



Homeland Security

July 31, 2008

Mr. David L. Sobel
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009

Re: **DHS/OS/PRIV 07-160/Sobel request**

Dear Mr. Sobel:

This is the fifteenth partial release to your Freedom of Information Act (FOIA) requests to the Department of Homeland Security (DHS), dated November 7, 2006 and December 6, 2006, requesting DHS records concerning the Automated Targeting System (ATS). These two requests were aggregated to simplify processing. The following is a consolidated list of records requested:

1. All Privacy Impact Assessments prepared for the ATS system or any predecessor system that served the same function but bore a different name.
2. A Memorandum of Understanding executed on or about March 9, 2005 between Customs and Border Protection (CBP) and the Canada Border Services Agency to facilitate the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information.
3. All records, including Privacy Act notices, which discuss or describe the use of personally-identifiable information by the CBP (or its predecessors) for purposes of screening air and sea travelers.
4. All System of Records Notices (SORNs) that discuss or describe targeting, screening, or assigning "risk assessments" of U.S. citizens by CBP or its predecessors.
5. All records that discuss or describe the redress that is available to individuals who believe that the ATS contains or utilizes inaccurate, incomplete or outdated information about them.
6. All records that discuss or describe the potential consequences that individuals might experience as a result of the agency's use of the ATS, including but not limited to arrest, physical searches, surveillance, denial of the opportunity to travel, and loss of employment opportunities.
7. All records that discuss or identify the number of individuals who have been arrested as a result of screening by the ATS and the offenses for which they were charged.
8. All complaints received from individuals concerning actions taken by the agency as a result of ATS "risk assessments" or other information contained in the ATS, and the agency's response to those complaints.
9. All records that discuss or describe Section 514 of the Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441) and its prohibition against the development or testing of "algorithms assigning risk to passengers whose names are not on Government watch lists."
10. All records that address any of the following issues:
 - a. Whether a system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights may appeal such decision and correct erroneous information contained in the ATS;

- b. Whether the underlying error rate of the government and private databases that will be used in the ATS to assign a risk level to an individual will not produce a large number of false positives that will result in a significant number of individuals being treated mistakenly or security resources being diverted;
- c. Whether the agency has stress-tested and demonstrated the efficacy and accuracy of all search tools in the ATS and has demonstrated that the ATS can make an accurate predictive assessment of those individuals who may constitute a threat;
- d. Whether the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which the ATS is being developed and prepared;
- e. Whether the agency has built in sufficient operational safeguards to reduce the opportunities for abuse;
- f. Whether substantial security measures are in place to protect the ATS from unauthorized access by hackers or other intruders;
- g. Whether the agency has adopted policies establishing effective oversight of the use and operation of the system;
- h. Whether there are no specific privacy concerns with the technological architecture of the system;
- i. Whether the agency has, pursuant to the requirements of section 44903(i)(2)(A) of Title 49, United States Code, modified the ATS with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger a high risk status; and
- j. Whether appropriate life-cycle estimates, expenditure and program plans exist.

A search directed to CBP has produced an additional 543 pages of records responsive to your request. We have determined that 535 pages are releasable to you in full or with certain information withheld pursuant to Exemptions 2(low) and (high), 5, 6, and 7 of the FOIA, and 8 pages are withheld in their entirety pursuant to Exemptions 2(low) and (high), 5, 6, and 7 of the FOIA.

Enclosed are 535 pages of releasable information. The withheld information, consists of names or initials, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, and 7E of the FOIA, 5 U.S.C. §§ 552 (b)(2), (b)(5), (b)(6), and (b)(7)(E).

Also enclosed is 1 blank sheet with several numbers that represent withheld documents. Each number corresponds to a page of withheld information and has the appropriate exemptions that apply to that document. In this instance, there are 8 pages of withheld information that comprise 1 document.

Exemption 2(low) exempts from disclosure records that are related to internal matters of a relatively trivial nature, such as internal administrative tracking. Exemption 2(high) protects information disclosure of which would risk the circumvention of a statute or agency regulation. Included within such information may be operating rules, guidelines, manuals of procedures for examiners or adjudicators, and homeland security information.

Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. It applies to facts divulged by a client to his attorney, and encompasses any

opinions given by an attorney to his client based upon, and thus reflecting, those facts, as well as communications between attorneys that reflect client-supplied information.

Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy.

Exemption 7E protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

As stated in the February 1, 2008 Status Report for the litigation which encompasses this FOIA request, we are continuing to process your request with regard to emails located at the following two CBP Offices: (1) Office of Field Operations, National Targeting and Security and (2) the Office of Chief Counsel. Consistent with the July 15, 2008 email correspondence between EFF and DOJ in this matter, the attached production includes a redacted version of the most recent, final version of the ATS-P User Guide corresponding to the current version of ATS-P, thereby completing the request with regard to the CBP Office of Information and Technology. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-160/Sobel request**. This office can be reached at 866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,



Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 536 pages

~~LAW ENFORCEMENT SENSITIVE~~

U. S. Customs and Border Protection

AUTOMATED TARGETING SYSTEM *PASSENGER*

Passenger Module



USER'S GUIDE AND REFERENCE MANUAL

*Revised Edition 2.3
Companion Edition to Software Version 4.6.0.28*

Office of Information and Technology

May 2007

~~LAW ENFORCEMENT SENSITIVE~~

003278

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

Disclosure Warning Statement

This document is provided as an education and referral guide for U.S. Customs and Border Protection personnel in the use of information technology to support official U.S. government business.

This document is the property of U.S. Customs and Border Protection and contains information about the operations of a U.S. Customs and Border Protection computer program that has an overall security classification of **LAW ENFORCEMENT SENSITIVE**.

This document and all data contained within are owned or controlled by U.S. Customs and Border Protection and may not be used for personal or unofficial use. Disclosure of any classified information found within this document is prohibited by law and may result in the assessment of criminal penalties.

~~LAW ENFORCEMENT SENSITIVE~~

003279

TABLE OF CONTENTS

CHAPTER ONE – GETTING STARTED..... 1

Introduction to this Guide 3

 Guide Layout.....3

 Presentation Conventions4

 Information Boxes 5

CHAPTER TWO – SECURITY..... 7

Overview 9

Responsibilities..... 9

Other Policies and Procedures 10

Application Rules..... 11

 Work at Home 11

 Dial-in Access..... 11

 Connection to the Internet..... 11

 Protection of Copyright Licenses (Software)..... 12

 Unofficial Use of Government Equipment..... 12

 Use of Passwords 14

 Passwords and Other Access Control Measures 15

 System Privileges..... 15

 System Access 15

 Individual Accountability 15

 Restoration of Service..... 16

 Data Protection..... 16

 Laptop Computers and Portable Electronic Devices (PEDs)..... 16

 Tips for Traveling with a Laptop or PED..... 16

 Incident Reporting 17

 Contact Information to Report Security Incidents 18

Additional ATS Security Information..... 19

Accessing ATS Data 19

ATS-P (Passenger) Access Requirements 19

Requesting Access to ATS-P (Passenger) 20

User Roles and Privileges for the Passenger Module 20

CHAPTER THREE – OVERVIEW..... 21

What is ATS? 23

What is the ATS-P (Passenger) Module? 24

 ATS-P (Passenger) Data Sources 25

ATS-P (Passenger) Points of Contact 26

ATS Computer Configuration Requirements..... 27

 Computer Hardware Recommendations..... 27

 Screen Resolution for Viewing ATS-P (Passenger) 27

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

The Microsoft Internet Explorer	27
Internet Explorer Toolbar Icons	27
Full Screen Mode	28
Auto-Hide Your Internet Explorer Toolbar	29
Internet Explorer Security Settings	30
How to Modify Your Internet Explorer Security Settings	30
Configuring Your Proxy Server Settings	32
How to Configure Your Internet Explorer Proxy Settings	33
Cookies	34
How to Set up Your Computer to Accept Cookies	34
Displaying the Latest Internet Explorer Page	35
How to Display Only the Latest Version of a Web Page	35
Accessing ATS-P (Passenger)	37
Accessing ATS-P (Passenger) from Your Desktop	37
Accessing ATS-P (Passenger) from CBPnet	38
The ATS Logon Screen	41
Related Information	41
Logging on to ATS-P (Passenger)	42
Field Descriptions for the ATS Logon Screen	42
First Time Logon to ATS-P	43
Changing Your ATS Password	44
How to Change Your ATS Password	44
Related Information	45
Working with ATS-P (Passenger) Screens	46
Logging off from ATS-P (Passenger)	46
CHAPTER FOUR – LEARNING ABOUT ATS-P	48
Overview	50
The Start Page	51
High (b)(2), Low (b)(2), (b)(7)(E)	53
.....	53
.....	53
Start Page	54
.....	55
.....	55
.....	57
.....	57
.....	58
.....	59
.....	59
.....	62
.....	62
.....	62
Reference Section	63
Reference Section Links	63
High (b)(2), Low (b)(2), (b)(7)(E)	64
.....	64
.....	64
.....	65
.....	66
The Home Option	68
Overview	68
Web Page Features	68

ATS-P (Passenger)

Printing the Current Screen Display	69
Downloading as a Word file	69
High (b)(2), Low (b)(2), (b)(7)(E)	70
[REDACTED]	71
[REDACTED]	71
[REDACTED]	72
[REDACTED]	72
[REDACTED]	72
[REDACTED]	74
[REDACTED]	74
[REDACTED]	74
[REDACTED]	75
[REDACTED]	76
[REDACTED]	76
[REDACTED]	77
[REDACTED]	77
Start Page Tab	79
Field Descriptions for the Change Personal Preferences (Start Page Tab) Screen	79
Button Descriptions for the Change Personal Preferences (Start Page Tab) Screen	80
How to Set Your Start Page Preferences	80
The Links Option	81
Overview	81
Internal Links	81
[REDACTED]	81
The Help Option	82
Overview	82
Online Help Topics	82
The Contents Tab	83
The Index Tab	84
The Search Tab	85
Online User's Guide	86
About ATS	87
CHAPTER FIVE –THE ATS-P (PASSENGER) USER'S GUIDE	89
Logging on to ATS-P (Passenger) for the First Time	91
Working with News Items	94
Creating a National or Local News Item from the Start Page	94
Creating a National or Local News Item from the Create Option	95
Browsing ATS-P Databases	97
Browsing an ATS-P Database	97
Running a Special Operation	99
[REDACTED]	100
[REDACTED]	100
[REDACTED]	103
[REDACTED]	105
[REDACTED]	105
[REDACTED]	107
[REDACTED]	109
[REDACTED]	111
[REDACTED]	113
[REDACTED]	115
[REDACTED]	117

ATS-P (Passenger)

High (b)(2), Low (b)(2), (b)(7)(E)	118
.....	120
.....	120
.....	121
.....	123
.....	126
.....	126
.....	126
.....	128
.....	132
.....	133
.....	135
.....	136
.....	137
.....	140
.....	140
.....	142
.....	142
.....	143
.....	143
.....	144
.....	146
.....	148
.....	150

CHAPTER SIX – THE ATS-P (PASSENGER) REFERENCE MANUAL 154

Overview	156
.....	157
Start Page Features	158
.....	158
.....	159
.....	159
.....	160
.....	161
.....	161
.....	163
.....	163
.....	163
Related Information	163
.....	164
.....	166
.....	167
.....	167
.....	168
.....	168
.....	169
.....	170
.....	170
.....	171
.....	172

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

High (b)(2), (b)(7)(E), Low (b)(2)	173
[REDACTED]	173
[REDACTED]	174
[REDACTED]	175
[REDACTED]	176
Overview	176
[REDACTED]	177
[REDACTED]	177
[REDACTED]	178
[REDACTED]	179
[REDACTED]	179
[REDACTED]	180
[REDACTED]	181
[REDACTED]	181
[REDACTED]	182
[REDACTED]	182
[REDACTED]	183
[REDACTED]	184
[REDACTED]	185
[REDACTED]	185
[REDACTED]	186
[REDACTED]	186
[REDACTED]	187
[REDACTED]	188
[REDACTED]	188
[REDACTED]	188
[REDACTED]	189
[REDACTED]	190
[REDACTED]	191
[REDACTED]	192
[REDACTED]	192
[REDACTED]	193
[REDACTED]	194
[REDACTED]	195
[REDACTED]	196
[REDACTED]	196
[REDACTED]	197
[REDACTED]	198
[REDACTED]	199
[REDACTED]	201
[REDACTED]	201
[REDACTED]	202
[REDACTED]	202
[REDACTED]	204
[REDACTED]	205
[REDACTED]	206
[REDACTED]	208
[REDACTED]	208
[REDACTED]	209
[REDACTED]	210

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

High (b)(2), Low (b)(2), (b)(7)(E)	211
[REDACTED]	212
[REDACTED]	212
[REDACTED]	213
[REDACTED]	213
[REDACTED]	214
[REDACTED]	215
[REDACTED]	215
[REDACTED]	216
[REDACTED]	216
[REDACTED]	217
[REDACTED]	218
[REDACTED]	218
[REDACTED]	219
[REDACTED]	220
[REDACTED]	220
[REDACTED]	221
[REDACTED]	221
[REDACTED]	223
[REDACTED]	223
[REDACTED]	224
[REDACTED]	224
[REDACTED]	225
[REDACTED]	226
[REDACTED]	226
[REDACTED]	227
[REDACTED]	227
[REDACTED]	228
[REDACTED]	229
[REDACTED]	230
[REDACTED]	230
[REDACTED]	231
[REDACTED]	232
[REDACTED]	232
[REDACTED]	234
[REDACTED]	235
[REDACTED]	235
[REDACTED]	236
[REDACTED]	237
[REDACTED]	237
[REDACTED]	239
[REDACTED]	240
[REDACTED]	240
[REDACTED]	241
[REDACTED]	242
[REDACTED]	242
[REDACTED]	243
[REDACTED]	244
[REDACTED]	244
[REDACTED]	244

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

High (b)(2), (b)(7)(E), Low (b)(2)	244
[REDACTED]	245
[REDACTED]	246
[REDACTED]	247
[REDACTED]	247
[REDACTED]	248
[REDACTED]	249
[REDACTED]	249
[REDACTED]	251
[REDACTED]	251
[REDACTED]	252
[REDACTED]	253
[REDACTED]	253
[REDACTED]	254
[REDACTED]	254
[REDACTED]	256
[REDACTED]	256
[REDACTED]	257
[REDACTED]	257
[REDACTED]	258
[REDACTED]	258
[REDACTED]	259
[REDACTED]	259
[REDACTED]	261
[REDACTED]	261
[REDACTED]	261
[REDACTED]	262
[REDACTED]	262
[REDACTED]	264
[REDACTED]	264
[REDACTED]	265
[REDACTED]	266
[REDACTED]	266
[REDACTED]	268
[REDACTED]	268
[REDACTED]	268
[REDACTED]	269
[REDACTED]	270
[REDACTED]	271
[REDACTED]	271
[REDACTED]	271
[REDACTED]	272
[REDACTED]	273
[REDACTED]	275
[REDACTED]	275
[REDACTED]	276
[REDACTED]	277
[REDACTED]	277
[REDACTED]	278
[REDACTED]	278
[REDACTED]	279
[REDACTED]	279

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

High (b)(2), (b)(7)(E), Low (b)(2)	279
[REDACTED]	281
[REDACTED]	281
[REDACTED]	282
[REDACTED]	283
[REDACTED]	283
[REDACTED]	283
[REDACTED]	284
[REDACTED]	285
[REDACTED]	285
[REDACTED]	285
[REDACTED]	286
[REDACTED]	287
[REDACTED]	287
[REDACTED]	287
[REDACTED]	289
[REDACTED]	290
[REDACTED]	290
[REDACTED]	292
[REDACTED]	292
[REDACTED]	292
[REDACTED]	294
[REDACTED]	294
[REDACTED]	295
[REDACTED]	296
[REDACTED]	297
[REDACTED]	297
[REDACTED]	299
[REDACTED]	299
[REDACTED]	299
[REDACTED]	300
[REDACTED]	301
[REDACTED]	301
[REDACTED]	302
[REDACTED]	303
[REDACTED]	303
[REDACTED]	304
[REDACTED]	305
[REDACTED]	306
[REDACTED]	306
[REDACTED]	307
[REDACTED]	309
[REDACTED]	309
[REDACTED]	310
[REDACTED]	312
[REDACTED]	313
[REDACTED]	314
[REDACTED]	315
[REDACTED]	315
[REDACTED]	315
[REDACTED]	316
[REDACTED]	318
[REDACTED]	318
[REDACTED]	319
[REDACTED]	320
[REDACTED]	320

ATS-P (Passenger)

High (b)(2), (b)(7)(E), Low (b)(2)	321
[REDACTED]	321
[REDACTED]	322
[REDACTED]	322
[REDACTED]	322
[REDACTED]	324
[REDACTED]	324
[REDACTED]	325
[REDACTED]	327
[REDACTED]	327
[REDACTED]	327
[REDACTED]	328
[REDACTED]	329
[REDACTED]	329
[REDACTED]	331
[REDACTED]	331
[REDACTED]	332
[REDACTED]	333
[REDACTED]	333
[REDACTED]	334
[REDACTED]	335
[REDACTED]	336
[REDACTED]	336
[REDACTED]	337
[REDACTED]	338
[REDACTED]	338
[REDACTED]	339
[REDACTED]	340
[REDACTED]	340
[REDACTED]	341
[REDACTED]	342
[REDACTED]	342
[REDACTED]	343
[REDACTED]	345
[REDACTED]	345
[REDACTED]	346
[REDACTED]	347
[REDACTED]	347
[REDACTED]	348
[REDACTED]	349
[REDACTED]	350
[REDACTED]	350
[REDACTED]	351
[REDACTED]	352
[REDACTED]	353
[REDACTED]	354
[REDACTED]	356
[REDACTED]	356
[REDACTED]	357
[REDACTED]	358
[REDACTED]	358
[REDACTED]	359
[REDACTED]	360
[REDACTED]	360
[REDACTED]	360
[REDACTED]	361

