could conceivably be set to pick up men or women from different ethnic backgrounds and different genders. This would then be a form of profiling, which could result in additional legal issues.

Another use for the facial recognition system is the ability to take video from the screening checkpoints and add that face to the database immediately for real time database entry. This would allow the person that ran through screening to be added to the database and used on all other cameras to search for and identify the individual. This could be used to increase the probability of identifying which flight a suspect boarded or attempted to board.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100666

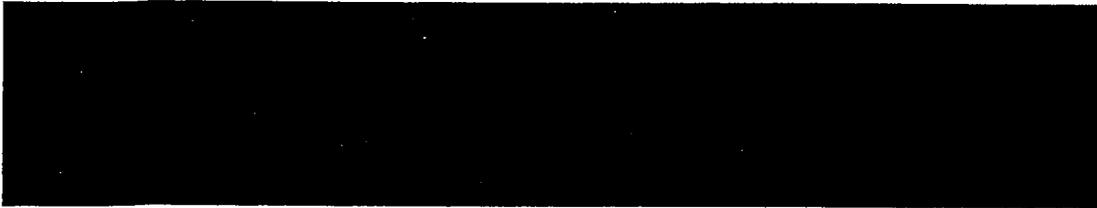
**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Furthermore, research is underway regarding the possibility to "blind set" a data base so that when a persons face triggers an alarm, that face and alarm would only go by data stream to the agency that put the photo into the data base. This way the FBI could add to their suspect list as well as the CIA and other investigative agencies without endangering National Security information.

To make any of this work, a data backbone must be available, either as part of an existing backbone or as part of a developed backbone. For the facial imaging system to work the most effective way is that by some means high quality data must reach the command center. Also, to effectively maintain a digital recording system, it is advisable to have all cameras readout to one point. If this infrastructure does not exist, and it appears that BOS engineers are uncertain that it does, then this backbone could be one of the highest costs of a developed CCTV system.



Nevertheless, with regard to a complete CCTV system, fixed cameras should be installed at screening checkpoints, terminals and all Jetway and FAR 107 portals. Individuals will be monitored boarding the plane and interacting with the ticket agents at the gate entrance. In the past, the use of PTZ cameras was used to watch multiple doors. Having one PTZ camera monitor more than one door is still a realistic approach, however, by having a digital recording system, operators at the command center can maximize the full use of the digital recording system.

For example, if a door goes into alarm, the digital recording system can be programmed to automatically back up 10 to 15 seconds, or more if needed so that the time immediately prior to the alarm can be viewed. This capability allows the very real potential to identify the suspect, what the individual was doing, and why the door went into alarm. If a PTZ camera is installed the command center operator will not have any pictures of the suspect if a door goes into alarm and the camera is not already aimed directly at the door.

By utilizing the digital recording system, if the camera has to automatically pan to the door, then the system cannot back up to see what set the door into alarm. Therefore, to be effective in these instances, the camera must be pointed directly at the door at the time of the alarm.

Although it is not in the best interest to utilize PTZ cameras in a digital recording system, it is CTI's recommendation to use PTZ cameras throughout the rest of the terminal areas to monitor additional alarm points. This would allow the command center to monitor those alarmed areas such as defibrillators, Emergency Exits, ATM machines and even monitor moving walkways to detect any problems. With cameras located throughout the terminal a suspect can also be monitored as they move up and down the terminals.

Nevertheless, PTZ cameras should be used to monitor the AOA area, especially the SIDA and secured areas of the airport. If a door goes into alarm, the system can be programmed to

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

direct the nearest camera to automatically view that area so that the suspect setting off the alarm can be viewed. This will assist a response team responding to that alarm, since they can be guided to the suspect by the command center. This is important due to the possibilities of determining if the suspect activated the alarm and accessed the AOA. For instance, if a child inadvertently bumped a door and set off the alarm, the command center can determine that no individuals went out onto the AOA and simply re-set the door.

The use of PTZ's on the outside of the terminals is also practical even when a digital recording system is being used. First, the fixed camera located on the inside of the terminal should provide at minimum a view of the suspect. Secondly, the PTZ camera located on the outside of the terminal will monitor that area where the breach is occurring and begin recording as the suspect enters the AOA.

PTZ cameras should be installed at the vehicle gates. These cameras should always view the gate until an alarm is set off. The command center operator can then retrieve video from the previous 10 to 15 seconds of recorded data, and then move the camera to follow the movement of the suspect. The camera must be set close enough to the gate and have sufficient resolution to insure that there is the opportunity to identify the vehicle and license plate if the suspect has a front plate. If the suspect does not have front plates, the PTZ can rotate and identify the back plate, as the vehicle is moving. After an alarm has been acknowledged and actions have been taken to secure the area, the PTZ cameras should be pre-programmed to return the camera to its original view of the gate.

These cameras are used with the greatest efficiency when all doors to the AOA have, at a minimum, door alarm contacts. If those doors are used on a consistent basis, then a card reader-PINpad should be installed at on the door. This will greatly change the way Massport does business. Most, if not all doors will be under the control of the airport. Companies can still utilize exclusive use agreements, but Massport will control employee access through those doors. This is a very expensive recommendation and if it is not implemented, the cost of installing cameras on all of the AOA doors would have to be questioned. If Massport does not take over the doors, then the closed circuit video system will become, for the most part, a historical log of what happens at each AOA door. This can be useful in identifying a suspect but not in attempting to proactively stop a suspect from committing a crime or terrorist act.

Recommendation #35

Develop and design a camera system for all the screening checkpoint systems that will be able to sustain a facial recognition system (if required).

Recommendation #36

Develop and design a camera system for jetways and other specific FAR 107 portals and gates as needed. Certain elements of the this system may be required to have the capability of sustaining facial recognition.

Recommendation #37

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

G. Photo ID Badging System (Access Media/ID)

The BOS photo ID badge office (security badge office) is responsible for providing tenants, construction workers, visitors and law enforcement personnel with airport approved and authorized access media. The security badge office also provides vehicle identification temporary permits and performs functions related to the authorization of AOA driving privileges on the perimeter road.

The security badge office is located on the second floor between terminals B and C, room number C2015. The security badge office is co-located with the airport parking violation office. The security badge office is open for normal operations Monday through Thursday, from 9 am to 4:30 pm, and on Friday's from 6 am to 4:30 pm.

Massport currently requires a \$30.00 application fee from ID badge applicants. Personnel are charged \$50.00 the first time they lose their security badge. Personnel are charged \$50.00 plus a fine the second time they lose their badge. On the third occasion where an employee loses his/her ID badge, he/she is charged \$50.00 and the security badge is suspended for 30 days or the badge can be terminated.

The photo ID Badge office produces over 100 photo and non-photo badges per day. All personnel performing duties at BOS are required to obtain an ID badge that denotes their security level.

There are currently five personnel performing duties at the security badge office. This number includes one temporary employee, three full time employees and one supervisor. The security badge office supervisor has overall responsibility for the operation of the office, and performs specific tasks including reconciling badge issues, reconciling daily reports, resolving application discrepancies, ensuring applications are compliant.

The supervisor is also responsible for dealing with the security badge coordinators and conducting SIDA training, which is conducted once a month.

Of the remaining personnel, one individual is responsible for systems documentation and testing, and the remaining personnel perform data entry, clerical and front desk duties.

There are two types of access to the restricted areas: unescorted access and escort required access.

Because BOS is a Security Category X airport, it must submit all individuals requesting unescorted access authority to an FBI fingerprint based, criminal history records check. Massachusetts State Police – Troop F, perform this function and submit the acquired prints to OPM for forwarding to the FBI.

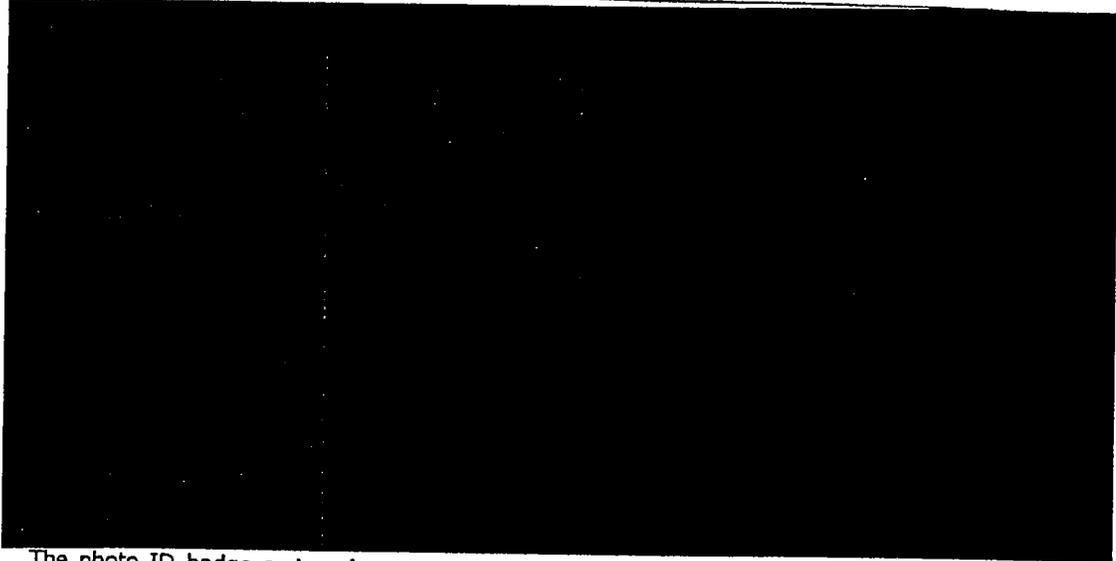
This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552

MP100669

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



The photo ID badge system has two capture stations and six workstations. The capture stations are comprised of: one Compaq workstation (approximately two years old), a JVC color camera and a NISCA model 5100 printer that is directly tied in to the capture workstation.

Ensuring the safety of BOS's employees, tenants, contractors, and passengers is a monumental task. An important part of this task is the issuance of airport media, some of which denotes that the holder has been granted unescorted access to the airport's Security Identification Display Area (SIDA).

Prior to December 23, 2000, the airport was required by FAR Part 107.31 to conduct employment history checks of any individual applying for a position requiring unescorted access to the SIDA. Since the passing of the Aviation Improvement Act of 2000 (P.L. 106-528 - effective date December 23, 2000), BOS, as well as all other Security Category X airports, are required to perform an FBI fingerprint based criminal history records check for all individuals applying for unescorted access to the SIDA.