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

High (b)(2), (b)(7)(E), Low (b)(2)	362
[REDACTED]	362
[REDACTED]	362
[REDACTED]	364
[REDACTED]	364
[REDACTED]	365
[REDACTED]	366
[REDACTED]	366
[REDACTED]	367
[REDACTED]	369
[REDACTED]	369
[REDACTED]	369
[REDACTED]	371
[REDACTED]	371
[REDACTED]	372
[REDACTED]	373
[REDACTED]	373
[REDACTED]	374
[REDACTED]	375
[REDACTED]	376
[REDACTED]	376
[REDACTED]	377
[REDACTED]	378
[REDACTED]	378
[REDACTED]	378
[REDACTED]	379
[REDACTED]	379
[REDACTED]	379
[REDACTED]	381
[REDACTED]	381
[REDACTED]	382
[REDACTED]	383
[REDACTED]	383
[REDACTED]	385
[REDACTED]	386
[REDACTED]	386
[REDACTED]	387
[REDACTED]	388
[REDACTED]	388
[REDACTED]	389
[REDACTED]	389
[REDACTED]	389
[REDACTED]	391
[REDACTED]	391
[REDACTED]	391
[REDACTED]	393
[REDACTED]	393
[REDACTED]	394
[REDACTED]	394
[REDACTED]	395
[REDACTED]	396
[REDACTED]	397
[REDACTED]	397
[REDACTED]	398

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

High (b)(2), (b)(7)(E), Low (b)(2)	398
[REDACTED]	399
[REDACTED]	400
[REDACTED]	400
[REDACTED]	401
[REDACTED]	402
[REDACTED]	402
[REDACTED]	403
[REDACTED]	404
[REDACTED]	404
[REDACTED]	405
[REDACTED]	406
[REDACTED]	406
[REDACTED]	406
[REDACTED]	407
[REDACTED]	407
[REDACTED]	408
[REDACTED]	409
[REDACTED]	409
[REDACTED]	409
[REDACTED]	411
[REDACTED]	412
[REDACTED]	413
[REDACTED]	413
[REDACTED]	413
[REDACTED]	414
[REDACTED]	414
[REDACTED]	415
[REDACTED]	416
[REDACTED]	417
[REDACTED]	417
[REDACTED]	418
[REDACTED]	419
[REDACTED]	419
[REDACTED]	420
[REDACTED]	420
[REDACTED]	420
[REDACTED]	421
[REDACTED]	422
[REDACTED]	423
[REDACTED]	424
[REDACTED]	424
[REDACTED]	425
[REDACTED]	426
[REDACTED]	427
[REDACTED]	427
[REDACTED]	428
[REDACTED]	429
[REDACTED]	429
[REDACTED]	430
[REDACTED]	430

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

High (b)(2), Low (b)(2), (b)(7)(E)	432
[REDACTED]	432
[REDACTED]	432
[REDACTED]	434
[REDACTED]	434
[REDACTED]	434
[REDACTED]	435
[REDACTED]	436
[REDACTED]	437
[REDACTED]	438
[REDACTED]	438
[REDACTED]	438
[REDACTED]	439
[REDACTED]	439
[REDACTED]	440
[REDACTED]	441
[REDACTED]	441
[REDACTED]	442
[REDACTED]	443
[REDACTED]	443
[REDACTED]	445
[REDACTED]	445
[REDACTED]	445
[REDACTED]	446
[REDACTED]	446
[REDACTED]	447
[REDACTED]	448
[REDACTED]	448
[REDACTED]	449
[REDACTED]	450
[REDACTED]	450
[REDACTED]	451
[REDACTED]	452
[REDACTED]	452
[REDACTED]	452
[REDACTED]	452
[REDACTED]	453
[REDACTED]	453
[REDACTED]	453
[REDACTED]	456
[REDACTED]	456
[REDACTED]	456
APPENDIX A	460
[REDACTED]	460
Search Operators	461
APPENDIX B	463
[REDACTED]	463
[REDACTED]	464

ATS-P (Passenger)

High (b)(2), Low (b)(2), (b)(7)(E)	465
.....	466
.....	467
.....	468
.....	469
.....	470
.....	471
.....	472
.....	476
Visa Type Codes	477

APPENDIX C 480

Breakdown of Countries By Country Group Region.....	480
Africa Proper Region	480
Australia and Oceania Region	480
Caribbean Countries Region	481
Caribbean and Jamaica Region	482
Central America Region	482
Central America and Columbia Region.....	483
CO, JM, MX, OR, UK, VE, and WA Region	483
Composite View Region	484
East Asia / Orient Region.....	486
Eastern Europe Region.....	486
Iraq and Middle East Region	487
Jamaica, Caribbean, and West Africa Region	487
Nigeria and West Africa Region	488
North America Region	489
Russia, et al. Region	489
South America Only Region.....	490
South America – Includes CO and VE Region	490
Southwest Asian Region	490
Western Europe Region	491

GLOSSARY 492

INDEX 500

ATS-P (Passenger) User's Guide Comments	514
---	-----

CHAPTER ONE – GETTING STARTED

This chapter will review the following:

- An introduction to this guide
- An overview of the chapter layout
- Text presentation conventions
- Information boxes

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

Chapter One – Getting Started

This Page Left Blank.

~~LAW ENFORCEMENT SENSITIVE~~

003294

CHAPTER ONE – GETTING STARTED



Welcome to the Automated Targeting System

Introduction to this Guide

Guide Layout

This guide is divided into chapters that address different aspects of using the **Automated Targeting System - Passenger (ATS-P)** program's **Passenger** module. Within each chapter, functions and tasks are presented in menu or logical processing order, not alphabetical order. Below is the layout of the chapters and appendixes that make up this guide.

- **Chapter One** provides overview information for this User's Guide and the text conventions used within it.
- **Chapter Two** reviews the security issues and requirements for ATS-P (Passenger), which is classified as **LAW ENFORCEMENT SENSITIVE**.
- **Chapter Three** gives you an overview of the ATS-P program and the Passenger module. This chapter also includes procedures for logging on to and off from the program.
- **Chapter Four** begins the review of the ATS-P program. The chapter is a review of the **ATS Logon** screen, the **Start Page**, and the features found organized under the **Home** and **Help** options.
- **Chapter Five** contains the *ATS-P (Passenger) User's Guide*, which gives you step-by-step instructions on using ATS-P (Passenger).
- **Chapter Six** is the *ATS-P (Passenger) Reference Manual*, which provides a screen-by-screen review of ATS-P (Passenger).
- **Appendixes** provide you with data tables listing the valid values and codes used.
- A **Glossary** of common terms.
- An **Index** of ATS-P (Passenger) subjects, in alphabetical order, and their page numbers.
- Information on ordering additional ATS-P (Passenger) User's Guides.
- A **Comments Form** to allow you to provide feedback for changes to this guide.

Presentation Conventions

In the course of reviewing data input for the ATS-P (Passenger) program, the conventions below will be used to indicate different types of data used in this guide.

Underlined text

- Indicates that the text's importance is being emphasized.
Example: Use a screen resolution of 1024 by 768 pixels.

Bold Text

- Indicates that the name of a screen or selection is being referred to.
Example: Click the **Home** option.
Example: Click **Change Password**.

Italicized Bold Text

- Indicates that a field is being referred to.
Example: Record the ***Flight Number***.
Example: Type the ***Last Name***.

"Bold Text in Quotes"

- Indicates that a literal data value is being referred to.
Example: Type **"[REDACTED]"** the **Search** field.
Example: Check the list for the name **"Low (b)(2), (b)(7)(E)"**

[BOLD CAPITAL TEXT IN BRACKETS]

- Indicates that a keyboard key is being referred to.
Example: Press the **[ENTER]** key.
Example: Hold down the **[SHIFT]+[TAB]** keys.

<Field Titles in Angle Brackets>

- Indicates that the title is dynamic, that is, it will display a value depending on a previous selection or action.
Example: **<Specific Entity>**.
Example: **<Entity / HTS>**.

(Text in Parentheses)

- Indicates supplemental information to the displayed text.

Example: High (b)(2), (b)(7)(E) LE, Low (b)(2)

Example: Sensitive But Unclassified (or greater) data.

- Indicates the introduction of an acronym.

Example: Automated Targeting System (ATS).

Information Boxes

NOTE

Shaded boxes entitled NOTE are provided to let you know when there is information or processes that you should keep in mind when using ATS-P (Passenger). These boxes can also contain cautionary information to remember when performing a task.

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

Chapter One – Getting Started

This Page Left Blank.

~~LAW ENFORCEMENT SENSITIVE~~

003298

CHAPTER TWO – SECURITY

This chapter will review the following:

- An overview of security and user responsibilities
- Computer security policy and procedures
- Working at home
- Dial-in access
- Connection to the Internet
- Protection of software copyright licenses
- Unofficial use of government equipment
- Use of passwords
- System privileges
- Individual accountability
- Data protection
- Laptops and PEDs
- Incident reporting
- Accessing ATS data
- ATS-P (Passenger) Access Requirements
- Requesting access to ATS-P (Passenger)
- ATS-P (Passenger) user roles and privileges

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

Chapter Two – Security

This Page Left Blank.

~~LAW ENFORCEMENT SENSITIVE~~

003300

CHAPTER TWO – SECURITY

Overview

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines are established to hold users accountable for their actions and responsible for Information Technology (IT) security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. OMB Circular A-130 requires that all major applications and general support systems have Rules of Behavior.

All users of the Dept. of Homeland Security / U.S. Customs and Border Protection (DHS / CBP) IT systems shall be trained on the Rules of Behavior for the systems to which they are granted access before receiving access. All users shall sign a statement acknowledging that they have received and understand the training.

Any failure to comply with the Rules of Behavior shall be considered a security incident. If the incident is deemed willful, it will be escalated to a security violation. Noncompliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation. Depending on the number of security violations and the sensitivity of the information involved, disciplinary actions for such violations may consist of a letter or warning/caution, a suspension, or removal from Federal service.

Responsibilities

Organizational Elements shall establish Rules of Behavior for each general support system and major application. Information Systems Security Officers (ISSOs) shall ensure that all users receive training concerning the Rules of Behavior and sign a statement acknowledging receipt of the Rules of Behavior. This statement may be filed in either the employee's official personnel file (OPF) or in the employee's personnel file (EPE) maintained by the office.

The ISSO for each system is responsible for ensuring the system has an adequate level of protection, through an appropriate mix of technical, administrative, and managerial controls. The ISSO develops policies and procedures, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot-checks to determine that an adequate level of compliance with security requirements exists. The ISSO is responsible for periodically conducting vulnerability analyses to help determine if security controls are adequate. Special attention will be given to those new and developing

technologies, systems, and applications that may result in vulnerabilities in DHS/CBP's security posture.

Users are responsible for following system procedures to minimize security threats. Managers will conduct periodic reviews to ascertain that users are operating systems in a secure manner.

Other Policies and Procedures

The rules are not to be used in place of existing policy. They are intended to enhance and further define the specific rules each user must follow while accessing major applications. Specific rules of behavior are available in documentation, guides, and directives associated with individual applications.

A letter for non-DHS / CBP users shall be provided to all non-DHS / CBP users who will use major applications or general support systems. The letter shall transmit the applicable DHS / CBP policies and user responsibilities while using DHS / CBP systems.

User responsibilities shall be included in the computer security training DHS / CBP provides for users and agency security points of contact. Interagency agreements or other formal agreements or documents between DHS and other organizations shall present DHS / CBP policies and user responsibilities pertaining to use of DHS / CBP systems.

Application Rules

Work at Home

Division Directors may designate employees in specific categories (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home.

Any work-at-home agreement should:

- Be in writing.
- Identify the time period the work at home will be allowed.
- Identify what government equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for.
- Identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization and the ISSO).
- Be reviewed by the DHS/CBP human resources office prior to commencement.
- Employees approved for telecommuting must adhere to the following rules of behavior:
- At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.
- I will physically protect any laptops or Personal Electronic Devices (PEDs) I use for telecommuting when they are not in use.
- I will protect sensitive data at my alternate workplace. This includes properly disposing of sensitive information (e.g., by shredding).

Dial-in Access

No dial-in access will be used to access DHS / CBP applications or general support systems, unless authorized in writing by the employee's ISSO or Designated Accrediting Authority (DAA). If dial-in access is allowed, the ISSO will regularly review telecommunications logs and DHS / CBP phone records and will conduct spot-checks to determine if users are complying with controls placed on the use of dial-in lines.

Connection to the Internet

Most DHS / CBP personnel have access to the Internet. User identification and authentication shall be required for access to systems and data. ISSOs should carefully document all external connections to ensure access to major applications is limited to controlled points of entry. Only DHS-authorized Internet connections will be allowed, and all connections must conform to DHS's security and communications

architecture.

- I understand that my Internet and e-mail use is for official use, with limited personal use allowed. Allowed personal use is described in DHS MD 4500 (DHS E-Mail Usage) and DHS MD 4400.1 (DHS Web and Information Systems). CBP HB 1400-05B, Section 6.8 (Email) and Appendix M (Internet Access) apply specifically to CBP.
- I understand that my Internet and e-mail use may be monitored, and I consent to this monitoring.

Protection of Copyright Licenses (Software)

DHS / CBP personnel and contractors shall comply with all copyright licenses associated with major applications, general support systems, or commercial off-the-shelf (COTS) software. End users, supervisors, and functional managers are ultimately responsible for this compliance. LAN and PC users shall not download LAN-resident software. Audit logs will be reviewed to determine whether employees attempt to access LAN servers to which users have not been granted access. Audit logs will also show users' use of a "copy" command, which may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited.

- I agree to comply with all software copyrights and licenses.
- I will not install unauthorized software (this includes software available for downloading from the Internet, software available on DHS / CBP networks, and personally owned software) on DHS / CBP equipment (e.g., DHS / CBP workstations, laptop computers, PEDs).

Unofficial Use of Government Equipment

Users should be aware that personal use of DHS / CBP information resources, applications, networks, LANS, and PCs is normally not authorized. However, under certain conditions, limited personal use of government office equipment, including information technology resources, is authorized. Specific direction for personal use is provided in DHS MD 4600.1, *Personal Use of Government Office Equipment* and limited personal use policy for CBP employees and vendor support use of CBP-owned office equipment in accordance with U.S. Customs Directive 5230-031, *Limited Personal Use of Government Office Equipment Including Information Technology, January 19, 2001*.

CBP authorizes "limited personal use" of government-owned systems in accordance with the following guidelines (U.S. Customs Directive 5230-031):

1. Intermingling of government and personally owned computing systems is prohibited. Employees are permitted to use a government system in its current configuration only.
2. All employees and vendor personnel who take advantage of this practice imply their consent to

monitoring, recording and disclosing, with or without cause, the contents of any files or information maintained or passed through government office equipment such as their computer, Internet, Intranet, bulletin boards and/or e-mail

3. Inappropriate personal use of government office equipment includes the following:
- Modifying equipment, including loading personal software or making configuration changes to accomplish work.
 - Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound, or other large file attachments can degrade the performance of the entire network.
 - Using government systems as a staging ground or platform to gain unauthorized access to other systems.
 - The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
 - Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public, e.g., hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.
 - The creation, download, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials and materials related to illegal gambling, illegal weapons, terrorist activities and any other illegal activities or activities otherwise prohibited.
 - Use for commercial purposes or in support of "for-profit" activities or in support of their outside employment or business activity, e.g., consulting for pay, sales or administration of business transactions, sale of goods or services.
 - Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity prohibited by the Hatch Act.
 - Use for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a government employee or representing the government as a vendor.
 - Any use that could generate more than minimal additional expense to the government.
 - The unauthorized acquisition, use, reproduction, transmission or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data or export controlled software or data.
 - If accessing non-CBP mail systems, do not open attachments. Opening attachments in a non-CBP mail system presents a security risk of introducing viruses, Trojans, or other malicious code into the CBP network.

- Users' official email addresses may be used only for official CBP business communications and not to sign up or register for unapproved mailings or services.
- I will comply with DHS / CBP policy regarding personal use of DHS / CBP office equipment. I understand that DHS / CBP office equipment is to be used for official use, with only limited personal use allowed. Personal use of government office equipment is described in DHS Management Directive (MD) 4600 (Personal Use of Government Office Equipment) and U.S. Customs Directive 5230-031, (Limited Personal Use Of Government Office Equipment Including Information Technology).
- I understand that my use of DHS / CBP office equipment may be monitored, and I consent to this monitoring.

Use of Passwords

Users shall follow DHS / CBP password management rules, as presented in the DHS Sensitive Systems Handbook and CBP Security Policy and Procedures Handbook. Users shall keep passwords confidential and not share passwords with anyone.

- CBP passwords must be 6-8 alphanumeric characters with the first character a numeric. For systems that require User-ID and password access controls, ensure the User-Ids and passwords conform to the requirements of the specific operating system or application.
- Protect your User-ID and password.
- Passwords will not be shared with anyone else. Use of another individual's password is prohibited. Do not allow anyone to access information through your computer once you have logged on using your password.
- Change your password immediately, if you suspect it has been compromised.
- Choose hard-to-guess but easy-to-remember passwords.
- Passwords should not be written down.
- Change your passwords at least every 90 days.
- Inform your system administrator if you are leaving your work area for more than 60 days so that all your access may be suspended.
- Passwords will not be included in programs or scripts.
- Password-protect all files containing any data needing special handling or protection.
- Passwords should be memorized and never shared or written down. If you suspect your password has been compromised contact your ISSO immediately.
- Avoid common words found in a dictionary and things personally associated with you (e.g., user's name, child's name, pet's name, favorite sports team, etc.).

Passwords and Other Access Control Measures

- **Low (b)(2), High (b)(2), (b)(7)(E) LE**
[REDACTED]
- I will protect passwords and access numbers from disclosure. I will not record passwords or access control numbers on paper or in electronic form and store them on or with DHS workstations, laptop computers, or PEDs. To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view as I enter my password.
- I will not store smart cards on or with DHS workstations, laptop computers, or PEDs.
- I will promptly change a password whenever the compromise of that password is known or suspected.
- I will not attempt to bypass access control measures.

System Privileges

Users are given access to major applications or general support systems based on a need to perform specific work. Users shall work within the confines of the access allowed and shall not attempt access to systems or applications to which access has not been authorized.

System Access

- I understand that I am given access to only those systems for which I require access to perform my official duties.
- I will not attempt to access systems I am not authorized to access.

Individual Accountability

Users will be held accountable for their actions on all DHS / CBP applications and systems. This accountability shall be stressed during computer security awareness training sessions.

- I understand that I have no expectation of privacy while using any DHS / CBP equipment and while using DHS / CBP Internet or e-mail services.
- I understand that I will be held accountable for my actions while accessing and using DHS / CBP systems and IT resources.

All users are individually responsible for ensuring that C-TPAT sensitive and proprietary materials are safeguarded in accordance with CIS HB 1400-05B. ATS sensitive materials must not be left unattended and will be secured under lock and key.

Users will ensure that when sensitive C-TPAT information is distributed it is packaged in a way that does not disclose its contents and is sent via the U.S. Postal Service, APO, commercial messenger, or unclassified registered pouch.

Restoration of Service

The availability of DHS / CBP systems and applications is a concern to all users. All users are responsible for facilitating the restoration of services in the event a major application or general support system is not operational.

Data Protection

All DHS / CBP users are responsible for proper handling and protection of hardware and media (hard and softcopy) used when accessing DHS / CBP systems.

- I will use only DHS / CBP office equipment (e.g., workstations, laptops, PEDs) to access DHS / CBP systems and information; I will not use personally owned equipment.
- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I step away from my work area, even for a short time; I will log off when I leave for the day.
- I will not access, process, or store classified information on DHS / CBP office equipment that has not been authorized for such processing.

Laptop Computers and Portable Electronic Devices (PEDs)

Rules of behavior that specifically apply to DHS / CBP laptop computers and portable electronic devices (PEDs) are listed below.

- I will use only DHS / CBP laptops or PEDs to access DHS / CBP systems and information.
- I will keep the laptop or PED under my physical control at all times, or I will secure it in a suitable locked container under my control.

Tips for Traveling with a Laptop or PED

- Keep the laptop or PED under your physical control at all times.
- At airport security, place the laptop or PED on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on the laptop

or PED until you can pick it up.

- Do not place the laptop or PED in checked luggage.
- Do not store the laptop or PED in an airport, a train or bus station, or any public locker.
- If you must leave a laptop or PED in a car, lock it in the trunk so that it is out of sight.
- Avoid leaving the laptop or PED in a hotel room. If you must leave it in a hotel room, lock it inside another piece of luggage.
- I will take all necessary precautions to protect the laptop / PED against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and removable media drives.
- I will keep anti-virus and firewall software on the laptop up to date.
- I will use only DHS / CBP-authorized Internet connections that conform to DHS / CBP security and communications standards.
- I will not make any changes to a laptop's system configuration unless I am directed to do so by a DHS / CBP system administrator.
- I will not program the laptop with sign-on sequences, passwords, or access phone numbers.
- I understand and will comply with the requirement that sensitive information stored on any laptop computer used in a residence or on travel shall be encrypted using FIPS 140-1- or FIPS 140-2- approved encryption.
- I understand and will comply with the requirement that sensitive information processed, stored, or transmitted on wireless devices must be encrypted using approved encryption methods.
- Users shall transmit data using web-enabled laptops or PEDs that rely on wireless access protocol (WAP) and / or use commercial wireless network providers only if data is encrypted end-to-end using a FIPS-validated crypto module.
- Users shall not use laptops or PEDs containing audio, video, or photographic recording and/or transmission capabilities in areas where DHS/CBP protected information is processed or discussed.
- Users will obtain written permission from the Targeting and Screening Program Office (TASPO) Director/Deputy or their designee before deploying with a CBP laptop overseas.
- Users shall not use laptops / PEDs to process classified information unless the equipment is certified by the Designated Accrediting Authority (DAA) for classified processing.

Incident Reporting

The following section is replicated from U.S. Customs and Border Protection (CBP) Security Policy and Procedures Handbook, February 7, 2005, CIS HB 1400-05B.

CBP established a formal Computer Security Incident Response Center (CSIRC) organization. CSIRC

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

Chapter Two – Security

charter provides detection and preliminary investigation of all known or suspected security violations posing a threat to CBP. These threats could be from either internal or external sources. All incidents of misuse of CBP systems must be reported to the CSIRC. NIST Special Publication SP 800-61 defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices". This definition can be expanded to "an event that is in violation of explicit or implicit security policies". SP 800-61 defines several classes of incidents:

1. Denial of service—an incident that prevents or impairs the authorized use of networks, systems, and applications by exhausting resources.
2. Malicious code—a virus, worm, Trojan horse application, or network backdoor that infects a host system.
3. Unauthorized use—actions resulting in an individual gaining logical or physical access to resources without permission.
4. Inappropriate use—actions in violation of acceptable use policies (accessing objectionable material, attempting to circumvent security mechanisms, etc.)
5. Multiple-component—an incident that encompasses one or more classes of incidents.

Any of these classes of incidents could pose a significant, negative impact to the confidentiality, integrity, and availability of CBP information systems. Should a computer security incident be suspected or detected, the CBP Computer Security Incident Response Center (CSIRC) should be contacted immediately, via telephone or email.

Once the CBP CSIRC has been contacted, the CSIRC staff will ensure that the investigation, analysis, documentation, and resolution of the reported incident are conducted.

Contact Information to Report Security Incidents

Contact Group Phone/Email Hours

- CBP Help Desk – ~~Low (b)(2)~~ 7 x 24 response
- CBP CSIRC Telephone – 6 a.m. – 6 p.m. EST M–F
- CBP CSIRC Email Address –
- DHS CSIRC – After hours, 7 x 24 response

- I will promptly report IT security incidents.

Additional ATS Security Information

Accessing ATS Data

Access to ATS information and data is strictly on a need-to-know basis. No individual within U.S. Customs and Border Protection has a right to access information solely by virtue of title or position.

- Do not access data or information for which you have not received official access authorization.
- Do not upload or download data files, databases, or portions thereof from mainframes or servers unless it is part of an official job related function.
- Do not release, disclose, or alter Customs and Border Protection data without proper authority or consent.

ATS-P (Passenger) Access Requirements

Before you can be considered for an ATS-P (Passenger) user account and password, you must first meet the following criteria.

- Have a completed U.S. Customs and Border Protection background investigation.
- Have access to the **Treasury Enforcement Communications System (TECS)**.
- Have an active user profile on TECS.
- Have a need to know.

Requesting Access to ATS-P (Passenger)

To be assigned access to ATS-P (Passenger), your supervisor must send e-mail to (b)(6) (HQ, CBP) to request a user account for ATS-P Passenger. For more information, please refer to the **ATS-P (Passenger) Points of Contact** section on page 26 of this User's Guide.

Your supervisor must provide the following information:

- Name of the person requiring access.
- The person's social security number.
- The person's **Low (b)(2)**
- The person's location/port of entry.

Your supervisor must also specify that access is for the Passenger module of the ATS-P program. Any other information will be pulled from the **TELE** database on the National Data Center mainframe computer, so you should ensure that your information there is up to date.

Once approval is granted and your ATS-P (Passenger) access account is established, you will be notified of the completed request and given your ATS temporary password.

User Roles and Privileges for the Passenger Module

Based on your job function, you will have different needs and uses for the Passenger module. To help you gain access to only those features that will be of the most help to you, there are special user roles that define your levels of access privileges. For more information on the user roles available with ATS-P (Passenger), your supervisor can contact (b)(6). For more information, please refer to the **ATS-P (Passenger) Points of Contact** section on page 26 of this User's Guide.

CHAPTER THREE – OVERVIEW

This chapter will review the following:

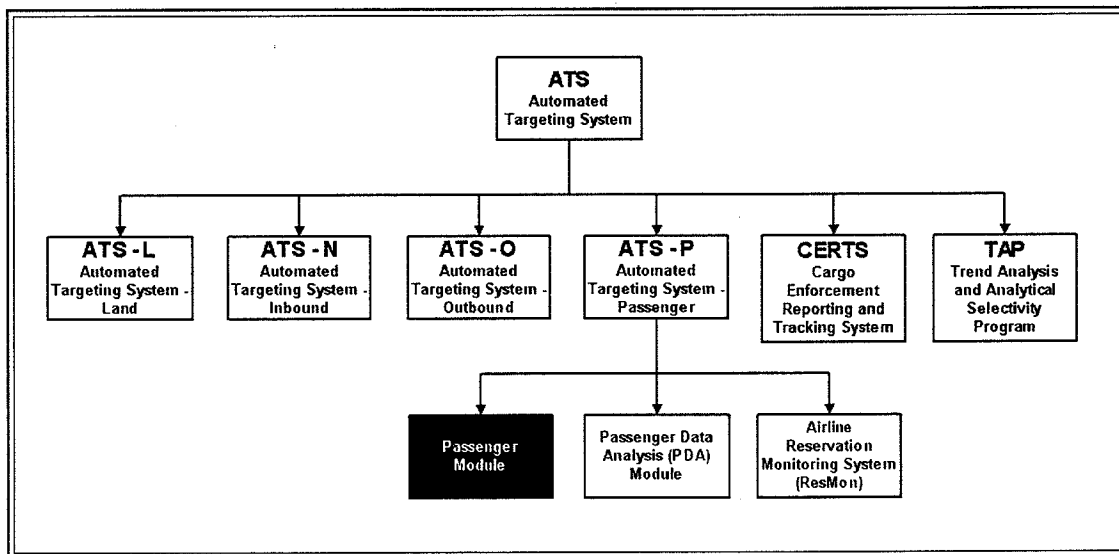
- Overview of ATS
- Overview of ATS-P (Passenger) module
- ATS-P (Passenger) data sources
- ATS-P (Passenger) points of contact
- Computer configuration requirements
- Accessing ATS-P (Passenger) from your desktop
- Accessing ATS-P (Passenger) from CBPnet
- Logging on to ATS-P (Passenger)
- Working with ATS-P (Passenger) screens
- Logging off from ATS-P (Passenger)

This Page Left Blank.

CHAPTER THREE – OVERVIEW

What is ATS?

The **Automated Targeting System (ATS)** program encompasses several Office of Information and Technology (OIT) developed projects. Those projects that fall under the ATS effort are intended to provide U.S. Customs and Border Protection (CBP) field staff with Intranet-based programs that can incorporate intelligence information and technologies to target suspect inbound and outbound traffic for inspection.



The development of the ATS-P (Passenger) program began with a request from the Office of Field Operations (OFO) for the automated capability to review and analyze international passengers arriving and departing from U.S. airports. All of the passenger information would need to be stored and then made available for analysis, via the Internet Explorer, from anywhere using the U.S. Customs and Border Protection Intranet.

What is the ATS-P (Passenger) Module?

The ATS-P (Passenger) Passenger module has its beginnings in the 1980's with a U.S. Customs and Border Protection organization called **CABINET**.

CABINET stands for the **Combined Agency Border Intelligence Network**. It is a multi-agency tactical intelligence center located at the U.S. Customs House in Chicago, IL. Since 1983, it has been providing intelligence support to law enforcement agencies worldwide to help counter transnational criminal groups.

CABINET developed targeted intelligence programs that electronically blended data over the widest possible geographic and jurisdictional scope. High (b)(2), (b)(7)(E)

The Passenger module is a computerized data system that is used at all international airports to evaluate passengers before arrival, and assist the officer's decision process with whether a passenger should be marked for a secondary examination. Specifically, the system analyzes the **Advance Passenger Information System (APIS)** data from the **Treasury Enforcement Communications System (TECS)** and passenger reservation data from the airlines.

The Passenger module that assists law enforcement personnel in the interdiction, investigation, and prosecution of terrorists, smugglers, and narcotics violators. The system is a product of electronically blending the **Non-Immigrant Information System (NIIS)**, **Suspect and Violator Indices (SAVI)**, and the **Visa** databases.

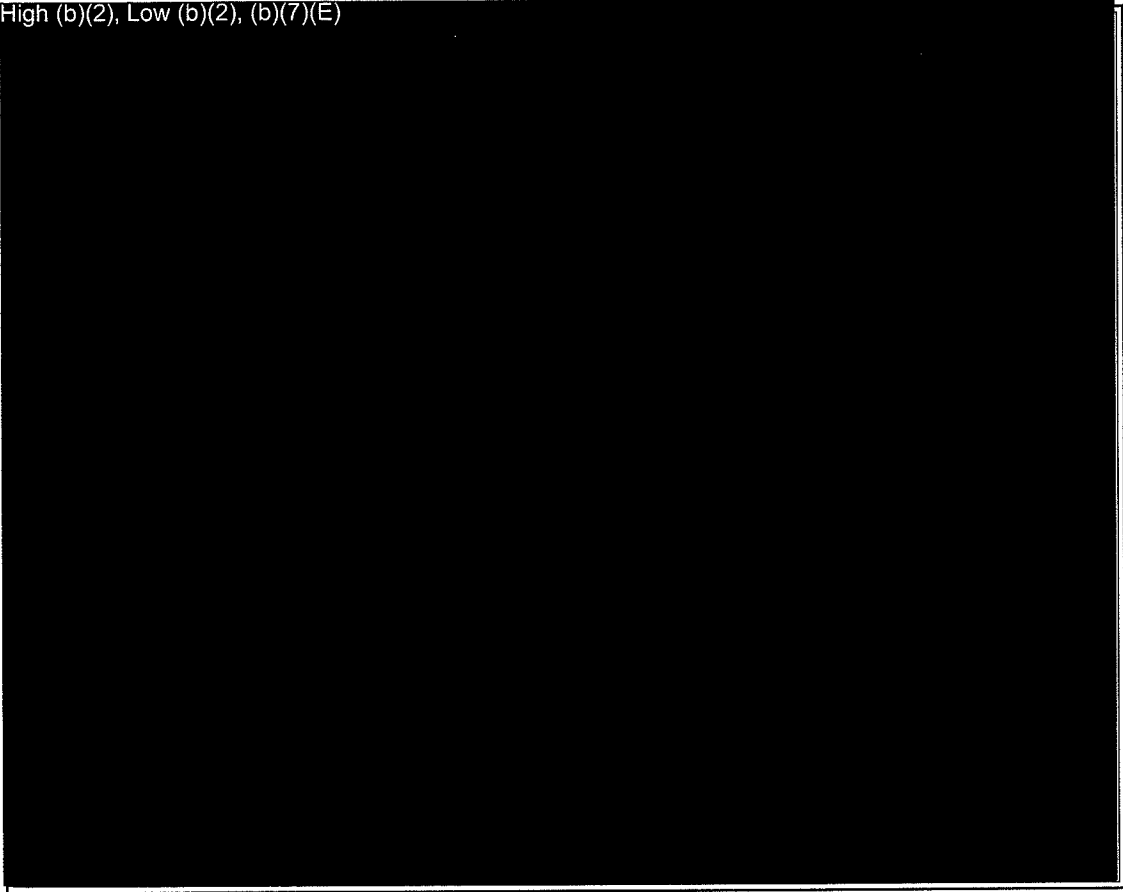
The Passenger module contains millions of travel records derived from NIIS as well as data gathered from such foreign sources as High (b)(2), (b)(7)(E), as well as law enforcement agencies within the United States.

The Passenger module provides access to travel records of citizens from 137 countries in a variety of groupings including High (b)(2), (b)(7)(E)

ATS-P (Passenger) Data Sources

ATS-P (Passenger) is a diverse software program. One reason for its power comes from the many varied types of data that stored within its several databases. The primary source of ATS-P (Passenger) data comes from the **Automated Commercial System (ACS)** and the **Treasury Enforcement Communications System (TECS)**, with data supplied to those databases from other U.S. and foreign sources.

High (b)(2), Low (b)(2), (b)(7)(E)



ATS-P (Passenger) Points of Contact

Below are the phone numbers and e-mail addresses of U.S. Customs and Border Protection personnel who are available to help you with any questions or problems you might have with ATS-P (Passenger).

ATS Technical Assistance (during working hours)

ATS Hotline (National Data Center, VA)

Phone: High (b)(2), (b)(7)(E), low (b)(2)

ATS Technical Assistance (after working hours)

Help Desk (National Data Center, VA)

Phone: High (b)(2), (b)(7)(E), low (b)(2)

cc:Mail or

Lotus Notes: HELPDESK, USCS

Internet E-mail: Low (b)(2)

Passenger Access

(b)(6) (HQ CBP, Washington, D.C.)