Although the airport is only required to complete fingerprinting for each new SIDA applicant, BOS has taken a more security-minded approach to the process of issuing airport media. The airport performs its own criminal records checks to determine if an individual is suitable to continue to the next step in the BOS process, which is the FBI fingerprint based criminal history records check. This is required of all new applicants for airport ID, regardless of access level.

CTI conducted a study of the BOS fingerprint process (operations, procedures, facility, and staffing) over a two-day site visit. Following are the details describing the current practices and procedures used at BOS's fingerprint section. CTI staff interviewed key BOS personnel, including members of the Massachusetts State Police Aerodrome Section (who perform the function of fingerprinting), employees of the Massport Security Badge Office, and the Deputy Director of Public Safety.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100670

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Fingerprints are taken Monday-Friday, between the hours of 9:00 AM to 12:00 PM. Fingerprints are also taken Tuesday's and Thursday's between the hours of 7:00 PM to 9:00 PM. All fingerprinting is conducted in the State Police offices located in Terminal D. Currently, most administrative functions are performed at a separate office (down the hall from the fingerprinting office) however, future plans include relocating personnel and equipment so that the fingerprint section will comprise of two connecting offices in close proximity to the lobby area, which also serves as the applicants waiting area.

There are currently three troopers assigned to complete fingerprint duties. These troopers, however, are not exclusively detailed to provide support for the fingerprinting of personnel and other fingerprint related matters. Fingerprinting of personnel is an additional duty that was added due to the requirements of the P.L. 106-528. According to the troopers who are assigned fingerprint duties, they are not always available to support the fingerprint section, as other duties take precedence, hence the hours of operation. Because the troopers are not available for fingerprint duties on a full-time basis, three hours each day, with an additional two hours on Tuesday and Thursday, have been designated for the hours of fingerprinting. Fingerprinting of personnel does not occur at any other time.

Troop F personnel performing fingerprint tasks utilize the Identix 600 fingerprint unit for the processing of fingerprints. BOS currently has one fingerprint unit available for use; there is no backup unit at this time. It is believed by the State Troopers that there is another fingerprint unit on order and it should be available for use in the near future. In the event of a loss of power or a malfunction, troopers conduct manual fingerprinting (rolled ink method).

BOS averages approximately three hundred twenty-five fingerprints per month. Applicants are not scheduled for fingerprints as all personnel are accepted on a walk-in basis during the hours specified. In addition, there are no set times scheduled for large groups.



In order for an individual to obtain an ID, he/she must first complete a Massport Security Badge Application. Each individual tenant/airport user has a designated individual that serves as a Security Badge Coordinator. The Security Badge Coordinator serves as a quality control check-person for the proper completion of the application and also perform SIDA training.

Once the application has been completed, it is submitted to the Massport Security Badge Office. All applicants are then instructed to wait between two and three days for processing before reporting to the fingerprint section in the State Police offices for fingerprints. BOS personnel will assign the application a badge number and enter the required information into the badging system. The application is then forwarded to the State Police in Terminal D.

Troopers assigned to the Aeordrome Unit will conduct a warrant check (for outstanding warrants) and a license data check (for proof of a valid state license) once an application has been received at the State Police offices. This is the reason that applicants are instructed to

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100671

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

allow up to three days of processing time. If an applicant reports for fingerprinting and his/her information has not been processed, he/she will be re-instructed to wait the standard amount of time to allow for processing of information and will be sent away. Once the warrant check and the license data check have been completed, the applications are filed pending the completion of the fingerprints.

Applicants who arrive for fingerprints must wait in the Troop F lobby while State Troopers perform data entry functions. One Trooper enters the required information into the Identix fingerprint unit, takes each individual's prints and sends them electronically to the Federal Bureau of Investigation (FBI) via the Office of Personnel Management (OPM). Applicants are instructed to wait between seven and ten days before reporting to the Security Badge Office for badge issuance. This is an extremely inordinate amount of time.

Applications for those applicants who are not found (during the warrant check and the license data check) to have unfavorable information and whose FBI results sheet does not disclose any FAA, legislative, and Massport designated disqualifying type crimes, will be signed by a Trooper and forwarded to the Security Badge Office for badge issuance. In addition, Troopers update an applicant's information in the badging system to reflect his/her badge issuance eligibility. The FBI results and a printout of the applicant's fingerprints will be filed alphabetically. Only then will those applicants be issued a BOS ID badge once they report to the Security Badge Office.

Applications for those individuals who are found (during the warrant check and the license data check) to have unfavorable information will be denied issuance of an ID and unescorted access. Those individuals will not be allowed to undergo fingerprinting for the FBI criminal history records check. They will instead receive a notification letter advising them to report to the State Police offices in Terminal D so that an officer may review the information with the applicant. This same notification letter will be sent to those individuals who have been fingerprinted and whose FBI results disclose evidence of FAA, legislative and/or Massport designated disqualifying type crimes.

If, once the information has been reviewed with the applicant and he/she has been informed that he/she is denied the issuance of an ID badge that provides unescorted access to BOS' SIDA, the applicant wishes to contest the findings, he/she will be referred to the Director of Public Safety for resolution. The Director of Public Safety will set a hearing date and forward his final decision in writing to the State Police, Aerodrome Unit. Final decisions may range from ID denial to temporary badge status based on successful periodic (30, 60 or 90 day) criminal records checks.

The current operating hours of the Security Badge Office are 9 am - 4:30 pm, Monday - Thursday and 6 am - 4:30 pm, on Fridays. All fingerprint results sheets and any other fingerprint related information is kept at the Troop F State Police office, fingerprint section. All Massport Security Badge Applications are also kept on file at the State Police offices during the badging process, until the applicant is either approved for or denied an ID badge. Once the process has been completed, all Massport Security Badge Applications are kept on file at the Security Badge Office.

When the FBI completes criminal history records checks, the results of those checks (if there is no record involved) are forwarded electronically to an FAA secure website. After authorized access, these results can be downloaded daily for printing and saved onto a

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100672

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

backup disk. Once the results sheets have been printed out, troopers file them with a copy of the individual's fingerprints printed on a fingerprint card. Massport uses these as proof for FAA auditors that fingerprinting was accomplished for each individual requesting SIDA access. All the Notice of Investigation sheets are discarded.

Currently, the Deputy Director of Public Safety is attempting to better track submitted fingerprints. State Police personnel are reluctant to get involved in the accounting of fees accumulated in the fingerprint process, as it is not a law enforcement issue. Each of the troopers can liaison with the FAA or OPM when fingerprint issues need to be resolved. If results for an individual have not been received, a list will be faxed to the OPM Investigations Office. OPM will respond with a status update.

Information for tenants/airport users is disseminated via the Badge Coordinators. Meetings are held with the Badge Coordinators whenever new information or procedures must be passed along. The Badge Coordinators are responsible for ensuring that those individuals for whom they are responsible receive this information.

The goal for Massport is to have in place a fingerprint section that can process all required applicants in a timely manner and that is responsible for the day-to-day maintenance, control and tracking of all fingerprint related matters while answering to the Director of Public Safety. The following recommendations provide options to reach this goal. However, the large amount of applicants, plus the additional requirements in the Massport ID process, lend to a higher probability for an unnecessary extended waiting period:

Recommendation #38

Massport should strongly consider simplifying recordkeeping procedures to only include the Results Sheets -- accomplished automatically and electronically, these sheets contain all necessary information needed to show proof of fingerprinting for an auditor.

Recommendation #39

Massport should develop and maintain a comprehensive fingerprinting financial tracking system.

Recommendation #40

Massport should extend the FBI fingerprint based criminal history records check hours of operation to five days a week (Monday through Friday), 8:30 AM to 4:30 PM each day.

Recommendation #41

All procedures and operations involving the fingerprint process, from the initial step (completing the application) to the final step (badge issuance), should be developed into a standard operating procedures manual

Recommendation #42

Massport should accomplish an FBI fingerprint based criminal history records check operations staffing, equipment, and training needs analysis.

Recommendation #43

Massport must make every effort to ensure that individuals who are not applying for unescorted SIDA access are not being subjected to an FBI fingerprint based criminal history records check at this time.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100673

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Recommendation #44

Massport should develop contingency plans for potential federally mandated fingerprinting of all active BOS security access ID holders employed previous to December 23, 2000.

Recommendation #45

Massport should consider a training and equipment needs analysis.

Recommendation #46

Massport should conduct a comprehensive study of the ID badging office operation, current hardware/software systems.

Recommendation #47

BOS ID badges should be reviewed for redesign and delineation of authorized access areas.

Recommendation #48

SIDA training should be updated to address the current security baseline.

Recommendation #49

Massport should consider the development of an ID badging and access control policy and procedures manual for system users.

H. Vehicle Identification and Control

An Aerodrome license allows an individual to operate a motor vehicle on the AOA. Only those individuals who have an Aerodrome license designation on their photo security badge are permitted to operate any motor vehicle on the Aerodrome. There are three different classes of licenses, Class 1, Class 2 and Class 3, issued at BOS.

All vehicles must permanently display company designs or insignias in a manner that makes them easily recognizable. All vehicles having access to the AOA are required to have one of the BOS issued permits (permanent, temporary long term, temporary short term, or escort).

Permanent permits are issued by the State Police and are issued for vehicles that are used for daily operations. Long-term temporary permits are issued by the State Police and are issued for contractor vehicles while the contractor is performing work at the Airport. The permit is subject to renewal, based on contract extension. Short-term temporary permits are issued by the Aerodrome Office and are issued to vehicles who are serving on an emergency or short term basis. Escort permits are arranged by the North or South Gate Guards. The Gate Guard logs in the required information prior to issuing an escort permit.

Other vehicles requiring access to the AOA through any of the authorized airline/tenant controlled vehicle access gates shall remain within the confines of that airline/tenant leased area through which access was provided. The airline/tenant is required to maintain a constant surveillance of the vehicles that have been provided access to their leased area, to ensure that penetration outside of their leased area does not occur.

Recommendation #50

Massport should develop and undertake a vehicle-permit audit and revalidation program to ensure 100% accountability of authorized vehicles entering and operating within the AOA.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

Subject to Confidentiality Protective Order

Page 33 of 59

In re September 11 Litigation

21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)

MP100673A

Do Not Copy or Disclose

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

I. Security Lock and Key Management and Control

The security lock and key program for BOS is a Facilities Department responsibility. Facilities personnel with lock and key responsibilities include three locksmiths: one foreman, one supervisor and one assistant manager. All lock and key services, which include providing preventative maintenance to all FAR 107 portals and other internal airport portals, including cutting and installing of all keys and key cores throughout the airport (except for tenant controlled areas), are performed at the BOS lock and key shop. All training for lock and key personnel is conducted in-house, that is, Massport employees train their own staff.