Phone: High (b)(2), (b)(7)(E)

cc:Mail or

Lotus Notes: (b)(6)

Internet E-mail: Low (b)(2), (b)(6)

Passenger Training

(b)(6) (HQ CBP, Washington, D.C.)

Phone: Low (b)(2), (b)(6)

cc:Mail or

Lotus Notes: Low (b)(2), (b)(6)

Internet E-mail: Low (b)(2), (b)(6)

ATS Computer Configuration Requirements

Computer Hardware Recommendations

Below is a list with the recommended hardware items and connectivity that your computer should have in order to run ATS-P (Passenger) efficiently. Note that your computer can operate with hardware items that perform at less than the below figures, but it will do so at a slower rate and may even suffer a loss of functionality.

- High (b)(2), (b)(7)(E), Low (b)(2)



Screen Resolution for Viewing ATS-P (Passenger)

ATS-P (Passenger) screens are best viewed using a screen resolution of 1024 by 768, rather than the conventional 800 by 600 resolution. This setting is changed using the **Display** feature found in the Windows Control Panel. However, if you need to change your monitor's screen resolution to the above resolution, you should contact your system or network administrator.

The Microsoft Internet Explorer

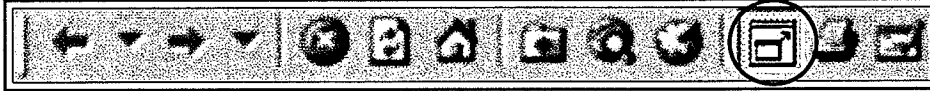
High (b)(2), (b)(7)(E), Low (b)(2) is the recommended tool for accessing and viewing ATS-P (Passenger) from the Intranet. If you have problems running ATS-P (Passenger) with the Internet Explorer, please contact your system administrator or the ATS Hotline. For more information, please refer to the **ATS-P (Passenger) Points of Contact** section, on page 26 of this User's Guide.

Internet Explorer Toolbar Icons

ATS-P (Passenger) was designed and developed to provide you ease of access to as much data as can be displayed in an orderly manner. Traveling between ATS-P (Passenger) screens can be done by using the buttons, options, and tabs that are a part of the ATS-P (Passenger) program. It is recommended that you not use the forward or back toolbar buttons that are part of the Internet Explorer.

Full Screen Mode

The only toolbar button that will be useful to you is the **Full Screen** button. When using the Internet Explorer to view ATS-P (Passenger), the screens are best displayed with the display mode set for Full Screen. This mode gives you more screen area in which to display ATS-P (Passenger) information without resorting to using scroll bars.

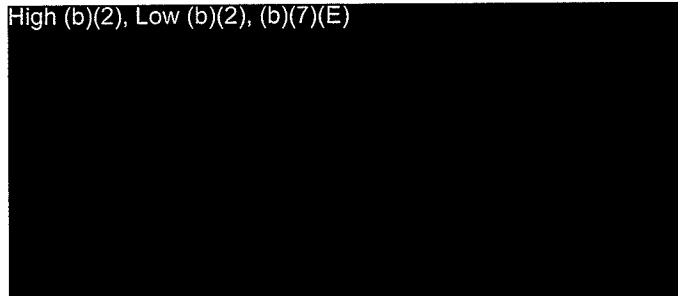


If there is no Full Screen button on the Internet Explorer toolbar, it will need to be placed there using Internet Explorer's Customize feature.

NOTE If you prefer to use your keyboard, you can toggle Full Screen off and on by using the **[F11]** key.

Auto-Hide Your Internet Explorer Toolbar

After you've set your monitor to Full Screen, you will have available to you an option to hide the Internet Explorer toolbar. Hiding this toolbar will further increase the amount of your monitor screen that can be devoted to displaying ATS-P (Passenger) screens. It is recommended that you hide your Internet Explorer toolbar.



To hide your Internet Explorer toolbar, first make sure that your monitor display is set to **Full Screen**. Next, use your mouse to right-click a blank area of the toolbar. From the drop-down menu, choose the **Auto-Hide** selection. After making this selection, the toolbar will disappear from the top of the screen. To re-display the toolbar, place your mouse cursor at the top of the screen and the toolbar will drop down again for your use.

Internet Explorer Security Settings

High (b)(2), (b)(7)(E), Low (b)(2)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Large Redacted Block]

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

Chapter Three – Overview

High (b)(2), (b)(7)(E), Low (b)(2)

[Redacted text block]

[Redacted text block]

Configuring Your Proxy Server Settings

High (b)(2), (b)(7)(E), Low (b)(2)
[Redacted]

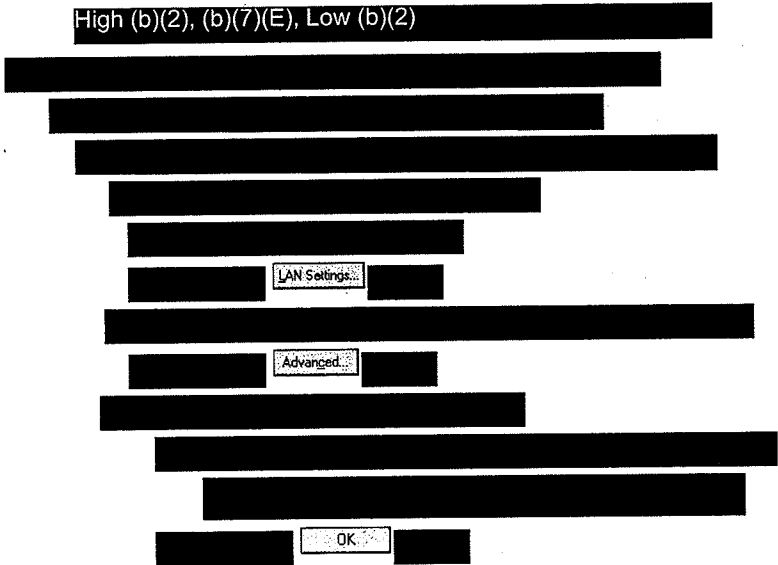
[Redacted]

[Redacted]

[Redacted]

[Large Redacted Area]

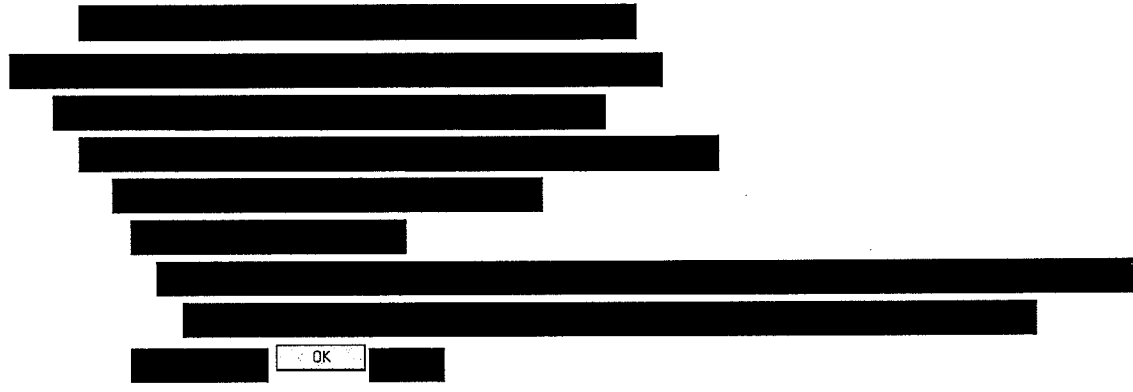
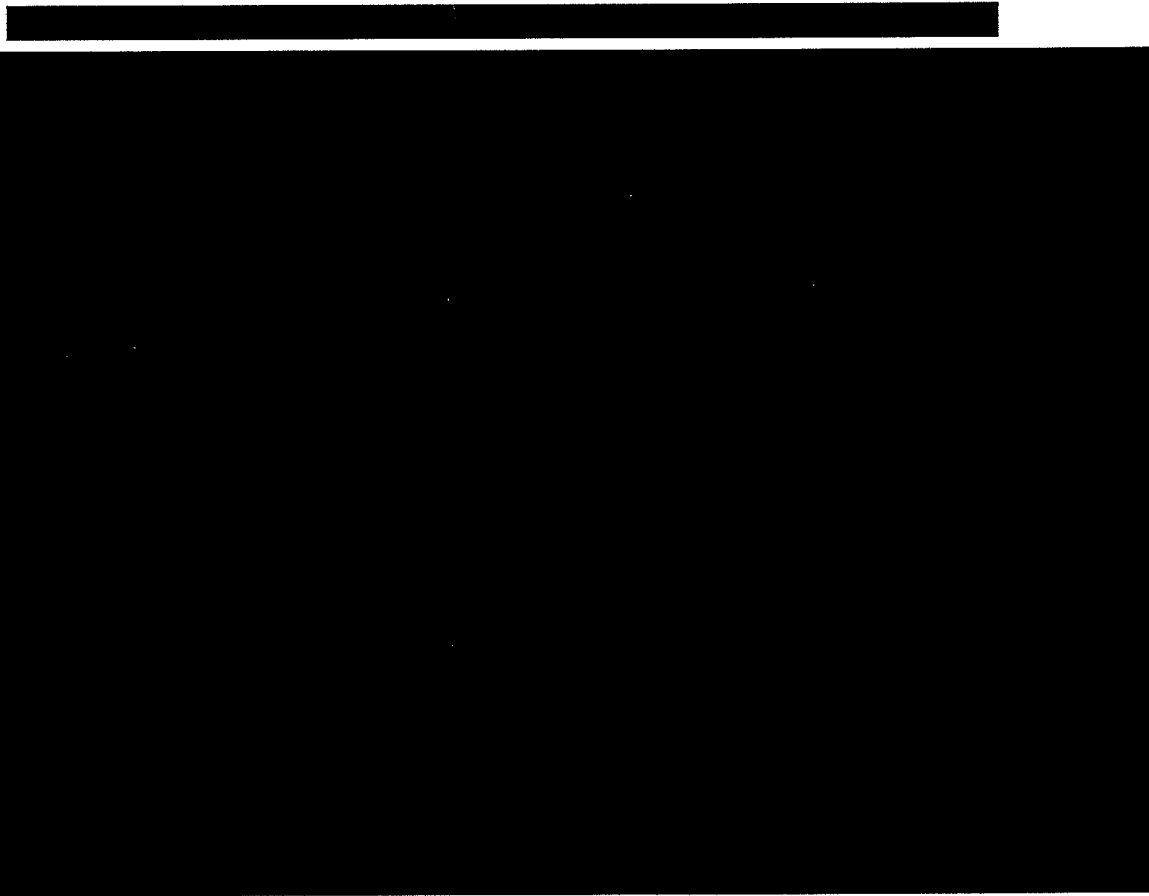
High (b)(2), (b)(7)(E), Low (b)(2)




Cookies

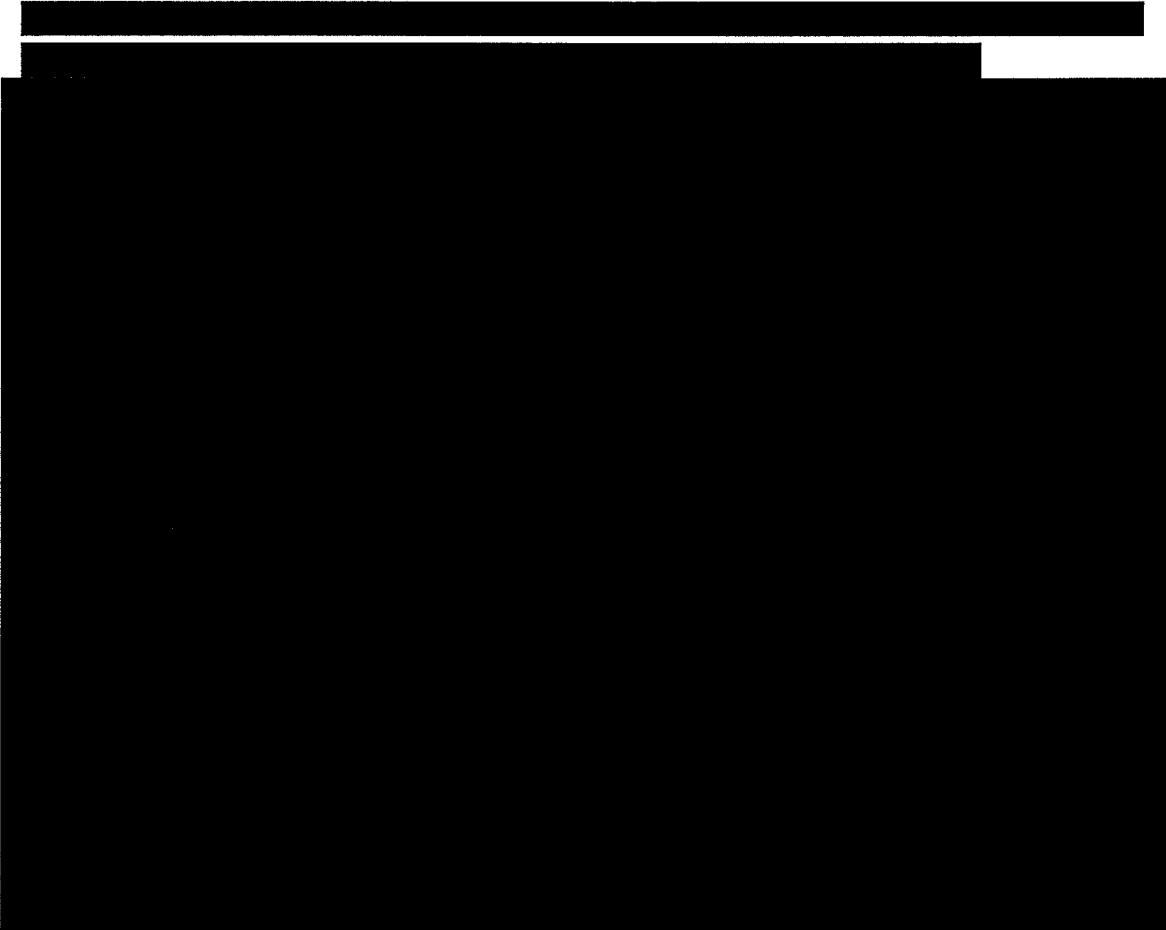
Cookies are text files that are used to store your user information on your hard drive for future reference.

High (b)(2), Low (b)(2), (b)(7)(E)



Displaying the Latest Internet Explorer Page

When you display an ATS screen using your web browser, Internet Explorer saves the web page for that screen as a temporary file. Unfortunately, if you travel away from that page and if it's then automatically updated, you could still see the old version if you return to it using the Internet Explorer  button or any High (b)(2), (b)(7)(E), Low (b)(2)



High (b)(2), (b)(7)(E), Low (b)(2)

Settings...

OK

OK

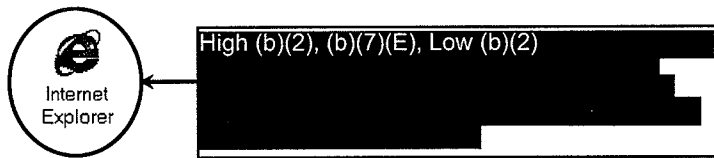
Accessing ATS-P (Passenger)

There are two ways of accessing ATS-P (Passenger). The program is available from the U.S. Customs and Border Protection's **CBPnet** intranet site (which is located within the CBP firewall) or directly from your Internet Explorer by typing the short form of the address for ATS-P (Passenger).

In either case, you must first make sure that you have a valid ATS-P (Passenger) user account. For more information, please refer to the **Requesting Access to ATS-P (Passenger)** section on page 20 of this User's Guide.

Accessing ATS-P (Passenger) from Your Desktop

To access the ATS-P (Passenger) Intranet program directly from your computer, you will first need to locate the Internet Explorer (IE) icon. This icon will be located on your computer's "desktop" or one of the Windows taskbars.



Double-click this icon. The Internet Explorer will start and its default home page will be displayed.

High (b)(2), (b)(7)(E), Low (b)(2)

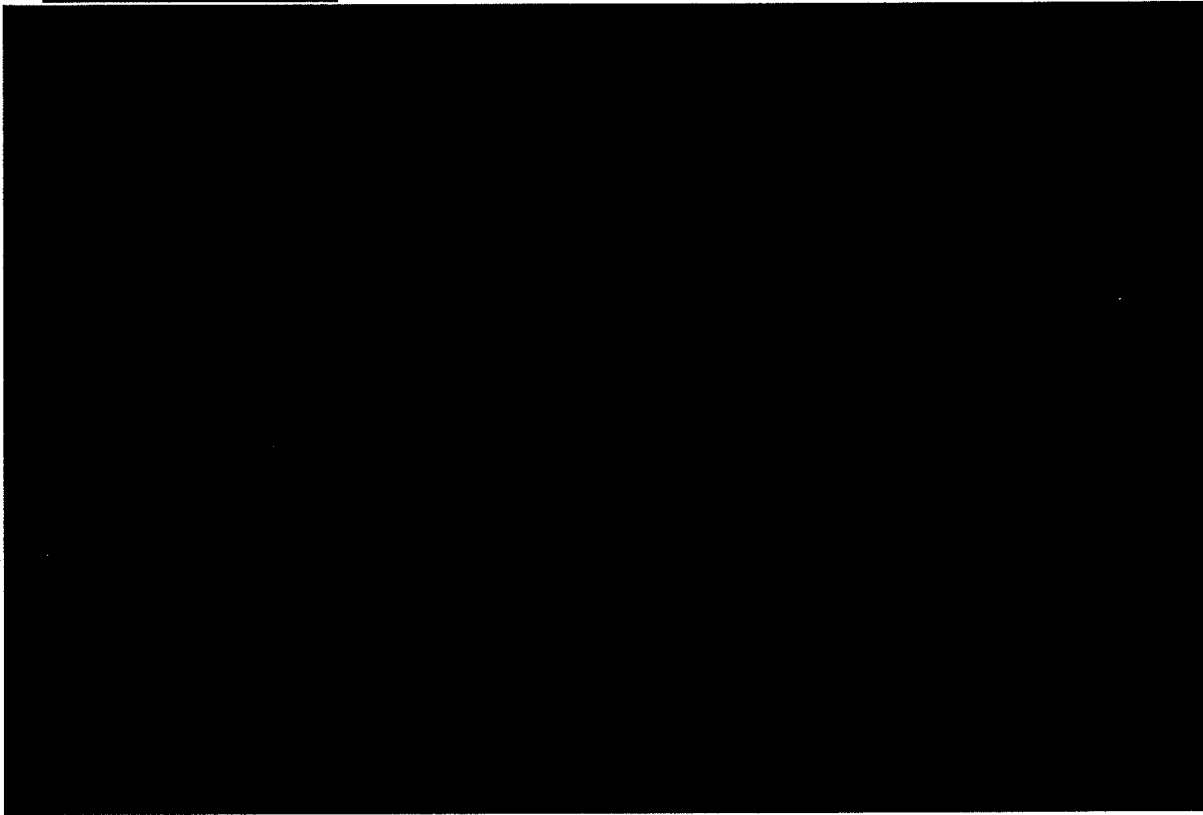


After accessing the ATS-P (Passenger) Intranet program, Internet Explorer will display the **ATS Logon** screen.

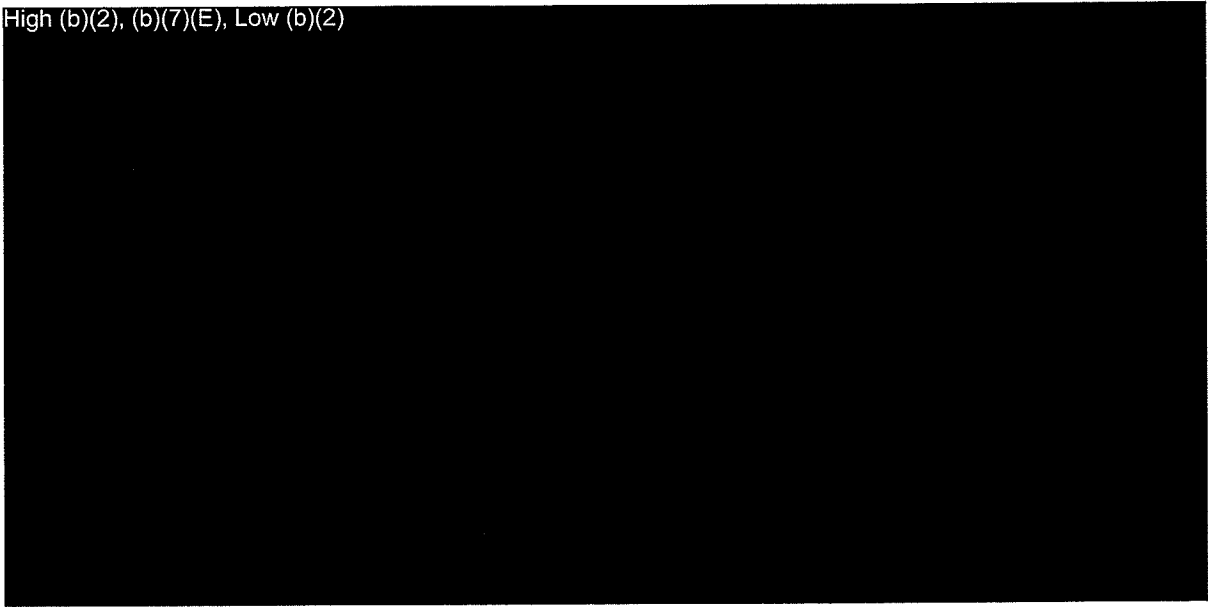
Accessing ATS-P (Passenger) from CBPnet

ATS-P (Passenger) is also available to you from the U.S. Customs and Border Protection's CBPnet Intranet site. High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]




High (b)(2), (b)(7)(E), Low (b)(2)



The **Automated Systems** web page contains the links to ATS-P (Passenger) as well as the **Automated Targeting System (ATS)** suite of software programs.

High (b)(2), (b)(7)(E), Low (b)(2)



High (b)(2), Low (b)(2), (b)(7)(E)


The Internet

Explorer will open a new window for ATS-P (Passenger) that will display the **ATS Logon** screen.

The ATS Logon Screen

The **ATS Logon** screen is the first screen displayed after you access the ATS-P (Passenger) program from your computer or from **CBPnet**. From this screen, you can either log on to ATS-P (Passenger) or change your ATS password.

High (b)(2), (b)(7)(E), Low (b)(2)



Related Information

- The **Logging on to ATS-P (Passenger) for the First Time** section on page 91 of this User's Guide.

Logging on to ATS-P (Passenger)

After starting ATS-P (Passenger), the **ATS Logon** screen will be displayed. High (b)(2), (b)(7)(E), Low (b)(2)



High (b)(2), (b)(7)(E), Low (b)(2)



Field Descriptions for the ATS Logon Screen

High (b)(2), (b)(7)(E), Low (b)(2)



Following your successful logon to the program, ATS-P (Passenger) displays its **Start Page**. From this screen, as well as any other ATS-P (Passenger) screen, you'll be able to access all ATS-P (Passenger) features using the selection options found in the upper right corner of each screen.

First Time Logon to ATS-P

When you log on to ATS-P (Passenger) for the first time, the **ATS Logon** screen will be displayed and you will be asked to change your temporary password to one of your choosing. For more information, please refer to **Logging on to ATS-P (Passenger) for the First Time**, on page 91 and to **Changing Your ATS Password**, on page 44 of this User's Guide.

High (b)(2), (b)(7)(E), Low (b)(2)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

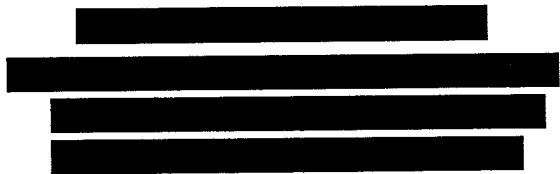
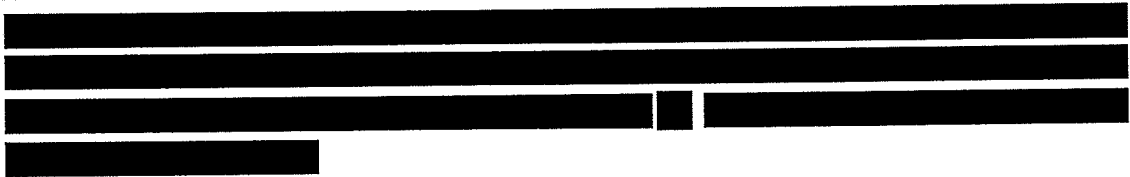
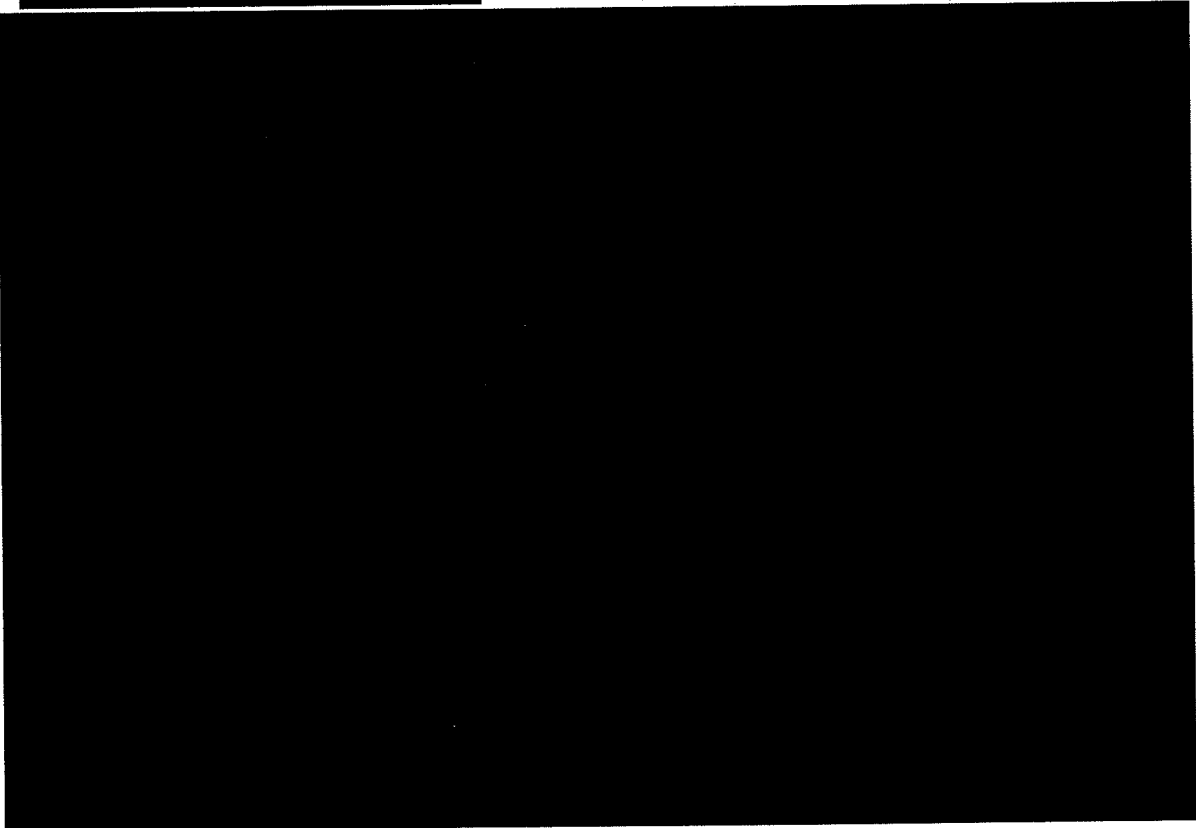
[Redacted]

[Redacted]

[Redacted]

Changing Your ATS Password

First time users of ATS-P (Passenger) will be required to change the temporary password that they received after obtaining access. In addition, U.S. Customs and Border Protection require that users of its software programs regularly change their access passwords to maintain the security of the program and protect sensitive law enforcement data. **High (b)(2), (b)(7)(E), Low (b)(2)**



LAW ENFORCEMENT SENSITIVE

High (b)(2), (b)(7)(E), Low (b)(2)

[Redacted text block containing approximately 15 lines of obscured content]


Related Information

- The Logging on to ATS-P (Passenger) for the First Time section on page 91 of this User's Guide.



Working with ATS-P (Passenger) Screens

ATS-P (Passenger) makes full use of the graphical nature of the Intranet. Each screen displayed by the program has one (or more) icons or buttons. Clicking one of these will, depending on the icon or button selected, perform a specific function. The below graphic shows a broad cross section of the icon and buttons used by ATS-P (Passenger) and some of the functions they perform.

High (b)(2), (b)(7)(E), Low (b)(2), (b)(6)



Logging off from ATS-P (Passenger)

After you're finished using the ATS-P (Passenger), you need to log off from the program 
High (b)(2), (b)(7)(E), Low (b)(2)  After logging off, ATS-P
(Passenger) will re-display the **ATS Logon** screen.

LAW ENFORCEMENT SENSITIVE

This Page Left Blank.

LAW ENFORCEMENT SENSITIVE

003339

CHAPTER FOUR – LEARNING ABOUT ATS-P

This chapter will review the following:

- The Start Page
- The Home option
- Managing queries
- Setting preferences
- The Create option
- The Links option
- The Help option

This Page Left Blank.

CHAPTER FOUR – LEARNING ABOUT ATS-P

Overview

After you log on to ATS-P (Passenger), you'll have the means available to keep yourself abreast of the latest news and information within the U.S. Customs and Border Protection ATS environment. The [REDACTED]

High (b)(2), (b)(7)(E)

ATS-P (Passenger) organizes its main features under the options located in the upper right corner of the display. High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The Start Page

The **Start Page** is displayed after you've successfully logged on to ATS-P (Passenger). [REDACTED]

High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]

[REDACTED]

Since this screen is designed to offer easy access to task-specific features [REDACTED] High (b)(2), (b)(7)(E), Low (b)(2) more information, please refer to **User Roles and Privileges for the Passenger Module**, on page 20 of this User's Guide.

High (b)(2), (b)(7)(E), Low (b)(2), (b)(6)



~~LAW ENFORCEMENT SENSITIVE~~

High (b)(2), (b)(7)(E), Low (b)(2)

[Redacted]

[Redacted]

[Redacted]

~~LAW ENFORCEMENT SENSITIVE~~

Start Page High (b)(2), (b)(7)(E), Low (b)(2)

High/Low (b)(2), (b)(7)(E)
[Redacted]

[Redacted]

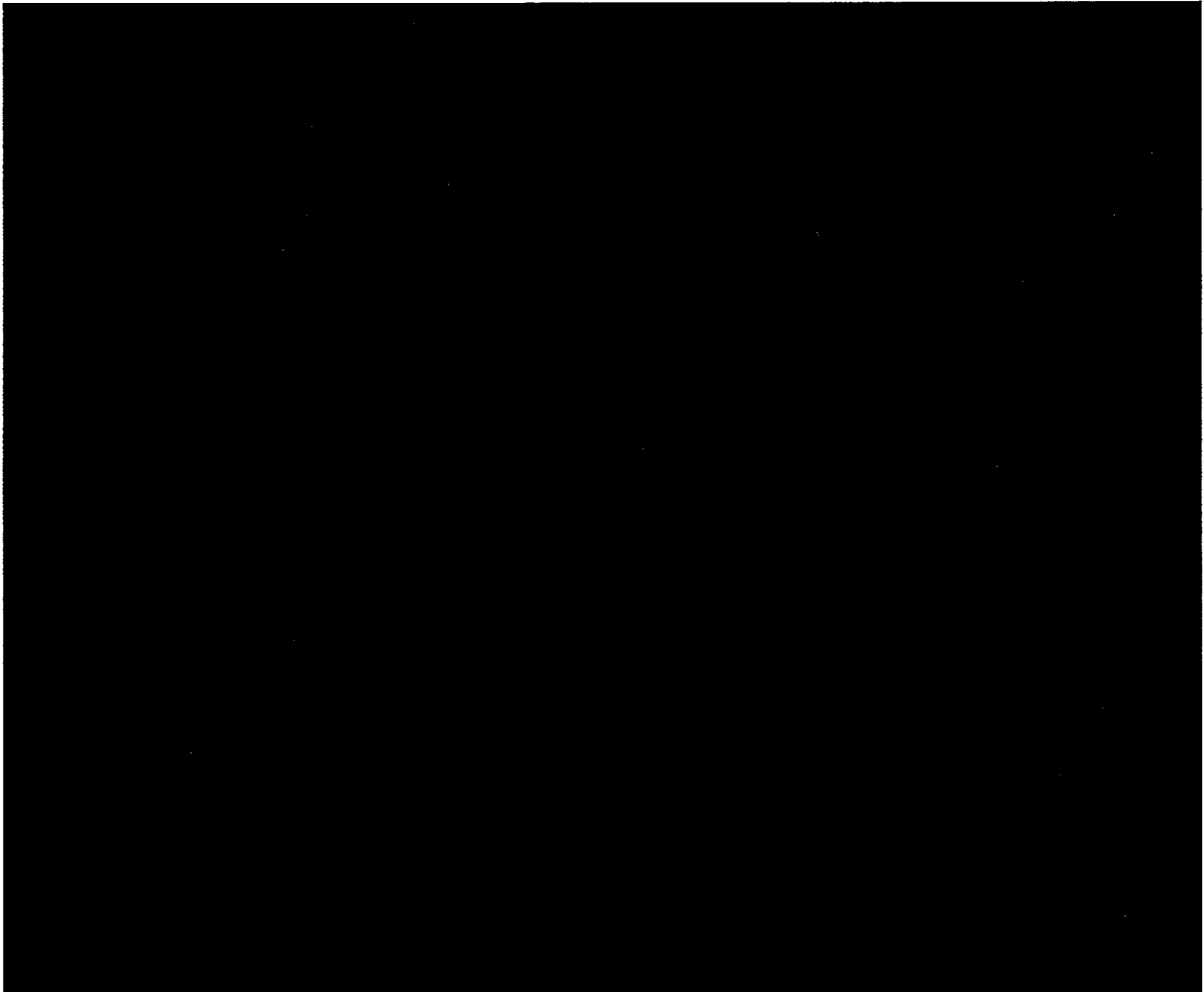
[Redacted]

[Redacted]