All key requests must be approved by the Assistant Director of Public Safety and the Deputy Director, Aviation Facilities. Individuals requesting issuance of security keys or installation of security locks, must complete and submit a Key Request Form, which are available at the ID badge office. If the request is approved, a copy of the request will be forwarded to the lock and key shop. Once an approved request has been received, lock and key personnel will perform the requested duties; cut new keys, install new locks, etc.



The lock and key shop orders approximately 300 keys on a quarterly basis. Keys are maintained inside the shop in a security cabinet.

The Deputy Director of Public Safety created a program to begin numbering all keys and to begin the electronic recording of all key related information (key number, person issued to, etc.). The program was used during the re-keying of all Massport gates. The eventual goal was to re-key the entire Airport and record the information electronically. However, it was quickly discovered that the resources available were not able to handle such a large task.

As a result of the manpower issue, it was determined that a consultant would be hired to conduct a re-keying assessment and the same or a different consultant firm would be hired to carry out the recommendations as found in the assessment. Although this is something the Deputy Director of Public Safety advocates as necessary, Massport has not moved forward in this issue.

Prior to the new key program being created, the lock and key shop kept a written record of issued keys, with no information being kept by electronic means. Since Massport decided that the re-keying of the Airport was to be contracted out, however, the lock and key shop continues to maintain a written record of all key related information.



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100674

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



Recommendation #51

Massport should develop and complete a comprehensive security lock and key control program audit of BOS, including tenant-controlled areas, regardless of the difficulties expected in accomplishing such a task

Recommendation #52

Massport should develop and implement a new from-scratch key control program, including the re-keying and re-coring of all applicable security portals, new managerial lines of responsibility, including maintenance responsibilities, and the establishment of a comprehensive audit cycle.

Recommendation #53

Massport should strongly consider an electronic security lock and key control recordkeeping database.

Recommendation #54

Massport should strongly consider the development of a comprehensive security lock and key control program to include a solid security rationale for the issuance and retrieval of all keys and combinations/cipher-codes, enforcement of lost/stolen key procedures, and set periods of time when locks must be re-cored or combinations/cipher-codes changed.

Recommendation #55



Recommendation #56

Massport should consider an extensive and effective security lock and key control enforcement program.

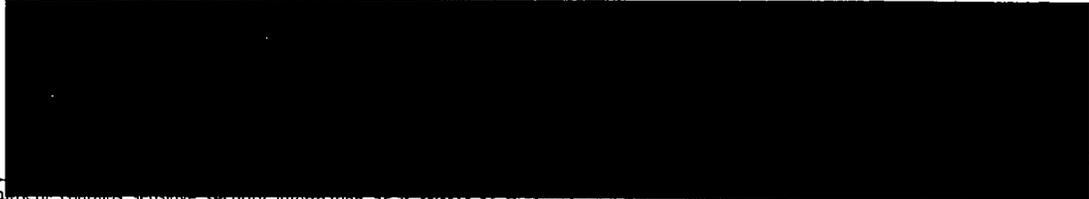
Recommendation #57



Recommendation #58



J. Security Communications



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100675

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100676

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



Recommendation #59

Massport should incorporate a program to ensure that all communication center personnel are certified to perform the duties and functions of a Keybase Operator.

Recommendation #60

Massport should upgrade the Access Control Alarm Monitoring System to ensure timely and effective system operation.

Recommendation #61



Recommendation #62

Massport should update and expand, in direct concert with Public Safety, a comprehensive Access Control and Alarm Monitoring Policies and Procedures Manual.

Recommendation #63

Massport should develop and perform an in depth review and analysis of communications center staff functions to determine, among other things, whether additional training and/or system modification are in order.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100677

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Recommendation #64

Massport should perform an evaluation of the communications centers organizational structure and operating efficiency to include comparison and review of ACS data vs. survey results, current training, operator knowledge and capabilities, system capabilities, and other conditions identified as needing modification.

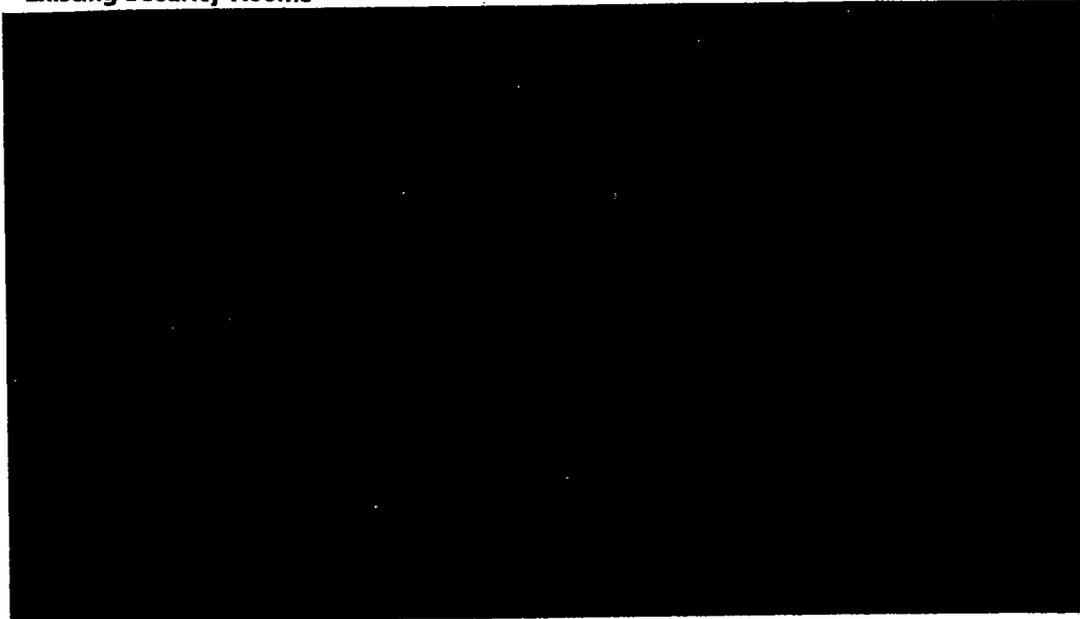
Recommendation #65

Massport should perform a complete system functional test of the entire access control and alarm monitoring system, including peripheral systems and programs.

Recommendation #66

Massport should perform a comprehensive feasibility study for the design and operation of a consolidated alarm monitoring and dispatch center.

K. Existing Security Rooms



Recommendation #67

Security controls and procedures should be assessed annually.

L. Perimeter Barriers/Exterior Security/Accessways

The Airport has a combination of chain link fence, masonry re-enforced wall (blast wall), plywood fence, and a water boundary that make up the airside perimeter. Several different facilities also make up part of perimeter.

There are two main vehicle access points into the Airport, the North Vehicle Gate and the South Vehicle Gates.

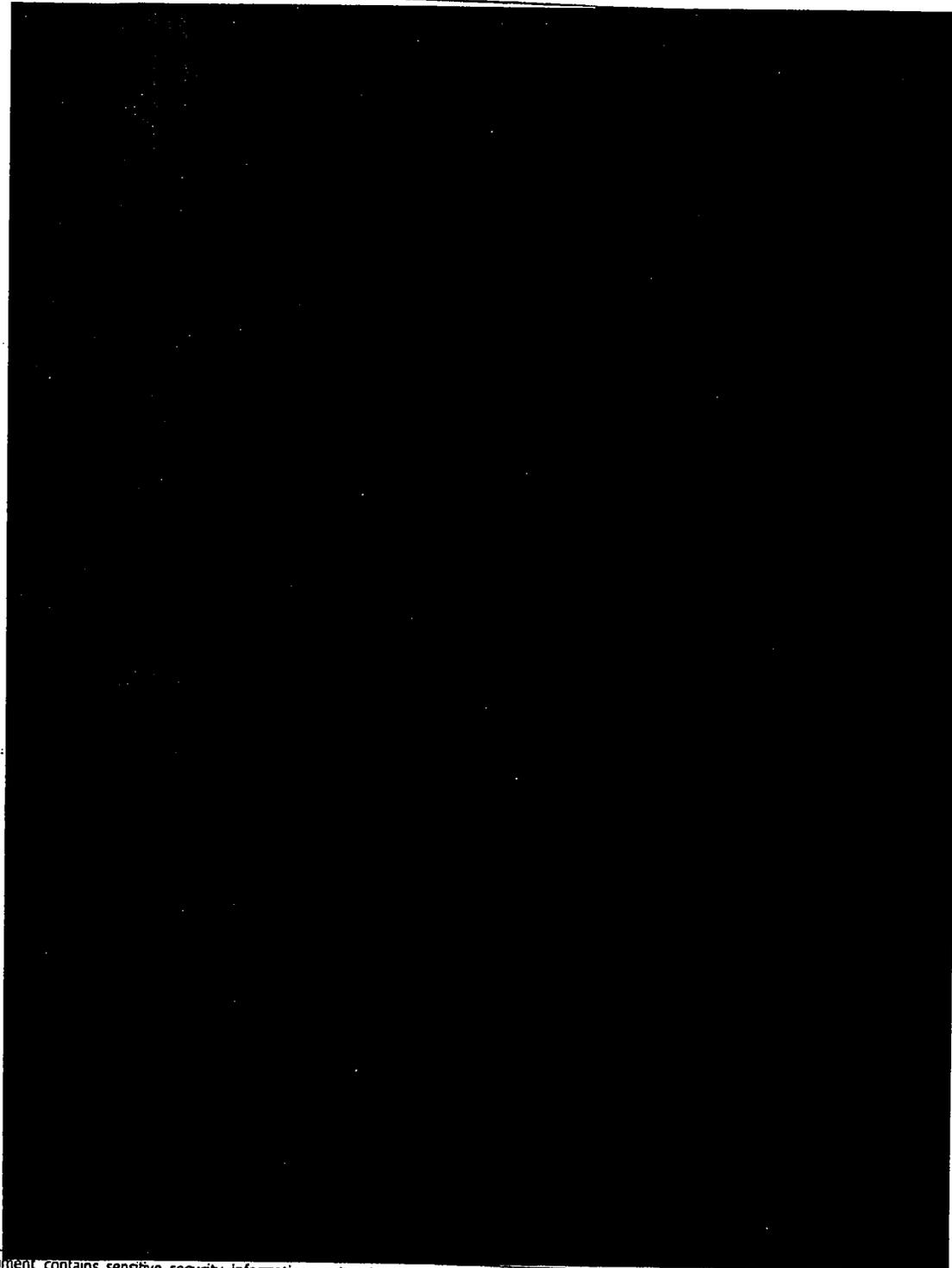
This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100678