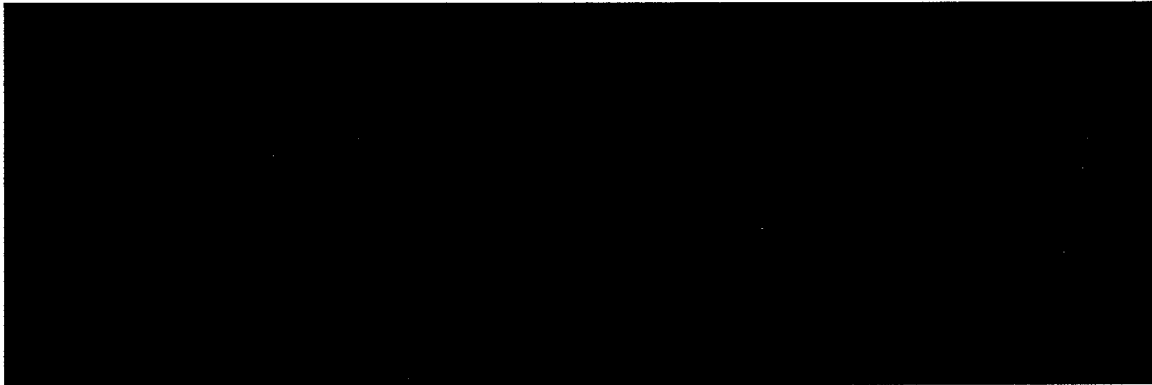
[Redacted]

High (b)(2), (b)(7)(E), Low (b)(2), (b)(6)
[Redacted]

High (b)(2), (b)(7)(E), Low (b)(2)



[Redacted line of text]



LAW ENFORCEMENT SENSITIVE

ATS-P (Passenger)
High (b)(2), (b)(7)(E), Low (b)(2)

Chapter Four – Learning About ATS-P



~~LAW ENFORCEMENT SENSITIVE~~

High (b)(2), (b)(7)(E), Low (b)(2)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

High (b)(2), (b)(7)(E), Low (b)(2), (b)(6)

[Redacted text block]

[Redacted text line]

High (b)(2), (b)(7)(E), Low (b)(2)




[Redacted text block]

LAW ENFORCEMENT SENSITIVE

ATS-P (Passenger)

Chapter Four – Learning About ATS-P

High (b)(2), (b)(7)(E), Low (b)(2)



LAW ENFORCEMENT SENSITIVE



003350

[REDACTED]
High (b)(2), (b)(7)(E), Low (b)(2)

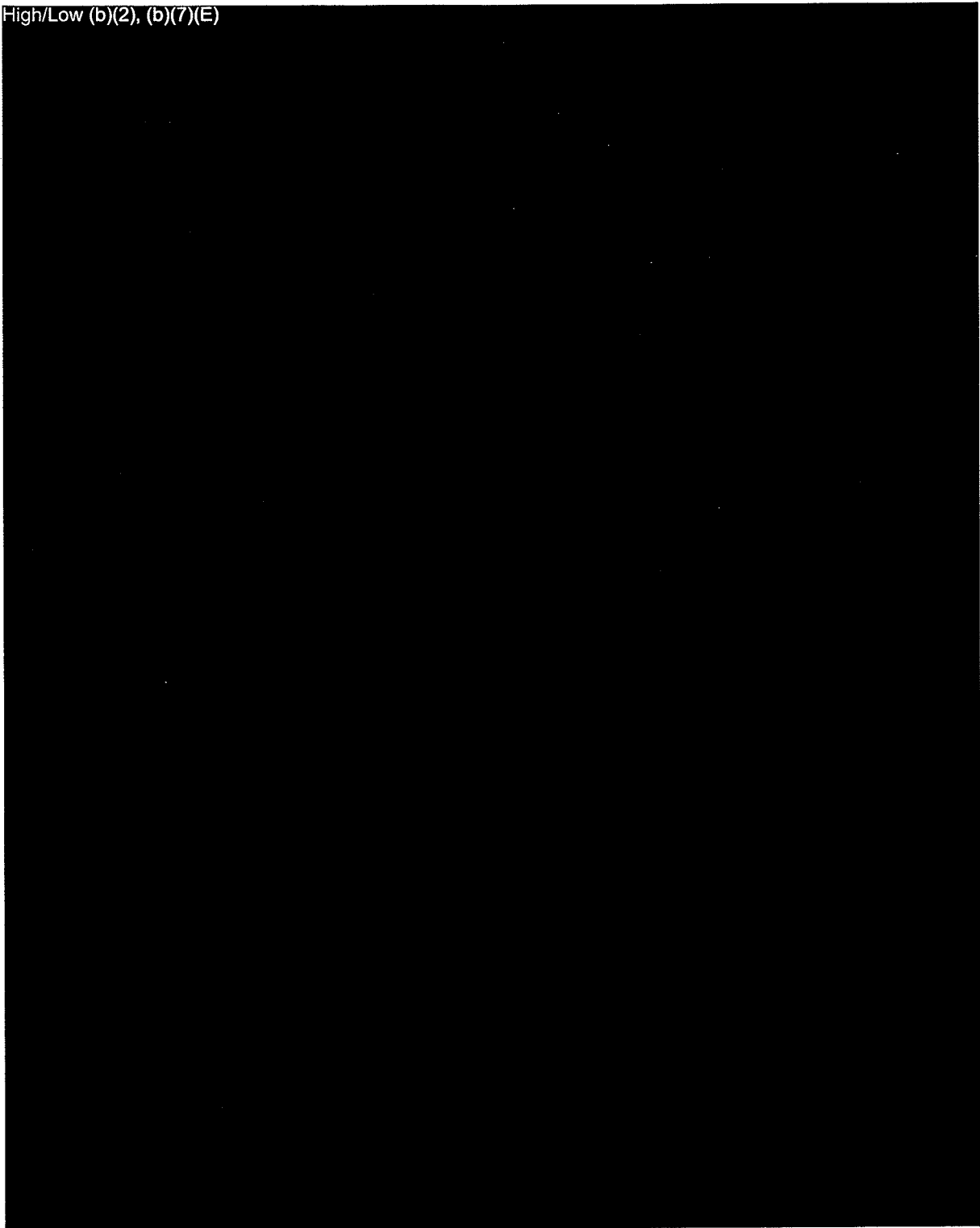
[REDACTED]

[REDACTED]
High/Low (b)(2), (b)(7)(E)

[REDACTED]

LAW ENFORCEMENT SENSITIVE

High/Low (b)(2), (b)(7)(E)



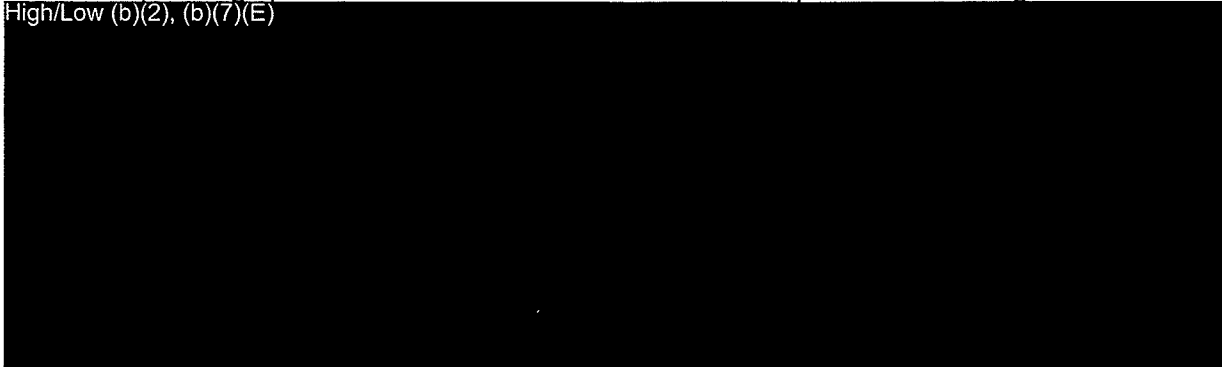
~~LAW ENFORCEMENT SENSITIVE~~

003352

LAW ENFORCEMENT SENSITIVE

ATS-P (Passenger)
High/Low (b)(2), (b)(7)(E)

Chapter Four – Learning About ATS-P



~~LAW ENFORCEMENT SENSITIVE~~

High/Low (b)(2), (b)(7)(E)

High (b)(2), (b)(7)(E), Low (b)(2)

High (b)(2), (b)(7)(E), (b)(6)

High (b)(2), (b)(7)(E), Low (b)(2)

Reference Section

This section of the **Start Page** is available to all ATS-P (Passenger) users. High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]

[REDACTED]

[REDACTED]

Reference Section Links

High/Low (b)(2), (b)(7)(E)

[REDACTED]

[REDACTED]
High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]

[REDACTED] For more information on this screen, refer to page 173 of this User's Guide.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]

[REDACTED]

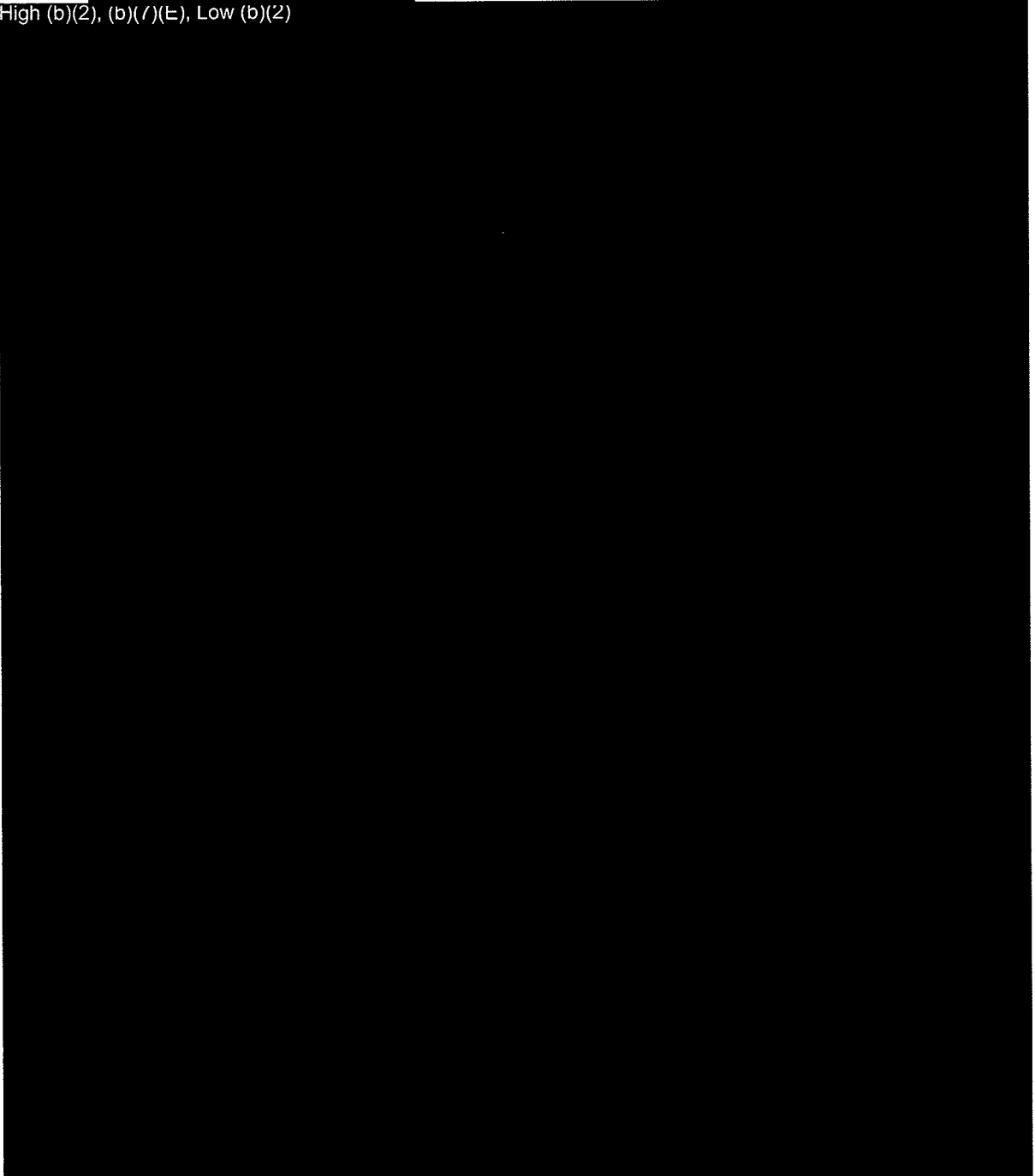
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

High (b)(2), (b)(7)(E), Low (b)(2)



The Home Option

Overview

The **Home** option provides you with easy access to features used for setting up and maintaining your ATS-P (Passenger) display. High (b)(2), (b)(7)(E) These features allow you to quickly jump to the **Start Page**, set or modify your ATS-P (Passenger) display preferences, or log off from ATS-P (Passenger). High (b)(2), (b)(7)(E), Low (b)(2)

High (b)(2), (b)(7)(E), Low (b)(2)



The first feature under the **Home** option allows you to navigate to the **Start Page**, ATS-P (Passenger)'s opening screen. High (b)(2), (b)(7)(E), Low (b)(2)

The third helps you with tailoring the layout of ATS-P (Passenger), while the last selection permits you to exit the program.

Click the Start page selection to jump directly to the **Start Page**. High (b)(2), (b)(7)(E), Low (b)(2)

Choosing the My Preferences selection will take you to ATS-P (Passenger)'s feature for changing certain screen displays. Clicking Logout will end ATS-P (Passenger) but allow you to remain in your current Internet Explorer window with the **ATS Logon** screen displayed.

Web Page Features

In addition to the general housekeeping features organized under the **Home** option,

High (b)(2), (b)(7)(E), Low (b)(2)

LAW ENFORCEMENT SENSITIVE

Printing the Current Screen Display

The Print... feature allows you to print the currently displayed screen using your designated printer. Note that the selection options and screen titles found at the top of the screen, as well as any buttons located at the bottom, will not be included in the printout.

High (b)(2), (b)(7)(E), Low (b)(2)

A large black rectangular redaction box covers the majority of the page's content, starting below the first paragraph and extending nearly to the bottom of the page.

[REDACTED]

High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

High (b)(2), (b)(7)(E), Low (b)(2), (b)(6)

[REDACTED]

High (b)(2), (b)(7)(E), Low (b)(2)

[REDACTED]

~~LAW ENFORCEMENT SENSITIVE~~

High (b)(2), (b)(7)(E), Low (b)(2)

[Redacted]

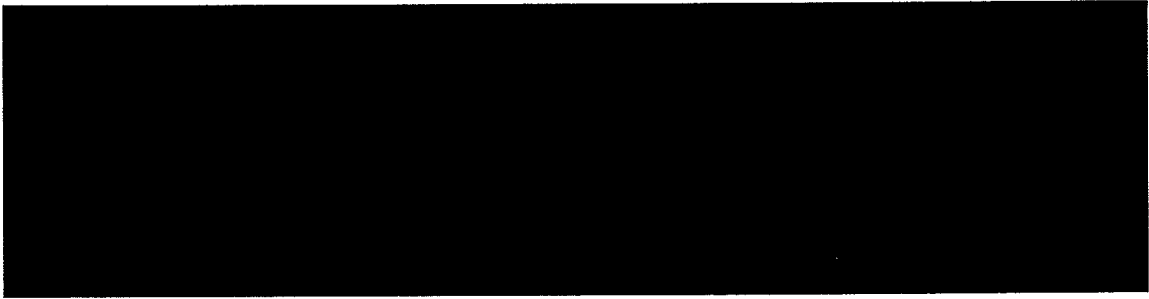
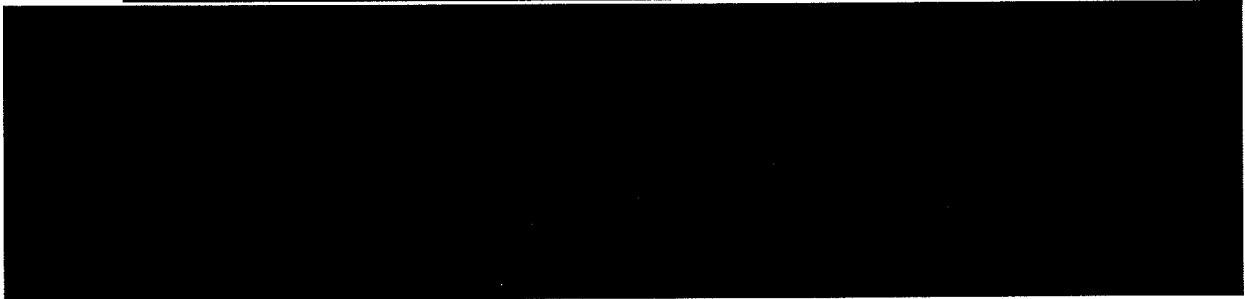

[Redacted]

[Redacted]


[Redacted]

[Large Redacted Block]

High (b)(2), (b)(7)(E), Low (b)(2)



High (b)(2), (b)(7)(E), Low (b)(2)



[REDACTED]
High (b)(2), (b)(7)(E), Low (b)(2)

NOTE [REDACTED]