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



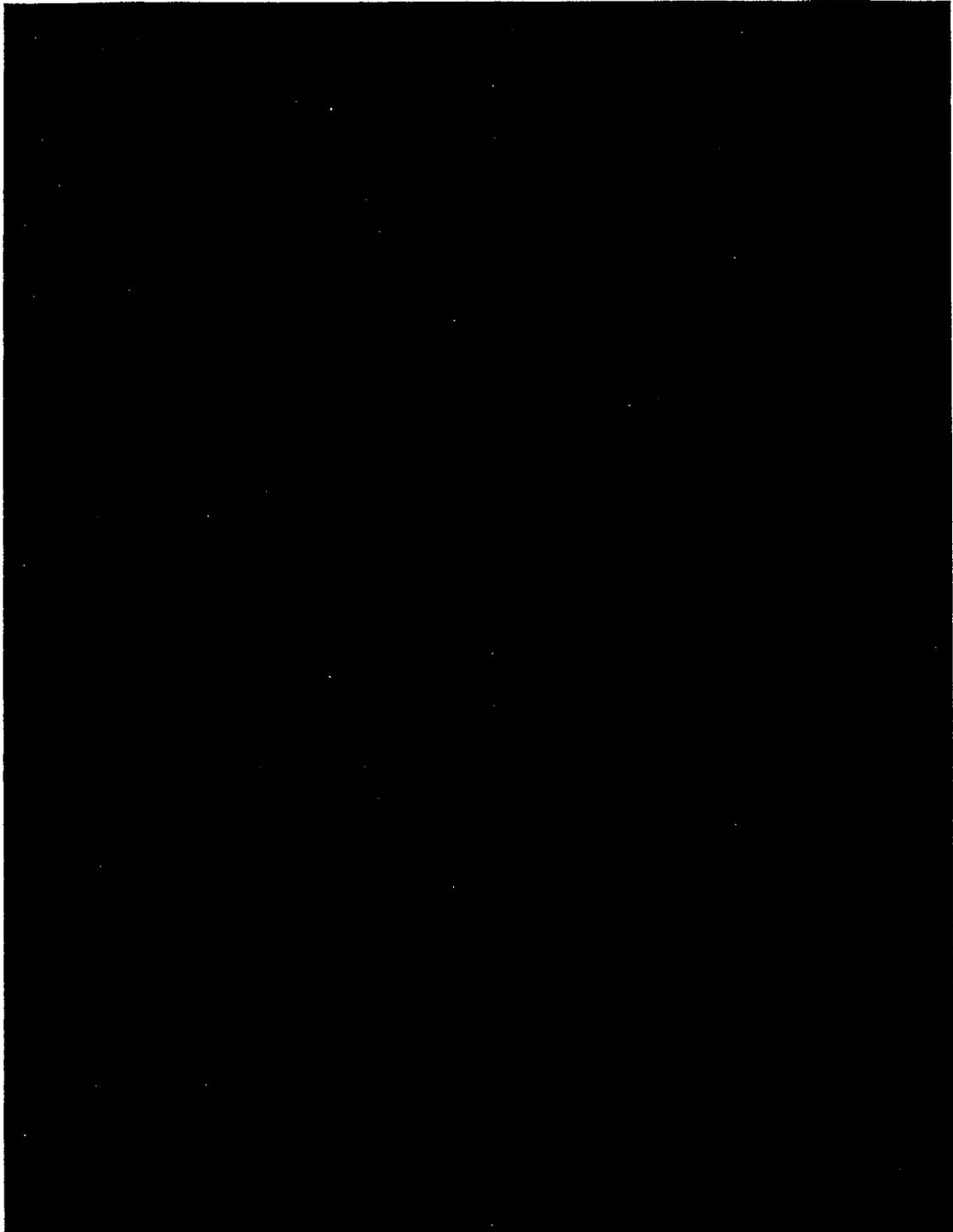
This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100679

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100680

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

This document contains information that is confidential to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100681

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Unfortunately, the use of any type of perimeter alarm system would have a minimal return on security as well as produce an extremely large number of nuisance alarms. Any attack on an aircraft at the Airport itself could be accomplished from the water and/or the residential areas across the water. Additionally, such a perimeter alarms system would have an inordinate number of maintenance issues. This system will ultimately be very costly because of the distance around the perimeter and the type of landscaping areas located adjacent to the harbor. If such a system can be programmed to become less sensitive, thus reducing the frequency and type of false, or nuisance, alarms, then the effectiveness of the system to assist in the apprehension of a suspect attempting to gain access to the AOA might be reduced.

The Department of Defense has provided grant money to a number of universities studying the use of video cameras, which have motion sensor perimeter alarm options. The FAA Tech Center, is part of the team that is studying these systems for possible use at airports. At this time, the two biggest problems being faced with regarding such a system include first the amount of light that has to be available, even low light cameras require additional lighting resources. The second problem involves the frequency of planes landing and taking off that will interrupt a cameras view and activate the motion sensor perimeter alarm.

An active infrared red (IR) system and/or a seismic motion sensor system each have various problems when installed at or near water. The leaky coax and similar capacitance type systems are also affected negatively around water. The two most promising systems include microwave fencing or passive infrared detectors. A number of microwave systems might be better able to handle a large perimeter, but a more detailed study regarding power and alarm signal capabilities should be performed. This also holds true for a passive IR system.

Areas that are of immediate concern to Massport could be developed immediately while the other areas of the perimeter are reviewed for a more effective perimeter alarm system. The threat of an intruder from the perimeter is low given the time and distance that the intruder would have to travel to get to an enplanement area for either a passenger or cargo aircraft. The weapon of choice from this perimeter would more likely be a rocket or missile being fired at an aircraft as it lands or takes off. These are the two most critical times for this type of attack on an aircraft.

Twelve "No Trespassing" signs were identified along the entire perimeter that borders the water, several of which were in the same general area. BOS does not have enough signage or posted warnings along the perimeter that borders the Boston Harbor Channel.

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

The cost for fencing and upkeep around the harbor separating it from the AOA will be considerable, and methods must be developed to prevent the fence from becoming a hazard to aircraft landing and taking off. There are types of bushes as well as other shrubbery that have a high degree of preventing individuals from entering a secured area. It will take time to study the area, and determine if the ground terrain and temperature will allow this type of barrier to be suitable. The upside is the lower cost and maintenance with the primary upkeep to the shrubbery to be trimming, which is something that would have had to be done anyway with a fence system.

Recommendation #68

Massport must identify and decide on one uniform type of perimeter barrier. This will require a comprehensive cost benefit needs analysis to identify the appropriate option.

Recommendation #69

Massport should add additional trespass prevention signage.

Recommendation #70

Massport should strictly enforce perimeter clear zones as described in the BOS FAA approved Airport Security Program and FAA Emergency Amendments.

Recommendation #71

Massport should perform a comprehensive cost benefit needs analysis for a perimeter control intrusion detection system.

Recommendation #72

Massport should establish and enforce a continuous and effective perimeter patrol program.

M. Protective Lighting

CTI staff conducted after hours and late night tours of the airside exterior areas, specifically the perimeter. The lighting assessment focused on nighttime artificial illumination. Lighting along the perimeter road was almost nonexistent. After the attacks on September 11, 2001, CTI made recommendations on the placement of temporary lighting structures along the perimeter fence area adjacent to landside (next to the water). These recommendations were immediately heeded.

Recommendation #73

Massport should perform a comprehensive assessment for the identification and installation permanent security lighting structures along the perimeter fence and other vital areas.

N. Law Enforcement Officers (LEO)

A detachment of the Massachusetts State Police, specifically Troop F, provides the LEO responsibilities at BOS. Troop F offices are located in Terminal D. The State Police are fully accredited peace officers in the state of Massachusetts and as such, are able to carry out police functions and execute arrests in accordance with FARs for Airport LEOs. State Police at BOS have the necessary resources to handle any law enforcement situation, including Explosives Ordinance Detachment (EOD), FAA Certified K-9 Explosives Unit, detective unit, and tactical operations from incidents involving hijackings, or hostage barricades. Unlike any other Security Category X Airport, BOS currently has on staff eight FAA certified explosives K-9 units with two more in training; FAA standards call for six.

This document contains security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5115C 552 .. 2

MP100683

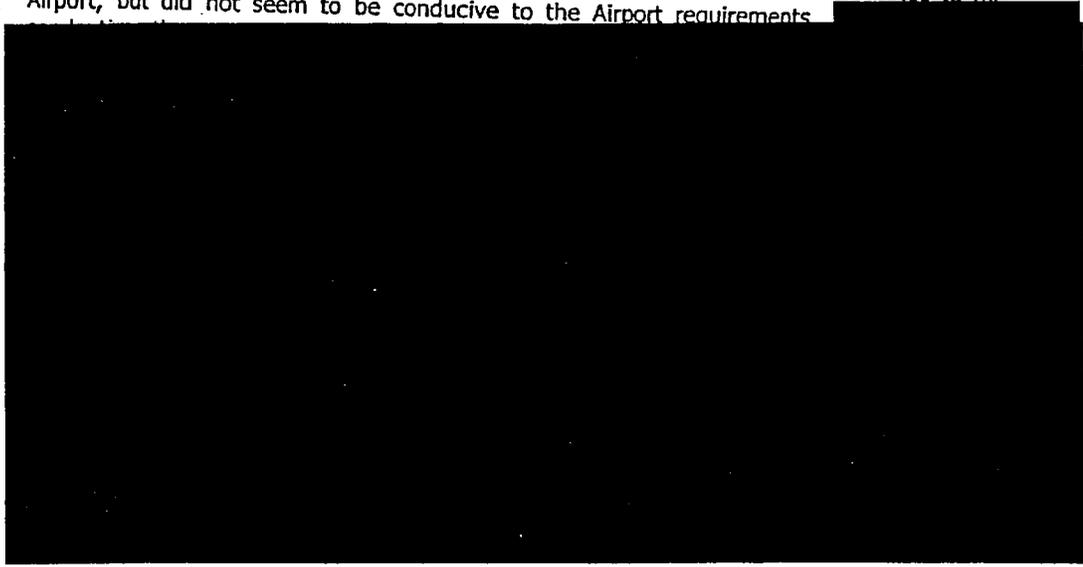
**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

The State Police are commanded at the Airport by senior police staff, with the overall commander holding the rank of Major. The Major, the Troop-F commander, reports to the Director of Public Safety who is responsible for oversight of police functions and coordination of services at the Airport.

Before September 11, the State Police had an adequate number of staff dedicated to the Airport, but did not seem to be conducive to the Airport requirements.



Troop F LEOs and Public Safety enjoy a good working relationship. Massport LEOs are not only well equipped, but also well funded by Massport. Because of this, LEOs are able to participate in several specialized training opportunities, such as Weapons of Mass Destruction training in Quantico, VA.

According to the Troop F commander, the LEO SOP is currently under revision and the Director of Public Safety is being included in its review. The last date of revision date of the LEO Training Manual is unknown. LEOs are active participants in Massport required tabletop exercises. Further, the Troop F officer in charge during an emergency is included in the Massport AEP as the designated incident commander for the following emergencies:

- Bomb Threats
- Civil Defense/Riots
- Hijacking
- Hostage Taking
- Roadway/Traffic Emergency
- Sabotage/Terrorism

Recommendation #74

Massport should develop and establish recurrent civil aviation security and terrorism training and awareness for Massport LEO members.

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

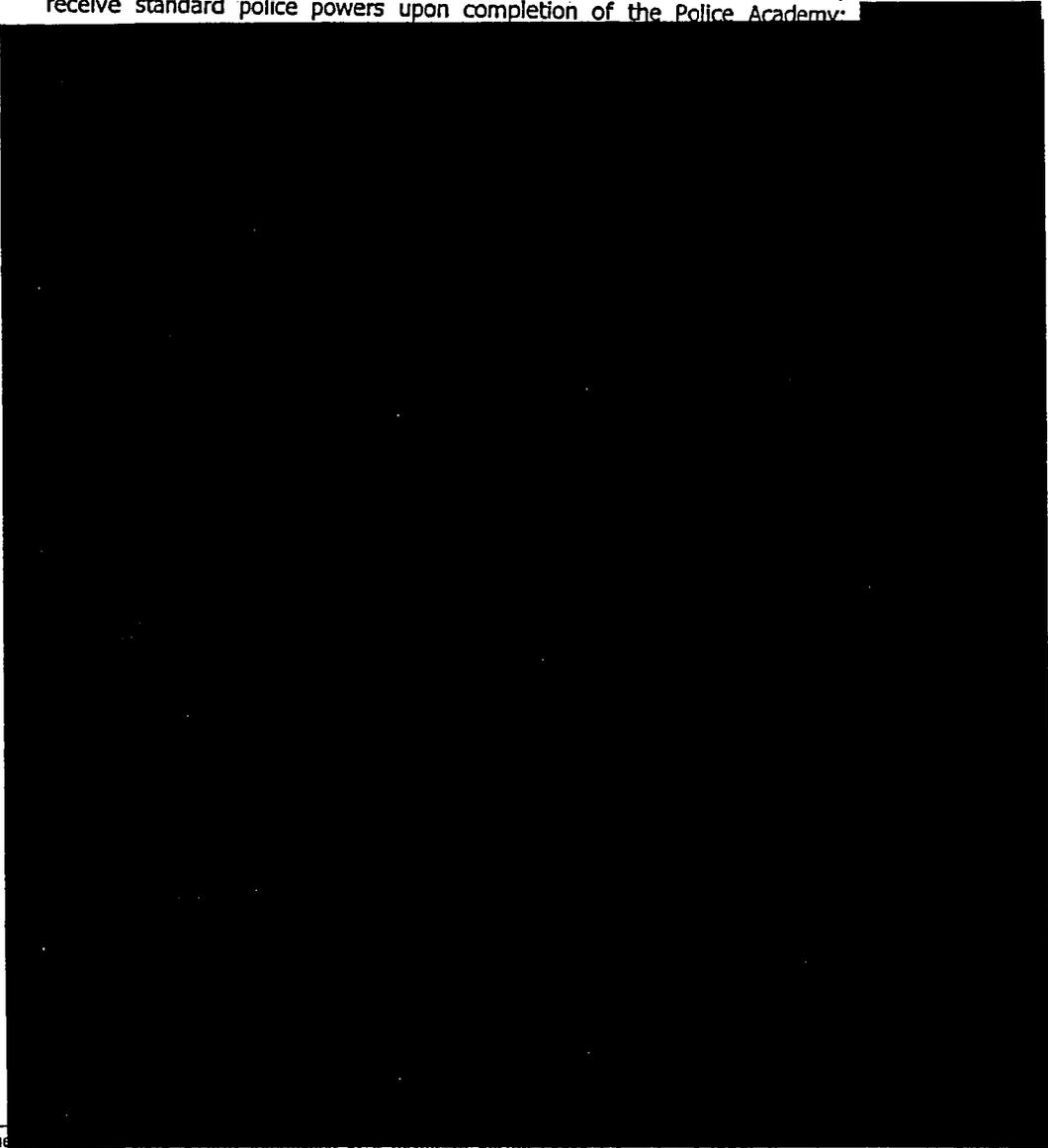
FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

O. Logan Guard Services

BOS utilizes Gate Guards to perform vehicle access control duties at the North Gate, the South Gate and the Community Gate (Maverick Street). They report to and are a function of Operations, not Public Safety. The authorized strength of the Gate Guard force is 18 (this number includes 1 supervisor, Sergeant rank). The Gate Guards' primary function is to deter unauthorized entry. Although the Gate Guards are issued ticket books and are authorized to write violations, they very rarely do so.

The requirements for employment as a Gate Guard mirror that of the State Police, that is, all Gate Guards must attend and successfully complete the Police Academy. Gate Guards receive standard police powers upon completion of the Police Academy:



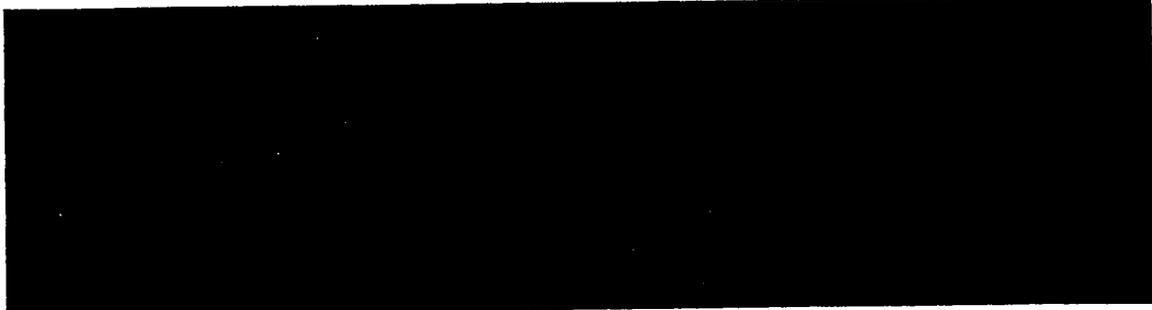
This document contains security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Acquisition Information, see FAR 101-11.6.

MP100685

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



P. Airport Security Program (Plan) Manual [ASP]

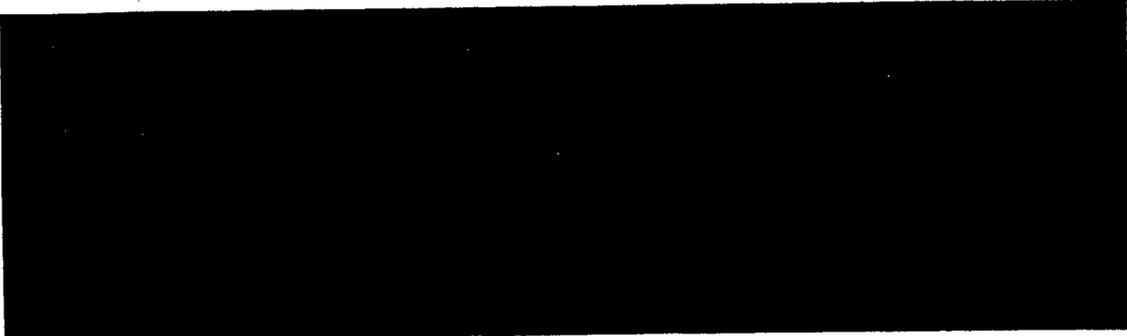
The main body of the BOS ASP is comparable to other Security Category X Airports, however, the appendices greatly increase the size of the manual, mainly because of the extraordinary amount of construction projects. Although the ASP does meet the FAR, it should be re-written. The last full revision occurred as a result of an earlier assessment.

The ASP will have to include information and structure as required by the new FAR 107, effective November 14, 2001, which includes such issues as the new ASC training requirements and the FAA required index. Although the FAA is not requiring a full re-write, it would be to BOS' advantage to re-write the ASP to incorporate these issues, to create a cleaner version since there have been several revisions and changed conditions, and to ensure that the information is current and accurate.

In the wake of the tragic events of September 11, 2001, and in direct consideration of the numerous Federal Aviation Administration (FAA) Emergency Amendments (EA) that continue to be developed and issued, CTI believes it prudent to stay any revisions to the ASP for further guidance from the FAA as it undoubtedly will continue to evolve. Further, all Massport resources are currently being directed towards addressing and supporting the requirements of, but not limited to, the numerous EAs that continue to arrive.

Nevertheless, revisions and changed conditions are accomplished by the Deputy Director of Public Safety. The ASP has had several different revisions that the current document has a patchwork effect. The page structuring and formatting (font style, font size and page numbering schemes) are suitable and allow for ease of reading and use.

The Deputy Director of Public Safety is responsible for reviewing the ASP on a regular basis to ensure that it is accurate, and that revisions and changed conditions are incorporated.



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US-Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100686

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Recommendation #75

Massport should immediately and respectfully request an indefinite extension of 14 CFR FAR Part 107 provisions that become effective November 14, 2001; specifically, those concerning the Content of the Airport Security Program, as found in 14 CFR FAR Part 107.103, et al.

Recommendation #76

Massport should begin to prepare materials and information for the updating of the ASP, to include the possibility of completely rewriting the document.

Q. Airport Emergency Plan (AEP)

The AEP was last revised on October 23, 2000. The BOS AEP is comparable in size with other Security Category X Airports. The AEP is written in such a way to where it addresses all the emergency issues necessary without being too detailed or too ambiguous in its language. The page structuring and formatting (font style, font size and page numbering schemes) are suitable and allow for easy reading and use.

The AEP is written in accordance with AC 150/5200-31A and FAR Part 139. FAR Part 139, however, is currently under re-write. Once published, the AEP will undoubtedly need to be revised. AEP revisions are accomplished by the Emergency Planning Committee. The AEP is reviewed on a regular basis by the Director of Public Safety for accuracy, revisions and changed conditions. The Director of Public Safety is charged with ensuring that all parties included in the AEP are consulted every twelve months to verify that all agencies are aware of their responsibilities and that the information in the AEP is current.

The AEP clearly assigns responsibility to organizations and individuals for carrying out specific actions at projected times and places in responding to an emergency. The AEP contains tables with clear lines of authority and organizational relationships. The tables list the type of emergency, the lead agency and the incident commander for each listed emergency.

Although the AEP is complete in its information and coordination with Massport entities and non-Massport emergency services for the listed emergency conditions, it appears that no formal Memorandum of Understanding or Memorandum of Agreement exists with any of the participating Massport and non-Massport agencies or departments. Thus, deficiencies could lead to breakdowns in the response or communications by non-Massport agencies.

Recommendation #77

Massport should begin to prepare materials and information for the updating of the AEP, to include the possibility of completely rewriting the document, in response to the official published date of the rewrite of 14 CFR FAR Part 139.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100687

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

R. Shipping and Receiving



Recommendation #78

Massport should perform a comprehensive assessment of all shipping and receiving procedures to ensure they are tightly controlled.



S. Construction/Renovation

Initial plans called for a 4.5 billion dollar, seven-year construction and Airport renovation program, however, some projects have been suspended because of the events of September 11, 2001. At its regularly scheduled board meeting held in October, Massport officials proposed cutting 37%, or \$280 million, from the Fiscal 2002 and 2003 capital budgets, allowing the vital modernization of Logan to continue while deferring 139 projects. The proposal cuts \$62 million out of \$322 million from the FY02 capital plan and \$218 million out of \$427 million from the FY03 capital plan. The Massport Board is set to vote on a detailed revision of the capital budget in November 2001.

Projects that are retained in the proposal include:

- Terminal A replacement
- International Gateway (Terminal E expansion and renovation)
- Central Garage renovation
- All roadway work at Logan
- Routine airfield maintenance projects

Projects that have been removed from the short-term capital budget include:

- West Concourse for International Gateway
- Customs facility at Terminal B (design work will continue)
- Terminal B Garage renovation



**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Enforcement of security rules and regulations in these areas has, according to the enforcement entity for construction security compliance, become a daunting task. Before September 11, there was clearly a lack of support for the consistent enforcement of the regulations as they were written. The enforcement entity responsible for issuing violations and the adjudication manager responsible for upholding or reducing the fines issued for violations did not work together to provide a consistent and effective enforcement policy of the CMRs as they are written.

Prior to September 11, the adjudication process for issued violations included a hearing with the Deputy Director of Public Safety. It was at that hearing that alleged violators could plead his/her case. It was also clearly evident that the Deputy Director of Public Safety and the Public Safety and Security Manager disagreed with the final disposition of a violation on many occasions, most particularly due to the frequent lowering of fines or the outright dismissal of the violation. At the time of this assessment, no indication was given that any measures had, or were in the process of being established to correct or mitigate any support issues of the enforcement policy.

Recommendation #80

Massport should develop procedures with construction management to detail notification to BOS of all security related facility modifications, before they occur.

Recommendation #81

Massport should enhance the duties and assignment of the SIDA security enforcement teams, with data collection and analysis to assist in identifying problem areas requiring coordination with various facilities' upgrade programs.

Recommendation #82

Massport should establish policies and procedures for updating as-builds for on-going and future BOS renovation and construction projects/programs.

T. Parking

The total number of commercial parking spaces under revenue control at Logan is 11,800, and the total number of parking meters is currently 84. These are large revenue producers for the Airport, approximately \$61 million in the last fiscal year.

Prior to September 11, parking services staffed approximately 170 employees. Since September 11, that number has decreased due to budget cuts and loss of parking facilities due to additional FAA security measures. Regardless, parking attendants perform several different functions, including being visible in the garages, which indirectly raises the level of security. All parking service employees are required to be able to receive an Airport issued photo ID, which requires an NCIC check and the successful completion of an FBI fingerprint based criminal history records check.

The majority of staff are employed as cashiers. Parking services also employs two full time ticket writers. These employees are responsible for issuing parking related tickets at all areas except for those in front of the Terminals. These tunnels are the responsibility of the State Police. Nonetheless, towing for the Airport is the responsibility of parking services personnel; these positions are Massport positions, not contractors. Parking services has five tow trucks available for use. Towing is conducted at the direction of the State Police and, since September 11, towing has been consistently enforced.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100689

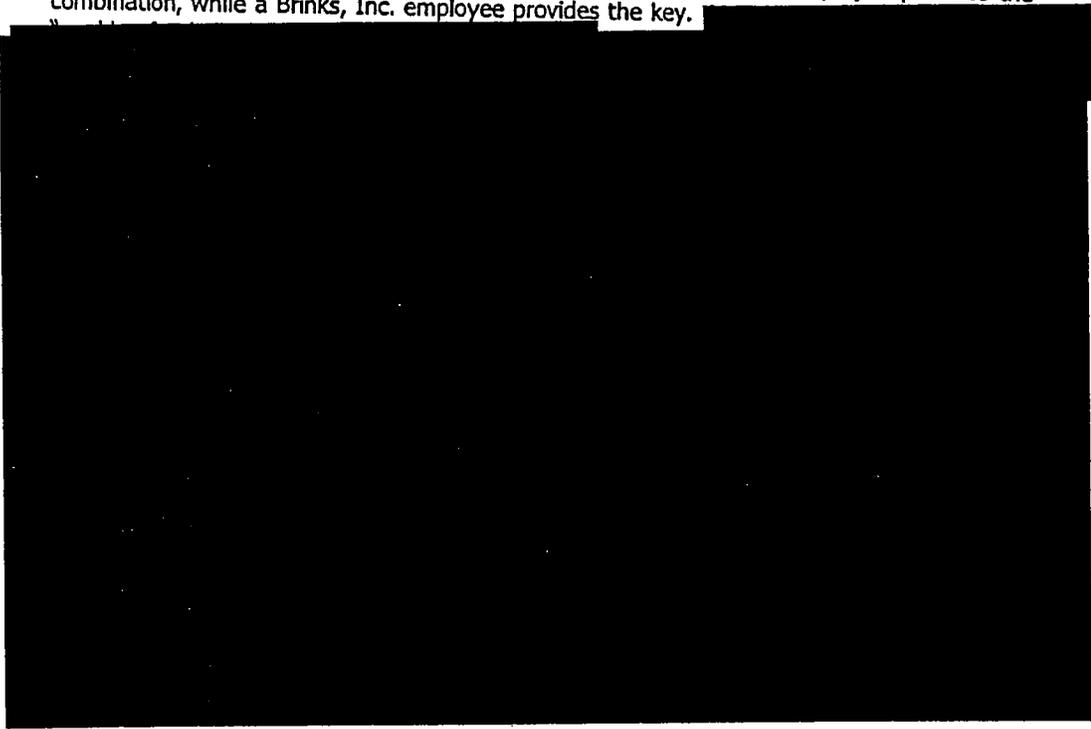
**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

Because of the large amounts of revenue parking produces, security is a legitimate concern. However, there have been few cases of theft of parking related funds (5 in 30 yrs); the last occurred in 1996. No thefts have occurred since the current CCTV system was put in place. Also, the parking areas are patrolled by parking service employees and the State Police on a regular basis. The Manager, Parking Facilities, will contact the State Police if there is a problem area (assaults, thefts, vandalism, etc.) anywhere on a Massport controlled parking area. State Police will enhance security in the problem area, i.e. providing plainclothes troopers to provide surveillance and additional presence.

All parking funds deposits are secured in the "deposit vault" until they are turned over to Brinks, Inc. personnel. Brinks, Inc. personnel retrieve the deposits on a daily basis. Both a combination and a key are required to open the vault. A Massport employee provides the combination, while a Brinks, Inc. employee provides the key.



Employee parking is contracted out to Pilgrim Parking in Chelsea. Parking employees must have the proper decal affixed on their vehicle to be authorized to park in an employee lot. If an employee is using a different vehicle without notifying the proper personnel, his/her vehicle will be tagged, as the employee lots are patrolled regularly.

Recommendation #83

Massport should provide recurrent security awareness training to all parking personnel.

U. Visitor Control for FAA/Massport Tower



This document is classified as "Confidential" because it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100690

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

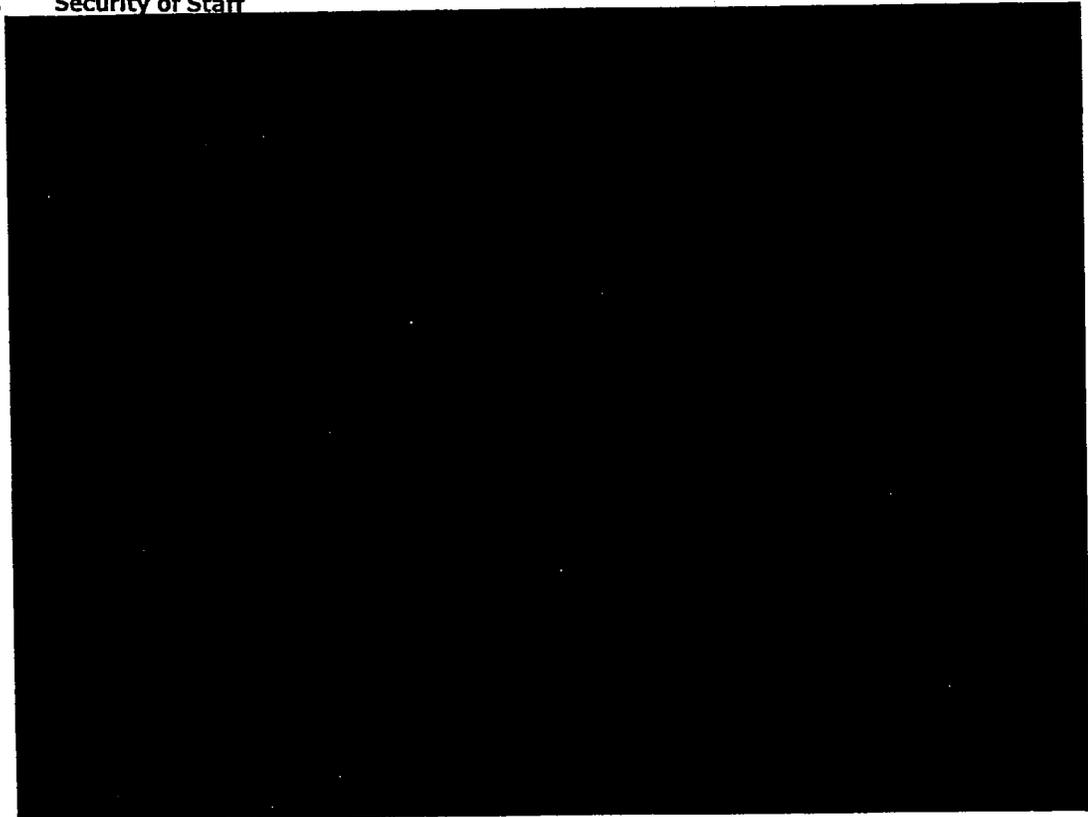
November 6, 2001



These new access control procedures went into effect on October 31, 2001. Further, also effective October 31, 2001, a Massport LEO is posted just outside the elevator bank in the lobby of the Old and New Tower.



V. Security of Staff



This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100691

**Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose**

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

her escape route, however, it is highly unlikely that she would be able to reach the back door and escape unless she was already standing very close to it.

This type of scenario may not exist at all offices, hence the need for a current site review. With panic alarms in place, State Police response could occur in under a minute since troopers already have a presence in the terminals. Regardless of whether panic alarms are feasible, LEO interior patrols could greatly assist with the security of staff in this type of situation.

Recommendation #84

Conduct a BOS site review for installation of panic alarm hardware. The site review should be conducted by the Department of Public Safety with assistance and input from the State Police.

Recommendation #85

Install a centrally monitored and frequently tested panic alarm system at those locations determined by the site review.

W. Workplace Violence, Safety and Security

The workplace violence program in place at BOS is the same for all of Massport. While the program includes a threat assessment team, it is difficult to make a determination as to whether or not the majority of employees are aware of its existence or its purpose. The reason for this is that while there is a document that deals with workplace violence at Massport, it is not issued to all employees. CTI was informed that all supervisors and department heads are supposed to receive a copy of this document, along with other documents, in a binder that together make up the "Massachusetts Port Authority Policies and Procedures Manual For Administrative Employees."

These Policies and Procedures are administered by the Human Resources Department and were last revised on January 1, 1999. Since the policies and procedures are not issued to every employee, it has been the responsibility of supervisors and department heads to disseminate the information as necessary and to make available the documents for Massport employees to read. The document is available electronically but only to those employees with Intranet access. Unfortunately, however, no notice has been given to employees notifying them that this document is available via the Massport Intranet.

The workplace violence program document, titled "Policy Against Violence in the Workplace," supersedes a December 1997 version titled, "Policy on Violence in the Workplace." The differences between the two are minor: spelling changes, a word change, an added telephone contact number (state police), and a revised formatting scheme.

Topics covered in the document include the following:

- Definitions and Scope
- Prohibited Conduct
- Procedures for Reporting Violations of this Policy
- Procedures for Investigations
- Preventative Measures

Upon further review, the program lacks in depth a thorough violence/threat assessment program, or a crisis management program that should include an incident response team,

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100692

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

and an incident/emergency notification strategy. The program also fails to address a zero tolerance policy statement to be acknowledged by each employee, the recordkeeping of such acknowledgements and incidents of threat or violence. Further, the program allows far too much time to elapse before the Threat Assessment Team is called to order; 24 hours.

While the program requires annual training, such training does not occur. The last formal workplace violence course apparently occurred in October 1998; a "lunch bag" session that had inadequate attendance. Furthermore, that training curriculum failed to identify the different types of violence, their causes, how one can protect themselves and their co-workers, and why reporting workplace violence is extremely important. The curriculum also failed to address such other topics as stress management and conflict resolution. Additionally, while the policy calls for an additional session specifically designed for supervisory staff, such training has not occurred.

Recommendation #86

Develop and establish a more comprehensive workplace violence program to include better documentation, clearer notification procedures, clearer after action activities, and a crisis management program that includes notification and communication procedures, incident response procedures and improved recurrent staff training.

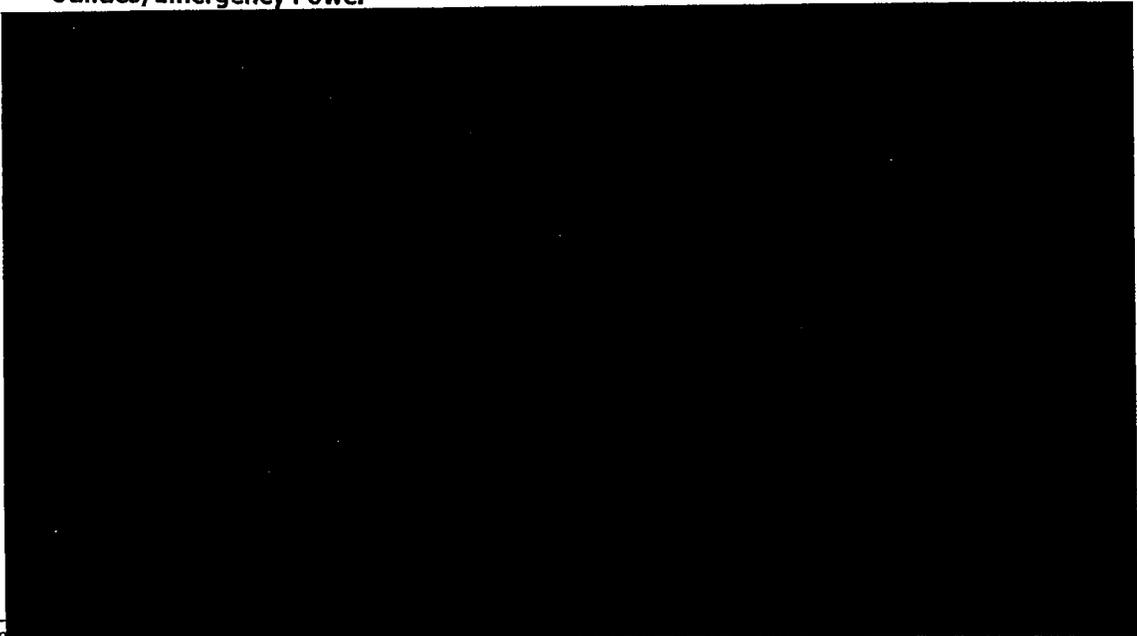
Recommendation #87

Develop and distribute for signature a Zero Tolerance Policy statement on the part of Massport, signed by the Massport Chief Executive Office and the Director of Public Safety.

Recommendation #88

Enhance Massport new hire orientation sessions with workplace violence zero tolerance and personal security awareness.

X. Utilities/Emergency Power



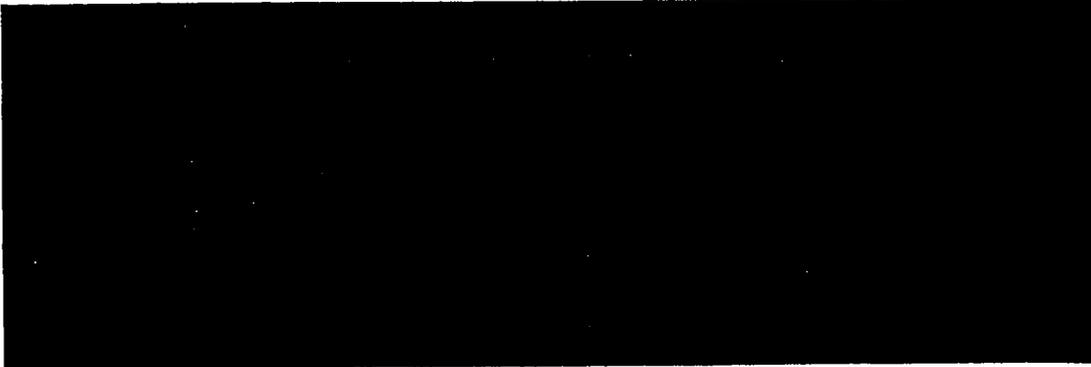
This document contains security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100693

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001



The preventative maintenance program is contracted to F&M Generators. F&M Generators representatives provide routine maintenance and respond as needed. Massport employees report that no problems have occurred with the current backup power system since its inception.

Recommendation #89



Recommendation #90



Y. Internal Security

Currently, Massport does not perform physical inventory inspections, periodically or otherwise, of office furniture, equipment and office conditions. According to the Manager, Support Services, the last physical inventory and inspection of all furniture and equipment at BOS was conducted in 1997 (approximately, could not recall a more exact date). This inventory did not include any IS equipment. The information was recorded electronically and each piece of equipment and furniture was labeled with a bar code sticker.

After the information was gathered and recorded, it was discovered that the program used to record the information was not Windows supported and therefore not compatible with the computer system at BOS. Consequently, the information does not exist, as it was not kept, except perhaps in hardcopy format. BOS has not conducted an inventory or inspection since. Although the Manager, Support Services has been addressing this issue, she has not yet been given direction to proceed with a full-scale physical inventory program.

BOS also does not perform inspections with regard to unsecured documents and open computer programs. Further, there does not exist a property control program regarding the inventory, tracking, auditing, and control of assets and information resources. Hence, high value or highly pilferable items are not protected. Indeed, the Manager, Support Services described an incident where a framed map, which was very old and considered a valuable asset, was discovered to be missing. Because BOS does not require property passes or the like, it was impossible to discover any information regarding the missing item.

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

An information resources protection program does not exist, a "clean desk" policy, clear documentation destruction policy, or other similar type safeguards to protect and preserve information sensitive to Massport and Massport personnel also do not exist.

IS does have an inventory program for all IS equipment. IS conducts their inventory following each budget cycle. Records are kept of newly issued equipment and outgoing equipment is compared to previously recorded inventory information. Smaller scale inventories are also conducted. This occurs when new IS equipment is installed in a section, then that section will be inventoried to ensure that all IS equipment is accounted for. The inventory information is kept on a database and the information is backed up on a disk.

Recommendation #91

Develop and establish a comprehensive asset protection program to include property removal procedures, i.e., property pass functions, recurrent property inventory and Massport property identification tagging.

Recommendation #92

Develop and implement a comprehensive information resources protection program to include document marking and destruction procedures, a "clean desk" policy, and the securing of electronic media such as personal computer terminals when such rooms are not occupied.

Z. Fire Safety

There are strategically placed fire extinguishers throughout the Airport. There are different types of fire extinguishers installed at BOS, ABC extinguishers and ASC dry chemical extinguishers. The communications room (Keybase) has a Halon system in place. All fire extinguishers are inspected on a quarterly basis. BOS has a fire extinguisher maintenance contract with Capital Fire. Under this maintenance contract, all fire extinguishers are serviced annually, or as needed.

BOS does have smoke detection devices installed throughout the Airport. Also, emergency lighting is in place and functions under zoned activation. BOS has a fire protection sprinkler system with cutoff valves and redundant water supply systems located throughout the airport. BOS does have a sprinkler system maintenance contract with Simplex, who provides inspection and maintenance as needed. BOS is divided into sections for the purposes of conducting fire drills, which are conducted annually per section, except for the Post Office, which conducts fire drills twice annually.

All fire drills are monitored by Massport Fire Department personnel. The last fire drill occurred in the old tower on October 30, 2001, with good results. All fire devices (strobe lights, sirens, etc.) functioned properly and personnel evacuated the area as required during the drill. CTI personnel participated in the drill and the only problems discovered included Fire Department personnel not ensuring that Massport employees responded to the appropriate pre-designated location. Also, and they did not notify the employees that the drill was over.

Lighted exit signs are in place throughout the Airport. The public address system is controlled from Keybase and is tested on a daily basis. Fire Department personnel and senior Massport personnel are authorized to order an evacuation. BOS is well equipped to handle handicapped visitors and employees during an evacuation or a fire emergency. Isle

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100695

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

chairs, stair chairs, backboards and other emergency equipment are available for use. Floor Wardens are responsible for guiding disabled employees during an emergency evacuation or a fire emergency.

Special fire and emergency training is available for Massport employees when requested. It is not clear at this time which employees receive and who makes that decision. Those employees that do receive training have the letters ER placed on their security badges to identify them as being trained. Initial and recurrent training is conducted by Fire Department personnel.

AA. Safety and Security Planning

Fire/rescue personnel have daily contact with local community fire officials ensuring pertinent information is passed as needed. Additionally, the State Police also communicate daily with the local and federal law enforcement departments on a regular and as needed basis.

Currently, Massport emergency personnel have at their disposal a number of written emergency response procedures, including:

- Mass Casualty Plan
- Family Support Center Plan
- Airport Emergency Plan
- Multiple Fatality Plan
- Air Craft Emergency Frequency Plan

Although Massport has a fully trained and available fire/rescue unit and law enforcement division, if additional emergency medical services and/or law enforcement services are required, support is readily available from various local, state and federal agencies. Each agency responsible for carrying out various duties during an emergency situation at BOS is listed in the AEP.

Fire rescue personnel check all first aid supplies on a monthly basis. The nearest hospital is Massachusetts General Hospital, which is approximately three miles away. Massachusetts General hospital, which actively participates in the Airport's full scale emergency exercise, is managed by Boston Central Medical, who, when necessary, will provide direction as to which secondary hospital(s) to use.

In the event of an emergency, the Airport will release a Tenant Advisory, signed by the Director of Aviation notifying all Airport personnel of the emergency events and any new permanent or temporary security or safety measures.

The Airport intercom system is controlled by keybase personnel and tested regularly. The intercom system can be used during an emergency, such as a fire alarm, or for routine verbal dissemination of operational advisories, such as public announcements that emphasize the need for all passengers to closely control baggage and packages. Visible prominent signage is also used in support of the public address system.

The Airport conducts annual tabletop exercises of its contingency plans with the participation of all air carriers and certain airport tenants. Only those tenants whose office space or operational facilities provide them with direct access to the AOA are allowed to participate.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

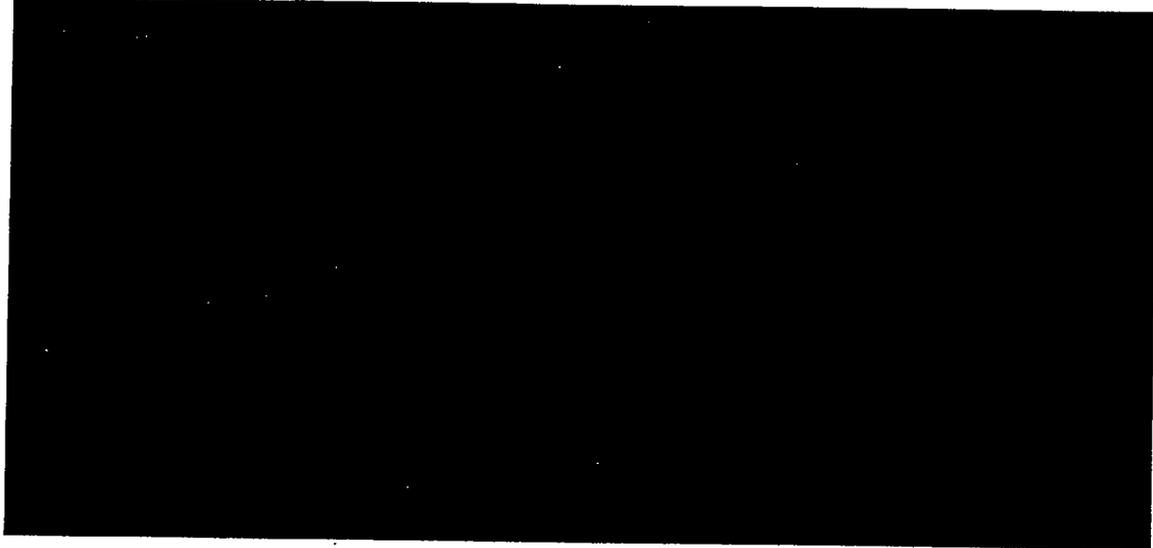
MP100696

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

BB. Intelligence Sharing



Recommendation #93

Ensure that at least two State Police representatives apply for and receive Top Secret clearances.

Recommendation #94

Identify a resource that can provide counter-terrorism guidance and support, specifically civil aviation security.

Recommendation #95

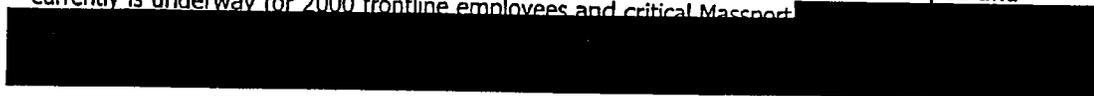
Initiate and foster relationships and communication lines with other security Category X Airport Security Coordinators (ASC).

Recommendation #96

Regularly participate and attend industry related security committee meetings and conferences.

CC. Training

Prior to September 11, security awareness training did not occur. Since September 11, and in direct response to federal mandates, an Airport wide security awareness was developed, established, and accomplished. Further, a counter-terrorism course has been developed and currently is underway for 2000 frontline employees and critical Massport



In addition, according to the AEP, employees are supposed to receive indoctrination training in reporting emergencies by unit managers to include the following:

- Location and proper use of available telephones nearest his/her normal place of activity
- Information to be identified when reporting an emergency
- Individual responsibilities in directing responding personnel to an emergency

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100697

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

- Availability of classes taught by the Massport Fire-Rescue Department. Employees are responsible for scheduling their own initial and recurrent training based on the Massport Fire-Rescue Department training schedule.



Recommendation #97

Massport should develop recurrent SIDA Awareness training for all BOS and tenant personnel.

Recommendation #98

Massport should develop and perform recurrent/annual airport-specific LEO training to include an intensive new-hire training program.

Subject to Confidentiality Protective Order
In re September 11 Litigation
21 MC 97 (AKH) (S.D.N.Y.) & 21 MC 101 (AKH) (S.D.N.Y.)
Do Not Copy or Disclose

FIRST DRAFT REPORT
"Physical Security Assessment:
Massachusetts Port Authority
Boston Logan International Airport"

November 6, 2001

VI. Conclusion

A major challenge facing Massport and BOS will be the understanding of why no action has apparently occurred on the many previous safety and security recommendations submitted from multiple sources, including its own Department of Public Safety. The basic premise is that Massport should build its Public Safety operating processes around its assigned Directors, Deputy Directors, staff, and outside resources, empowering the Department of Public Safety to develop plans to create and operate missions, providing them resources to succeed, and holding them accountable for the success and failure of these missions.

Although extremely limited in such critical resources, as manpower and formal training, the Massport Public Safety Department has worked exceedingly well at keeping its security program efficient and compliant with all applicable laws, rules and regulations despite the numerous hurdles continuously presented before them as described in this First Draft Report. This has been compounded by the events of September 11, 2001. Because of the events, and numerous other security related matters, the Department of Public Safety has received much more response and cooperation from Massport senior staff not previously experienced. Indeed, as confirmed by senior Massport staff, permanent and temporary, CTI readily discerned an obvious existence within Massport that has led to a split in authority and division of responsibility that has guaranteed inefficiency, encouraged rivalries, and disrupted communication.

Nevertheless, this First Draft Report, while comprehensive in nature, is not an exhaustive examination of all issues facing Massport today and in the future. Hence, CTI's recommendations focus on actions that must be taken as a matter of urgency for the very survival and success of Massport and BOS. CTI's principal conclusion is that BOS must address several systemic elements just to begin to prepare themselves to meet only minimum-security standards with regard to today's threats and risks. The principal recommendation is that Public Safety authority, responsibility, manpower and objectives must be clearly enhanced, delineated and expressed without ambiguity to all Massport entities in an effort to begin to bring BOS up to an acceptable and effective level of security as quickly as possible.

Indeed, implementation of many of the recommendations contained with this First Draft Report assumes and in most cases requires the availability of sufficient additional manpower, available time/schedule and funding. They also presume there will be no intervening Massport or City of Boston mandates, either on a local or state level, which tend to establish competing priorities not in keeping with Public Safety's immediate ability to respond.

CTI cannot yet offer an estimate of the resources required for each suggested recommendation or action, partly because it would depend not only on fully establishing the true existing conditions and anomalies at BOS beyond those identified in this First Draft Report, but also to the extent to which recommendations are implemented and accomplished. Indeed, retrofitting facilities and programs due to current and/or new safety and security demands can be extremely costly. To this end, available Federal funds must be aggressively sought out.

Finally, Massport must be commended for seeking outside assistance in assessing and supporting its security systems, a first step in upgrading its security program at BOS.

This document contains sensitive security information as it relates to Boston Logan International (BOS) Airport's security program, its systems, methods, and procedures. This document and the information contained herein is therefore controlled under the provisions of 14 CFR FAR Part 191, et al. No part of this document and the information contained herein may be released without the express written permission of the Associate Administrator for Civil Aviation Security, Federal Aviation Administration, Washington, DC 20591. Unauthorized release may result in civil penalty or other action. For US Government Agencies, public availability may be determined under 5 U.S.C. 552.

MP100699