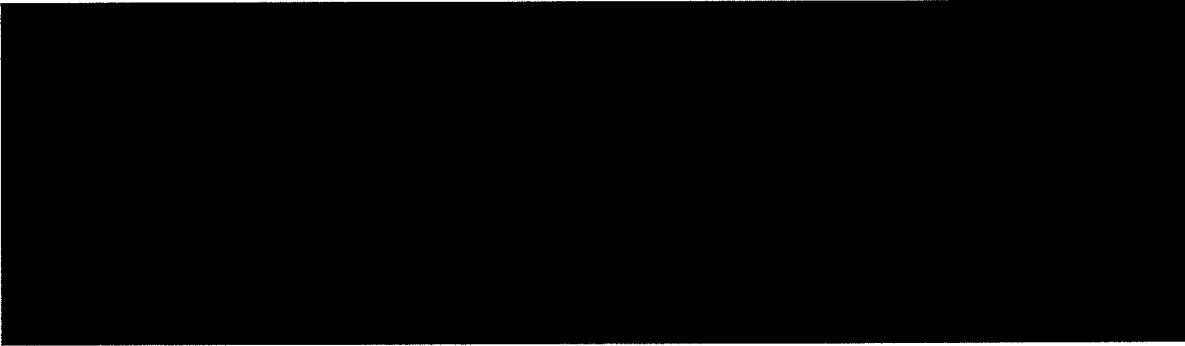
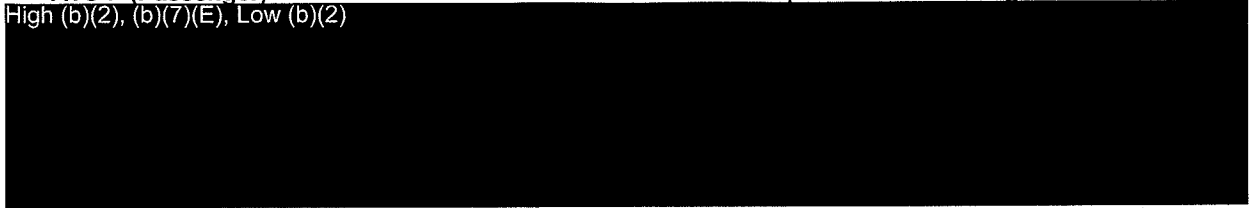
[REDACTED]

[REDACTED]

[REDACTED]

ATS-P (Passenger)
High (b)(2), (b)(7)(E), Low (b)(2)

Chapter Four – Learning About ATS-P

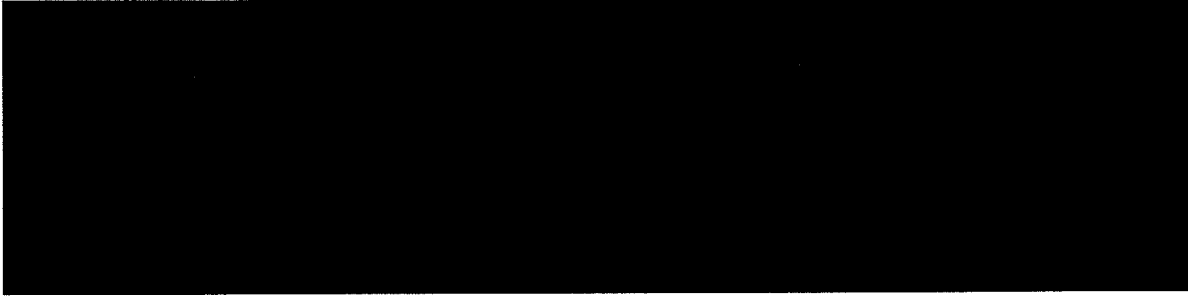
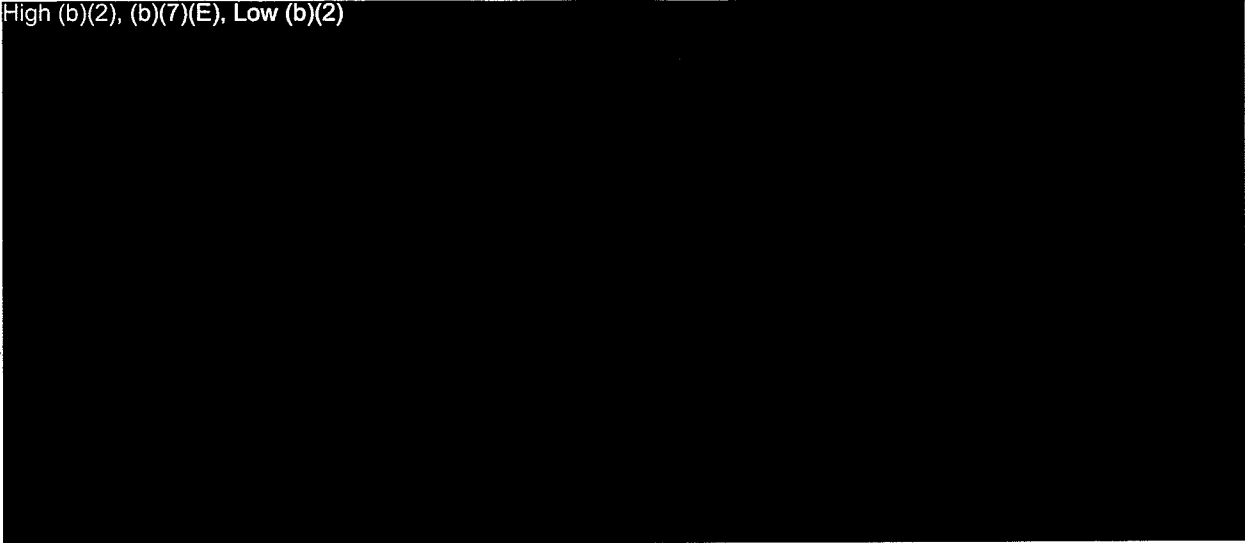


[REDACTED]
High (b)(2), (b)(7)(E), Low (b)(2)
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

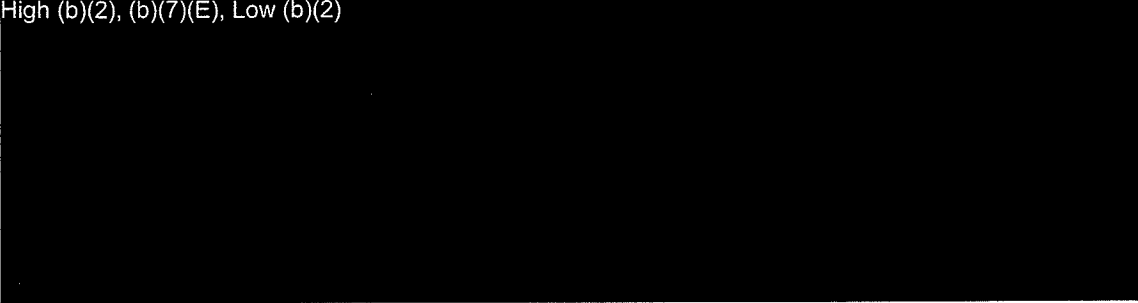
[REDACTED]

[REDACTED]

High (b)(2), (b)(7)(E), Low (b)(2)

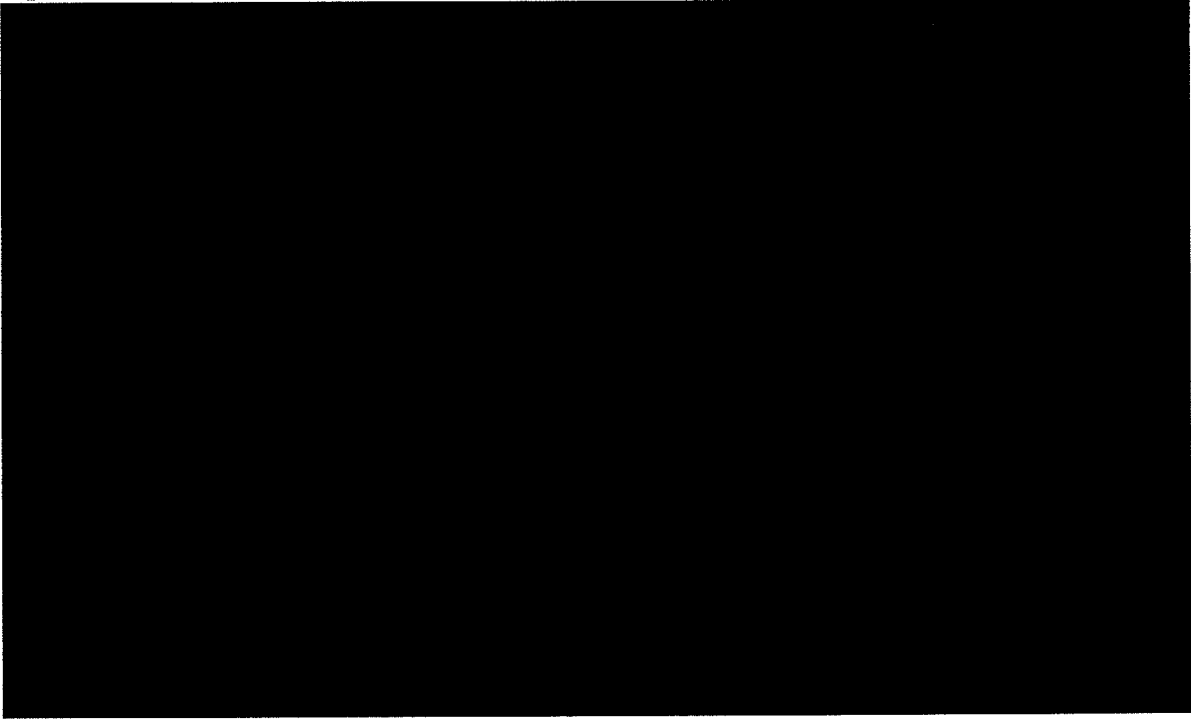


High (b)(2), (b)(7)(E), Low (b)(2)

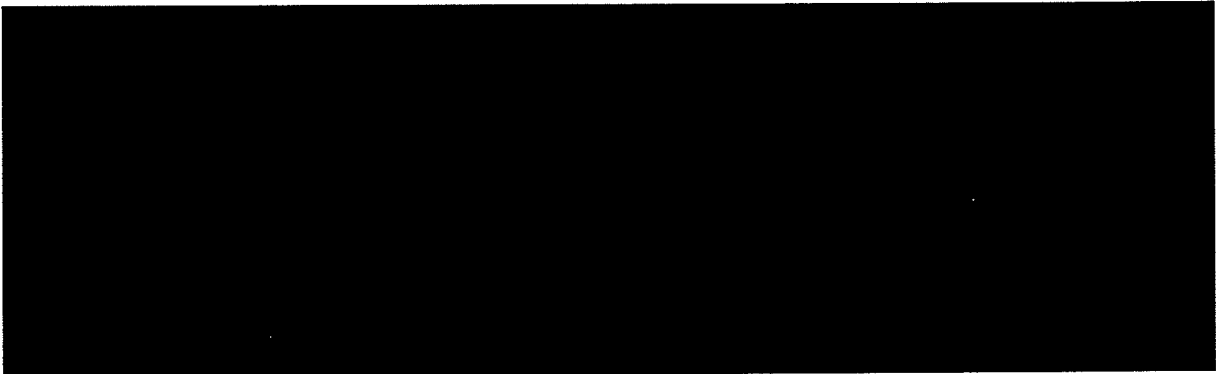


Start Page Tab

From this tab, you can specify the type of information that will be displayed in the **Report Information** section of the **Start Page**. High (b)(2), (b)(7)(E), Low (b)(2)



Field Descriptions for the Change Personal Preferences (Start Page Tab) Screen



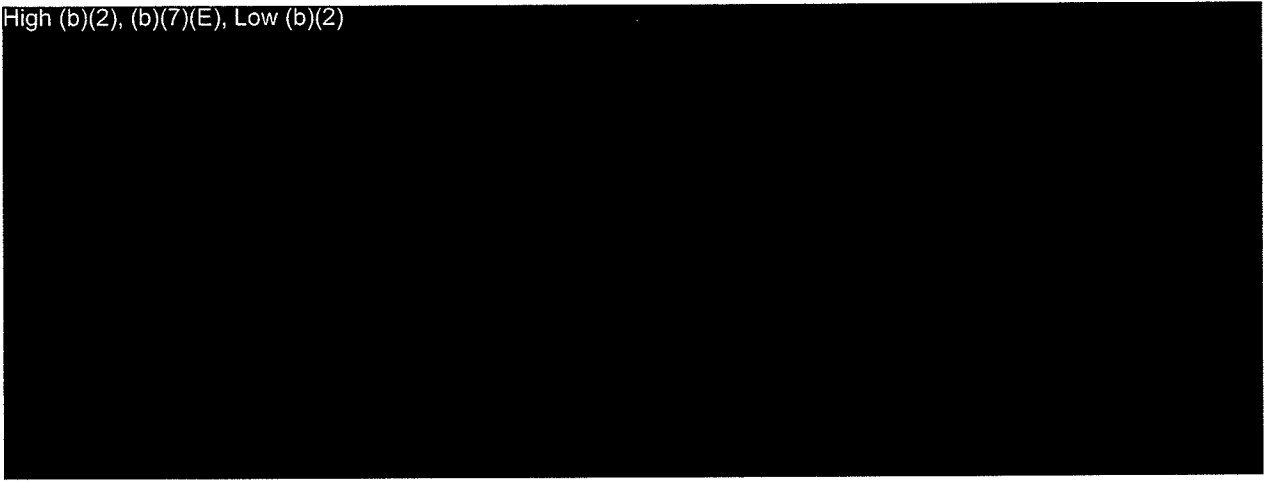
Button Descriptions for the Change Personal Preferences (Start Page Tab) Screen

<i>Button</i>	<i>Description</i>
	Print the currently displayed screen using your designated printer.
	<u>S</u> ave the current settings and exit the screen.
	Close and exit the screen.

How to Set Your Start Page Preferences

From the **Change Personal Preferences** screen, perform the following:

High (b)(2), (b)(7)(E), Low (b)(2)



The Links Option

Overview

High (b)(2), (b)(7)(E), Low (b)(2)

These Internet sites provide research information that can give you background data to support the research you're performing. These Internet sites are organized under several different categories.



Internal Links

The **Code of Federal Regulations** link gives you access to information on foreign trade that is provided by the Department of Commerce. The information comes from Title 15, Volume 2, Parts 300 to 799 of the Code of Federal Regulations. This link does not require that you have Internet access.

High (b)(2), (b)(7)(E), Low (b)(2)

High (b)(2), (b)(7)(E), Low (b)(2)

[Redacted]

[Redacted]

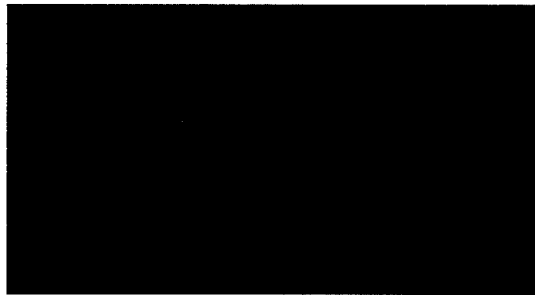
[Redacted]

The Help Option

Overview

The **Help** option provides you easy access to the **Online Help Topics** feature. The **Online Help Topics** feature gives you quick access to information on ATS-P (Passenger) and how to use it. [REDACTED]


High (b)(2), (b)(7)(E), Low (b)(2)
[REDACTED]






Online Help Topics


ATS-P (Passenger) offers you online help to assist you in working with the program. With this feature, you can review the help topics contents available to you, locate the help item you want by selecting it from an index, or use the search tool to locate selected text from the online help pages.

The Contents Tab


Help topics located under the **Contents** tab are organized using a table of contents structure. At the highest level are sections. Sections are identified by the  icon and serve to provide a high-level title for the information organized under them. They themselves do not contain online help information.

Organized under these section books are either sub-sections (also having the  icon) or pages of help text, represented by the  icon. As with sections, sub-sections do not contain help data, they further break down the organization of the information found under the section they belong to.

To open a section or sub-section and view its contents, just click on it and it will expand to display the information that is organized under it. The  icon will be displayed to show that you've "opened" the book.

Online help data is found at the page level. To view a page of help data, click on any  icon and its corresponding help text will be displayed on the right portion of the screen.


High (b)(2), (b)(7)(E), Low (b)(2)



The Index Tab

The **Index** tab allows you to access help text by typing a keyword or keyword phrase. These keywords and phrases are associated with help pages and offer you multiple methods of locating help text. Selecting a keyword or phrase will display the associated help topic page in the right portion of the screen.

High (b)(2), (b)(7)(E), Low (b)(2)



The Search Tab

The **Search** tab enables you to view help text pages that contain specific words found on help topic pages. After typing in the appropriate search word from either of the two **Search** fields available to you, all qualifying help topic pages that include that word will be displayed. Selecting the appropriate help topic will display that topic page in the right portion of the screen.

High (b)(2), (b)(7)(E), Low (b)(2)






Online User's Guide

Located within the online help topics is an electronic version of the ATS-P (Passenger) User's Guide and Reference Manual. It is available as a **Portable Document Format (PDF)** document that is accessible only by using the Adobe Acrobat Reader.


NOTE

If you do not have the Adobe Acrobat Reader installed on your computer, please contact your local System Administrator.

To access the online ATS-P (Passenger) User's Guide and Reference Manual, click the **Online User's Guide** selection (identified by the  icon) from the online help topics menu. After expanding the section () to display the help page () , click the **ATS-P (Passenger) User's Guide and Reference Manual** selection.

The displayed help topic contains a link to an electronic version of this ATS-P (Passenger) User's Guide and Reference Manual. To display the document, click the small facsimile icon of the User's Guide cover page. This will start the Acrobat Reader software, which will display the User's Guide and Reference Manual using a new Internet Explorer window.

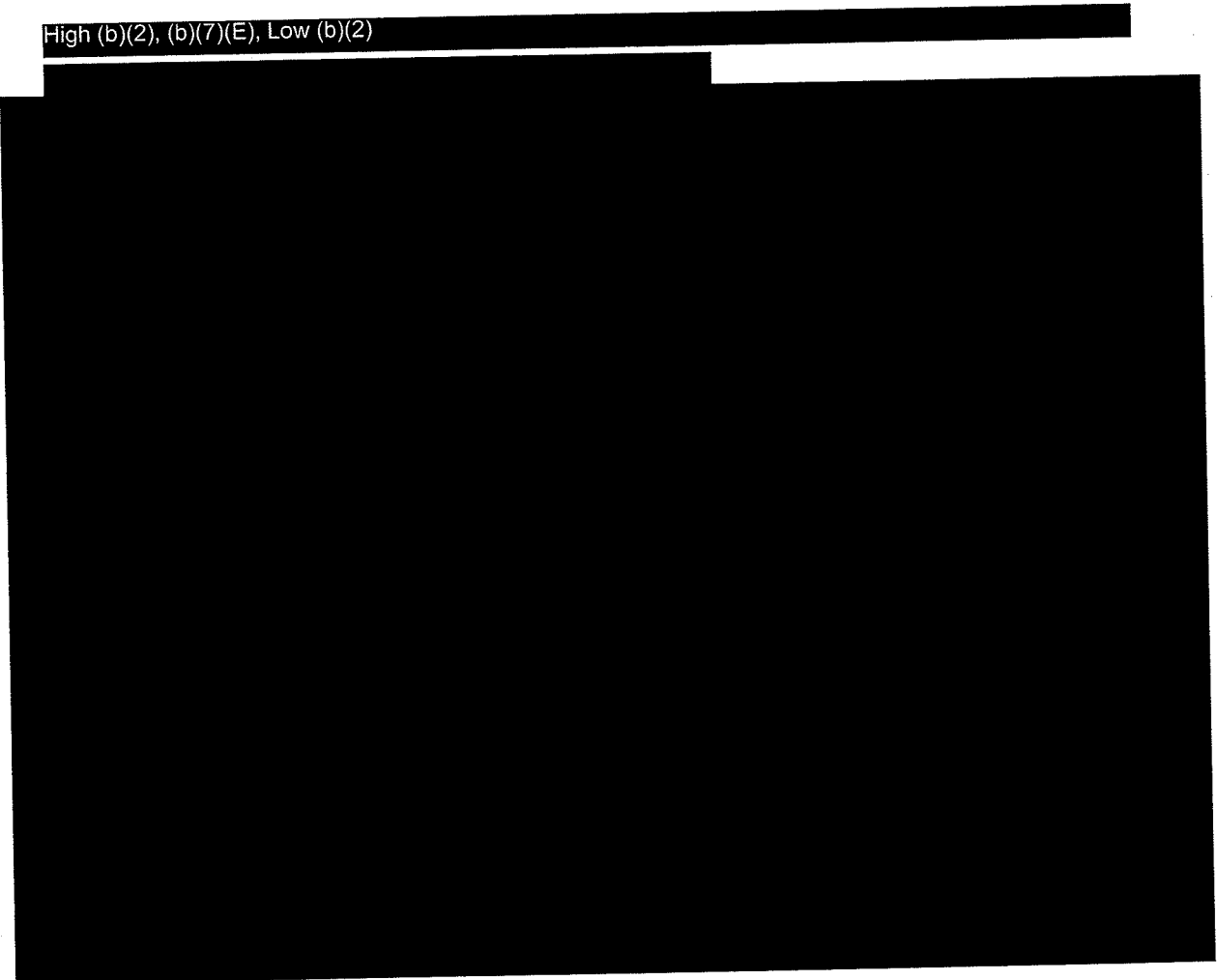
High (b)(2), (b)(7)(E), Low (b)(2)



About ATS

The **About ATS** screen displays a warning message informing you of U.S. Customs and Border Protection's rights concerning your use of ATS-P (Passenger) and notifies you of the secure nature of the information within the ATS-P databases and penalties for violating system security.

High (b)(2), (b)(7)(E), Low (b)(2)



~~LAW ENFORCEMENT SENSITIVE~~

ATS-P (Passenger)

Chapter Four – Learning About ATS-P

This Page Left Blank.

~~LAW ENFORCEMENT SENSITIVE~~

003380

CHAPTER FIVE –THE ATS-P (PASSENGER) USER'S GUIDE

This chapter will review the following:

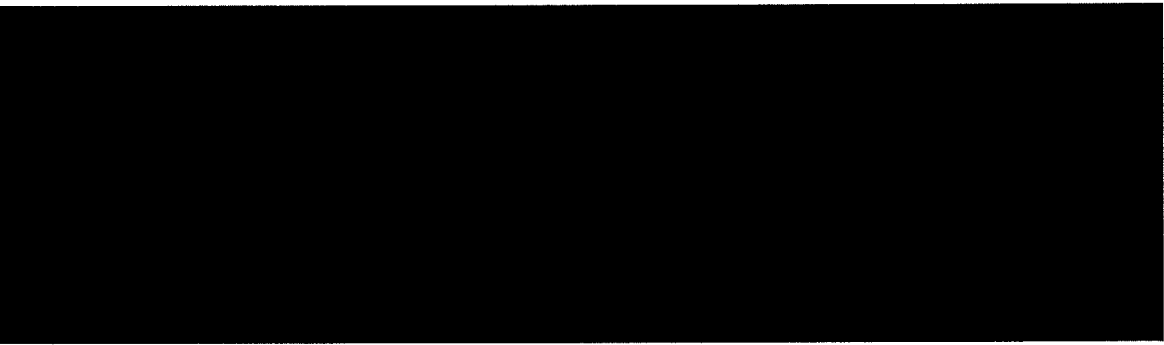

- > Logging on to ATS-P (Passenger) for the first time
- > Working with news items
- > Browsing ATS-P databases
- High (b)(2), (b)(7)(E), Low (b)(2)
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

This Page Left Blank.

CHAPTER FIVE – WORKING WITH THE PASSENGER MODULE

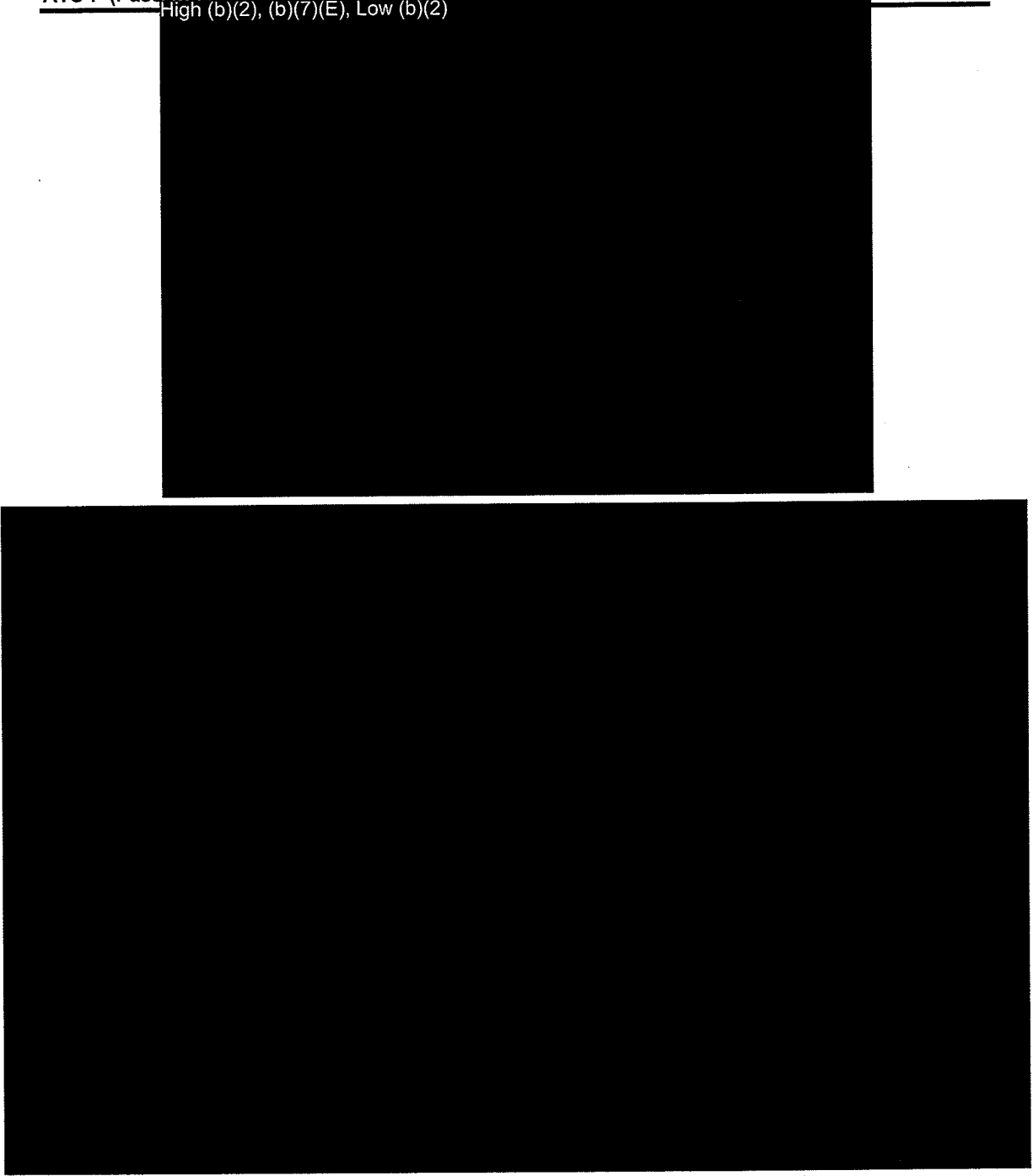
Logging on to ATS-P (Passenger) for the First Time

High (b)(2), (b)(7)(E), Low (b)(2)



~~LAW ENFORCEMENT SENSITIVE~~

High (b)(2), (b)(7)(E), Low (b)(2)




NOTE	High (b)(2), (b)(7)(E), Low (b)(2) <i>For more information on this screen, please refer to page 71 of this User's Guide.</i>
-------------	---

For more information, please refer to page 41 of this User's Guide.

Working with News Items





Creating a National or Local News Item from the Start Page

High (b)(2), (b)(7)(E), Low (b)(2)




From the **Start Page**, perform the following:

High (b)(2), (b)(7)(E), Low (b)(2)

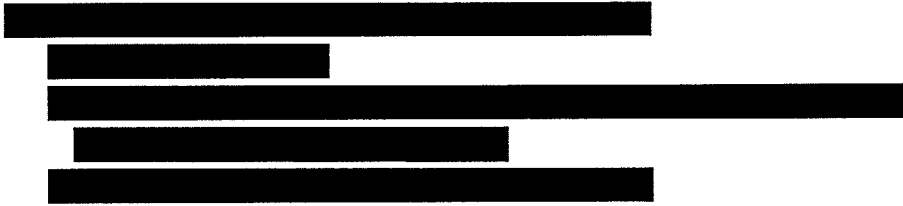
- i. For more information, please refer to page 406 of this User's Guide.

High (b)(2), (b)(7)(E), Low (b)(2)



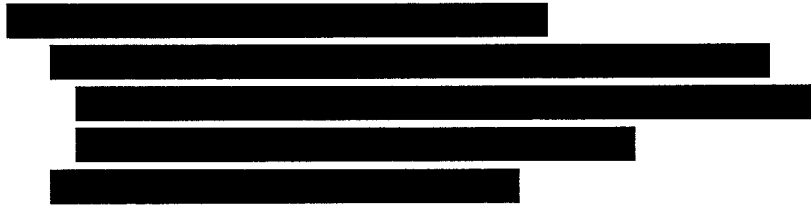
Creating a National or Local News Item from the Create Option

High (b)(2), (b)(7)(E), Low (b)(2)



a. For more information on this screen, please refer to page 406 of this User's Guide.

High (b)(2), (b)(7)(E), Low (b)(2)




LAW ENFORCEMENT SENSITIVE

ATS-P (Passenger)

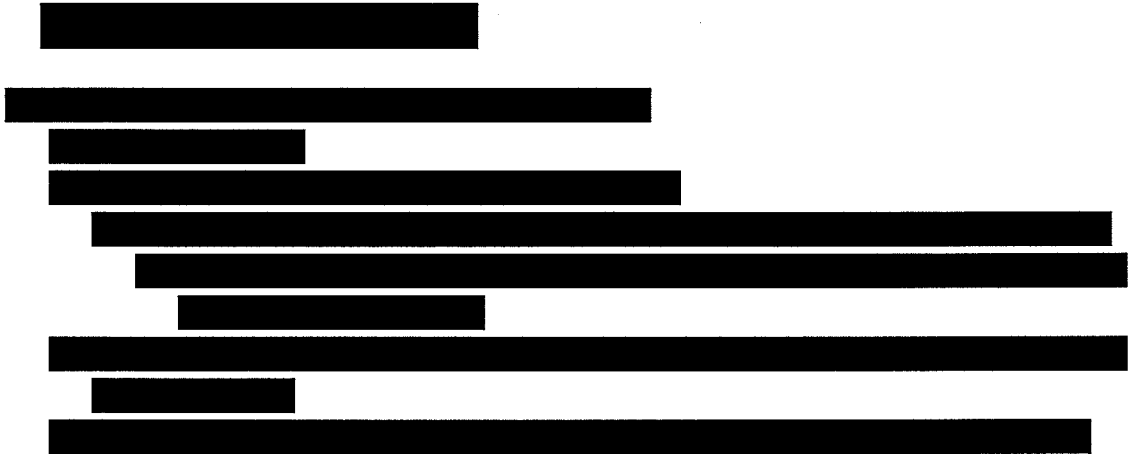
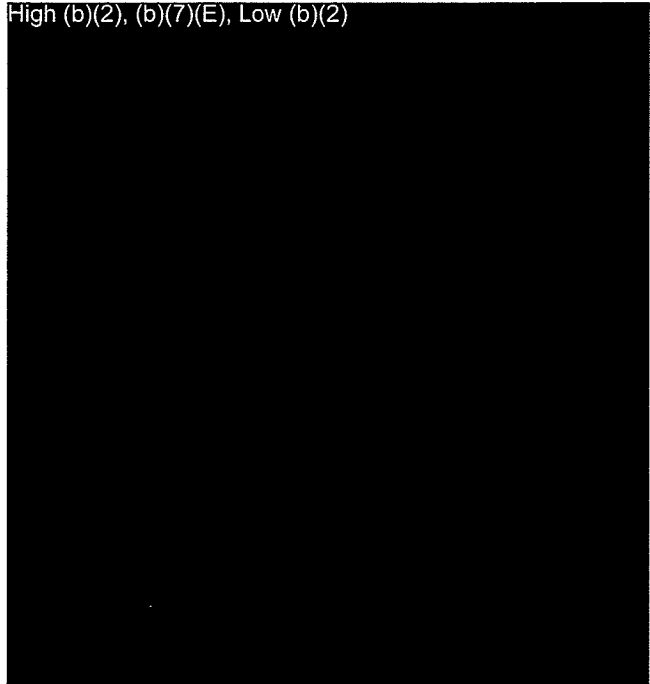
Chapter Five –The ATS-P (Passenger) User's Guide

High (b)(2), (b)(7)(E), Low (b)(2)



Browsing ATS-P Databases

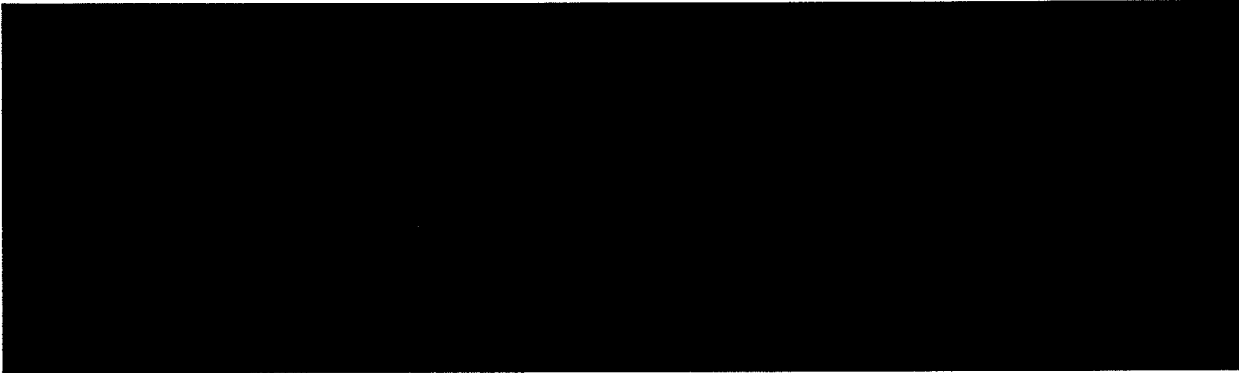

High (b)(2), (b)(7)(E), Low (b)(2)



For more information, please refer to page 179 of this User's Guide.

LAW ENFORCEMENT SENSITIVE

High (b)(2), (b)(7)(E), Low (b)(2)



High (b)(2), (b)(7)(E), Low (b)(2), (b)(6)



High (b)(2), (b)(7)(E), Low (b)(2)

NOTE [Redacted]

[Redacted]

[Redacted]

[Redacted]

For more information, please refer to page 424 of this User's Guide.

High (b)(2), (b)(7)(E), Low (b)(2)

High (b)(2), (b)(7)(E), Low (b)(2), (b)(6)



High (b)(2), (b)(7)(E), Low (b)(2)



High (b)(2), (b)(7)(E), Low (b)(2)



following: