



CARWASH SUMMARY REPORT

U.S. Department of Homeland Security (DHS)



Executive Summary

DHS Carwash provides static and dynamic security scanning for iOS and Android applications, leveraging open source, government-off-the-shelf, and commercial-off-the-shelf scanning systems to evaluate mobile applications based on aspects such as permissions, behaviors, networks, power consumption, and collusion. The information in this summary report is a highlight of results produced by multiple scanning tools and consolidated by a Carwash analyst. This information should not be used as a risk assessment of your application. Please work with your ISSO or information assurance team to provide a formal risk assessment based on the information in this report and the raw scan results provided to you.

Application Data

Application Name: Alerts

Package Name: com.java.ice

Platform(s): Android

Version: 2.0

Date of Scan: June 23, 2016

Carwash Scan Results

The information below is a summary of the results of the scanning tools we used.

Potential Issues – General

(b)(5);(b)(7)(E)



Carwash Summary Report

(b)(5);(b)(7)(E)

Permissions

Requested but not Used

(b)(5);(b)(7)(E)

Requests and Used

(b)(5);(b)(7)(E)

Network

Network Traffic

(b)(7)(E);(b)(5)



Carwash Summary Report

(b)(5),(b)(7)(E)

URLs

(b)(5),(b)(7)(E)



Carwash Summary Report

(b)(7)(E)

Note: The information in this summary report should not be used as a risk assessment of your application. Please work with your ISSO or information assurance team to provide a formal risk assessment.

Please let us know if you want to setup a call to discuss these findings or review any of the scan results. You can reach us at (b)(6);(b)(7)(C)



Mobile Threat Prevention

Logged in as: (b)(6);()
Logout (/login/logout)

- App Details
- Dashboard (/dashboard/index)
- Submit App (/submit/index)
- Gallery (/gallery/index)
- Settings (/settings/index)
- Filesystem (0)
- Network Traffic (14)
- About (/about/index)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Standard analysis Advanced analysis

Export results

App Details



Name: Alerts (com.java.ice)

Version: 2.0

Platform: Lollipop

Submitted on: 6/23/2016

Developer: U.S. Immigration and Customs Enforcement

Category: Books_And_Reference

Analysis SDK version: 21

FireEye Threat Score™

6 / 10

(b)(7)(E)

Threat Summary

Tip: Hover your mouse over a threat category to see more details.

Malware

- Developer certificate used to publish malware
- Behaviors match known malware
- Network traffic match to known malware
- Performs Masque attack
- Code matches known malware family
- Contains known invasive adware

SMS

- Sends confirmation message via SMS
- Sends premium SMS messages
- Monitors incoming SMS messages
- Deletes SMS messages
- Blocks incoming SMS messages
- Sends possibly-premium SMS messages
- Reads SMS messages
- Opens SMS compose window
- Sends spam SMS messages
- Modifies SMS messages
- Sends bulk SMS messages
- Sends SMS text messages
- Uploads SMS messages
- Sends SMS text messages directly
- Opens SMS compose window to shortcode

Telephony

- Terminates a phone call
- Opens phone dial window
- Makes phone call directly

Monitoring

- Monitors phone state
- Monitors phone call state
- Reads telephony state
- Bluetooth monitoring
- Monitors telephony state
- Monitors motion sensor

Accessing sensitive information

- Reads incoming/outgoing call's phone number
- Reads browser history
- Reads call log
- Reads audio and/or video
- Monitors GSM Location
- Modifies call log

© Copyright 2016 FireEye, Inc. All rights reserved.

App Details

Threat Summary (8)

Filesystem (0)

Network Traffic (14)

URLs (26)

Cloud Services (1)

Cryptography (0)

Permissions (17)

Library calls (333)

System calls (37,246)

Export results

Writes Passbook payment information	Modifies contacts
Modifies calendar	Modifies accounts
Modifies sensitive data	Reads list of installed apps
Modifies Passbook information	Access files on SD card
Reads list of running apps	Reads Passbook payment information
Records audio	Reads Apple identifier for vendor
Records video	Reads account information
Reads device identifier	Code to read GPS location
Reads contacts	Reads Apple unique device identifier
Reads list of running processes	Reads Apple advertising identifier
Reads device phone number	Reads location
Code to monitor GPS location	Reads calendar

Vulnerabilities

(b)(7)(E)

Exploits and obfuscation

Performs a permission-bypass exploit	Performs a root exploit
Performs a privilege-escalation exploit	Performs a code-signing exploit
Performs Fake ID signature exploit	Obfuscated method invocation
Obfuscated method names	Contains embedded app
Obfuscated file name	Malformed manifest
Contains embedded ELF file	Obfuscated method invocation
Loads native library at run-time	Loads Java class at run-time

Data upload

Uploads password to third-party server	Leaks sensitive data via SMS messages
Uploads contacts	Uploads calendar
Uploads audio/video recording	Uploads list of running apps

App Details

Threat Summary (8)

Filesystem (0)

Network Traffic (14)

URLs (26)

Cloud Services (1)

Cryptography (0)

Permissions (17)

Library calls (333)

System calls (37,246)

Export results

Uploads browser history

Listens on socket

Uploads device identifiers

Uploads list of installed apps

Uploads location

Uploads files from SD card

System and settings

Runs executable

Modifies telephony settings

Disables location updates

Modifies HTTP proxy settings

Modifies sideloading settings

Uses sysctl interface to kernel

Modifies Bluetooth settings

Executes shell commands

Modifies keyguard settings

Modifies device settings

Kills or restarts applications

Activates device administrator

Escalates privilege

Modifies shortcuts

Modifies debugging settings

Reads system logs

Modifies password settings

Requests to install an app

Modifies ringtone setting

Uses IOKit features

Developer reputation

Verified developer digital certificate

Developer certificate used to publish adware

Unverified digital certificate

Code features

Uses private Apple framework

Loads library bundle

Loads private framework

Permissions

Requests medium risk permission

Requests system permission

Requests risky permission

Filesystem

No filesystem accesses.

Network Traffic

Host	Location	Traffic	Ports	Alerts
(b)(7)(E)				

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

Host	Location	Traffic	Ports	Alerts
(b)(7)(E)				

URLs

(b)(7)(E)

Cloud Services

Social Networks

Facebook	Twitter
LinkedIn	Instagram
Google+	Pinterest

Cloud Storage

Google Drive	Dropbox
Microsoft OneDrive	Amazon Cloud Drive

Cloud Services

Amazon Cloud Services	Google Cloud Messaging
Google In-app Billing	

Cryptography

No use of cryptography observed.

Permissions

Permission name	Requested	Used	Description	Risk Level
(b)(7)(E)				

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

Permission name	Requested	Used	Description	Risk Level
(b)(7)(E)				

Library calls

#	Method
(b)(7)(E)	

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

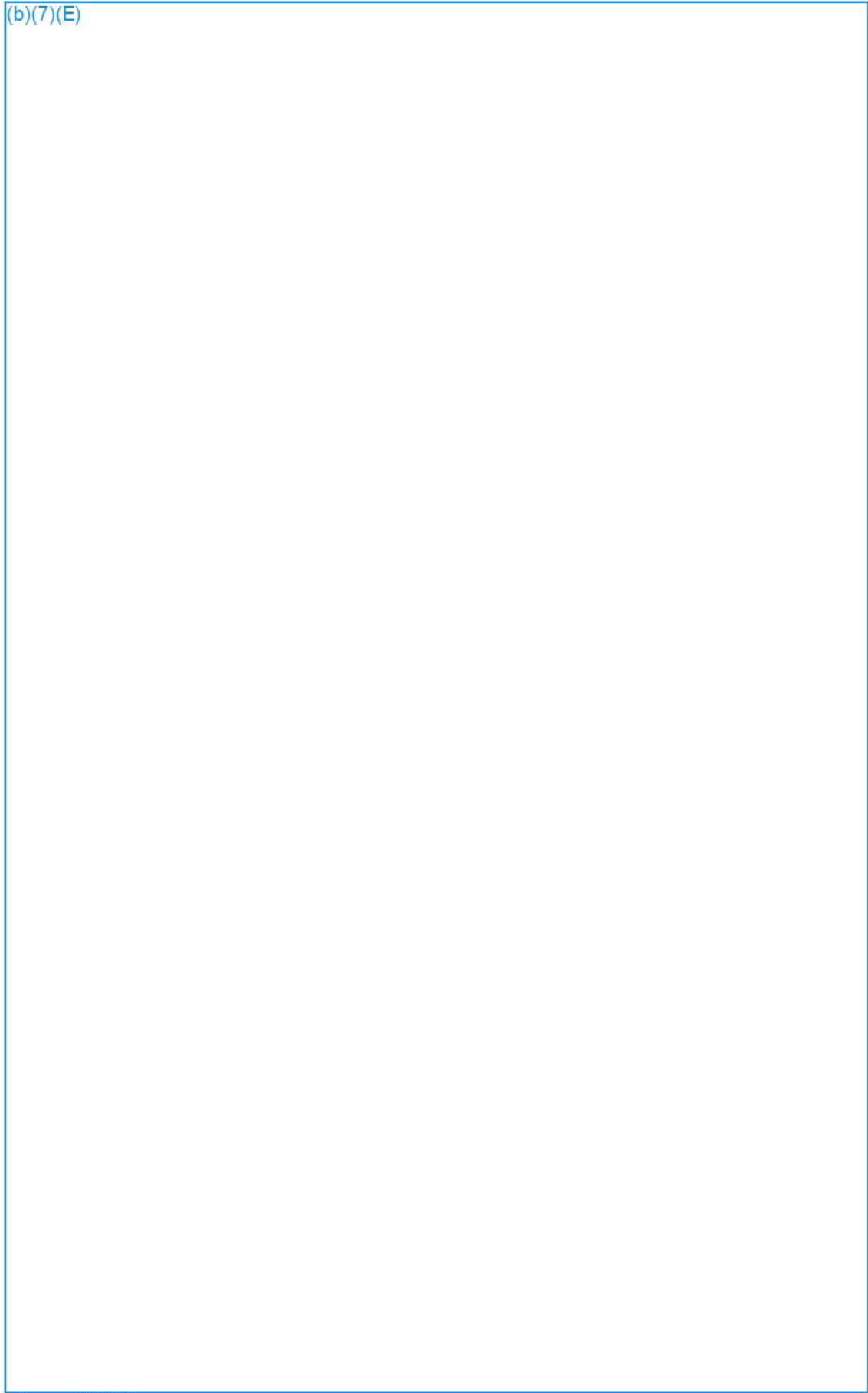
Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)



- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

(b)(7)(E)

83 more library calls (available in export)

System calls

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
 - Threat Summary (8)
 - Filesystem (0)
 - Network Traffic (14)
 - URLs (26)
 - Cloud Services (1)
 - Cryptography (0)
 - Permissions (17)
 - Library calls (333)
 - System calls (37,246)
- Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
 - Threat Summary (8)
 - Filesystem (0)
 - Network Traffic (14)
 - URLs (26)
 - Cloud Services (1)
 - Cryptography (0)
 - Permissions (17)
 - Library calls (333)
 - System calls (37,246)
- Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
 - Threat Summary (8)
 - Filesystem (0)
 - Network Traffic (14)
 - URLs (26)
 - Cloud Services (1)
 - Cryptography (0)
 - Permissions (17)
 - Library calls (333)
 - System calls (37,246)
- Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
 - Threat Summary (8)
 - Filesystem (0)
 - Network Traffic (14)
 - URLs (26)
 - Cloud Services (1)
 - Cryptography (0)
 - Permissions (17)
 - Library calls (333)
 - System calls (37,246)
- Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					

- App Details
- Threat Summary (8)
- Filesystem (0)
- Network Traffic (14)
- URLs (26)
- Cloud Services (1)
- Cryptography (0)
- Permissions (17)
- Library calls (333)
- System calls (37,246)

Export results

#	PID/TID	Process	Syscall	Return	Params
(b)(7)(E)					



Summary

Package Name: com.java.ice
Minimum SDK Version: 15
Target SDK Version: 22
Code Size: (b)(7)(E)
Lines of Code: 4 (b)(7)(E)
SHA1 CheckSum: (b)(7)(E)
App Version: 2.0

Vulnerability Summary

(b)(7)(E)

Permissions-Related Findings

Normal Permissions Requested

(b)(7)(E)

Dangerous Permissions Requested

(b)(7)(E)

Signature Permissions Requested

None

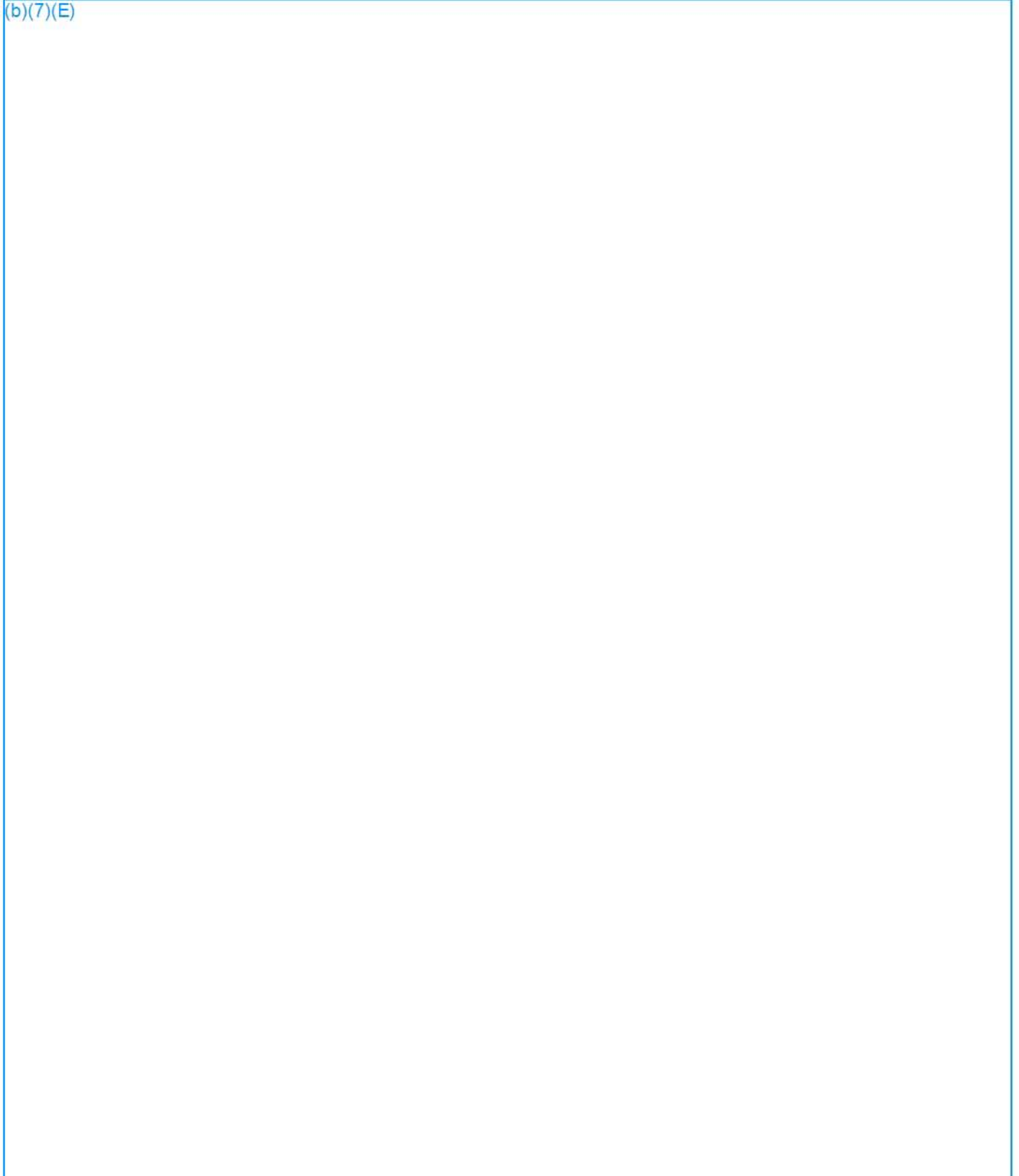
SignatureOrSystem Permissions Requested

None

Actual Permissions Required

ACCESS_NETWORK_STATE:

(b)(7)(E)



(b)(7)(E)



(b)(7)(E)

(b)(7)(E)



(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

Unnecessary Permissions Requested

(b)(7)(E)

Permissions not Requested but Needed

(b)(7)(E)

(b)(7)(E)

Created Permissions

(b)(7)(E)

Non-Library Permissions

(b)(7)(E)

Removed Permissions

(b)(7)(E)

Android Component Findings

Exported Activities with No Permissions

(b)(7)(E)

Exported Services with No Permissions

(b)(7)(E)

Exported Content Providers

None

Exported Broadcast Receivers

(b)(7)(E)

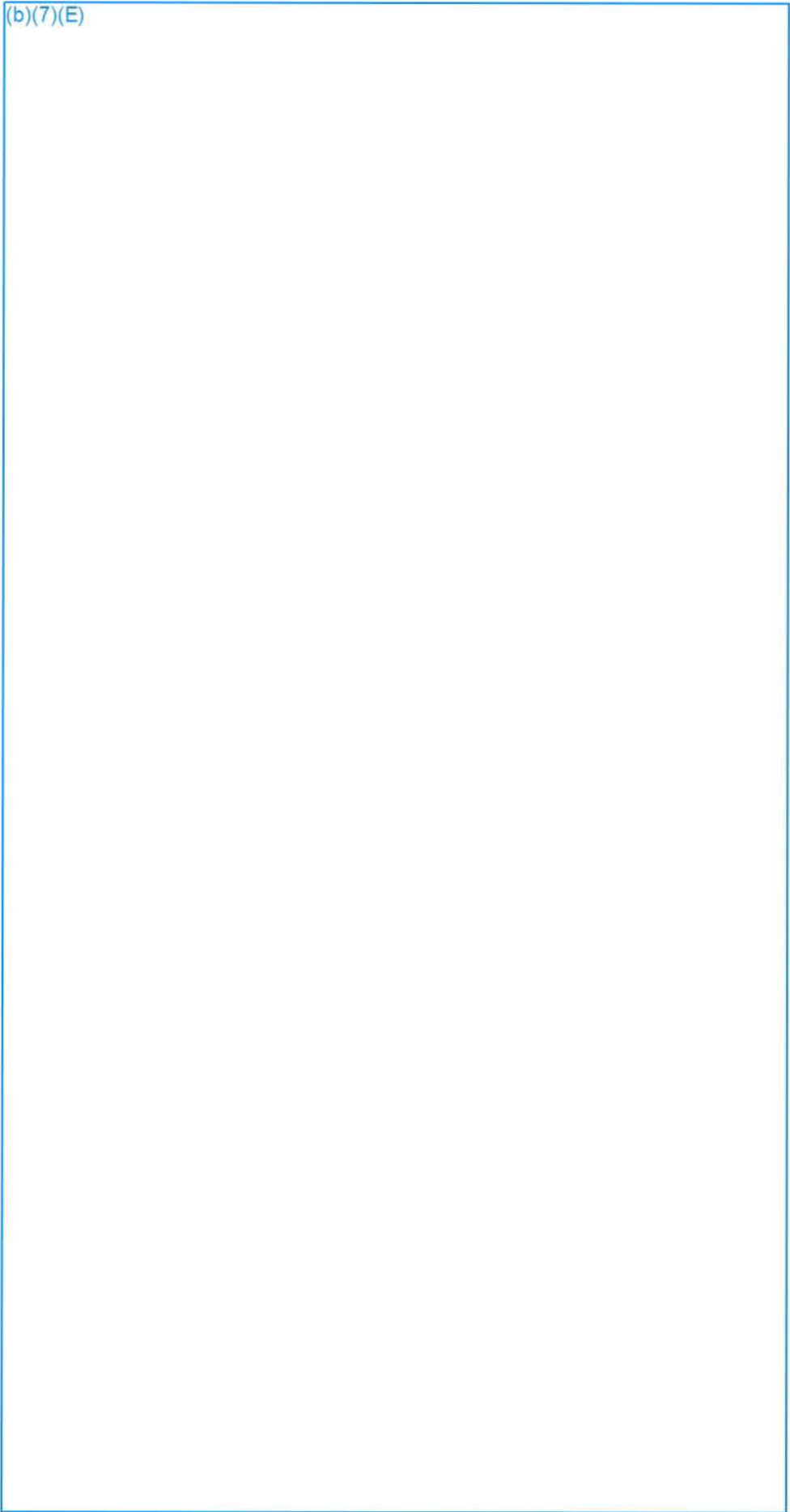
Debug Flag

Not Enabled

Intent Usage

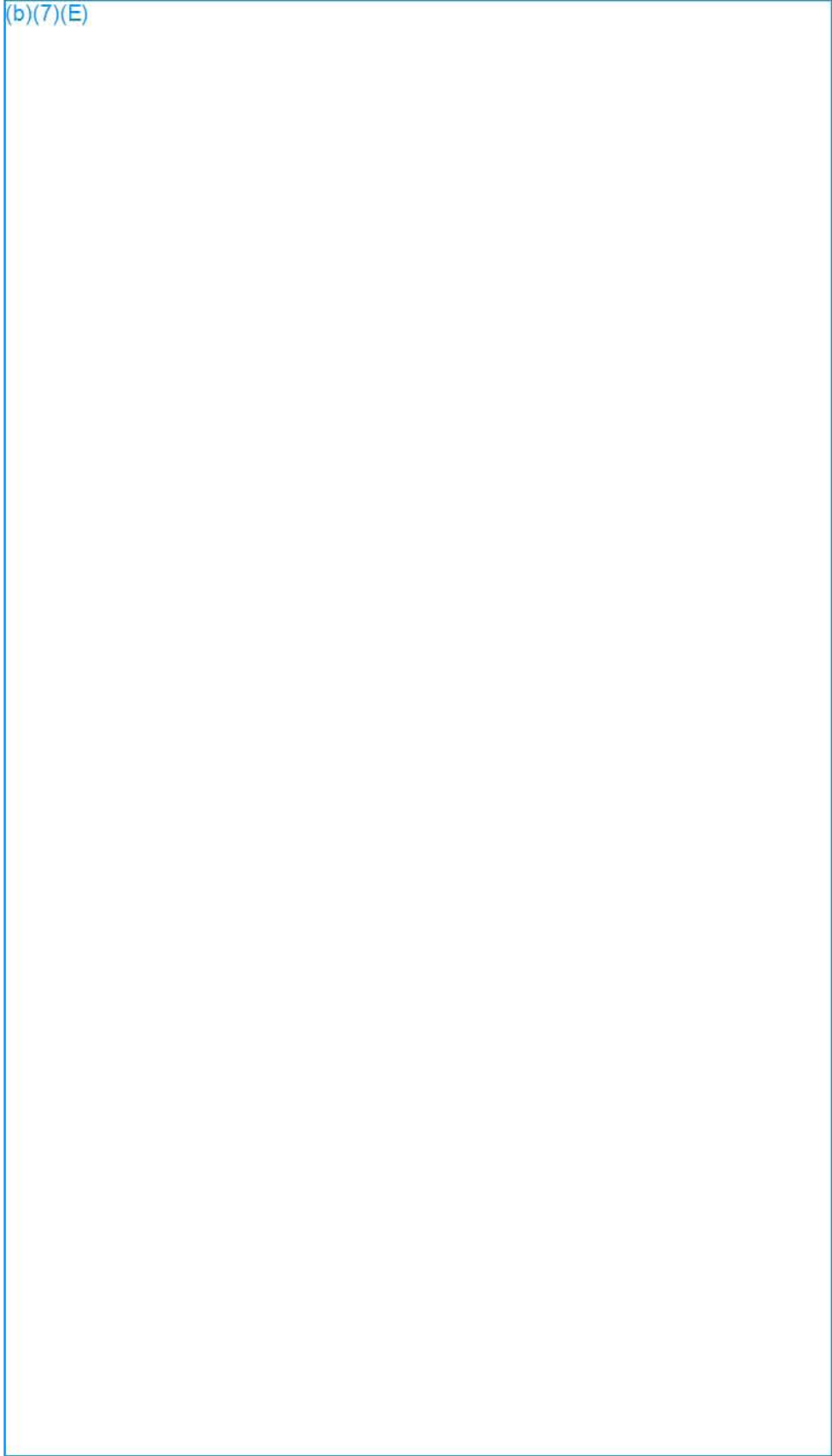
(b)(7)(E)

(b)(7)(E)

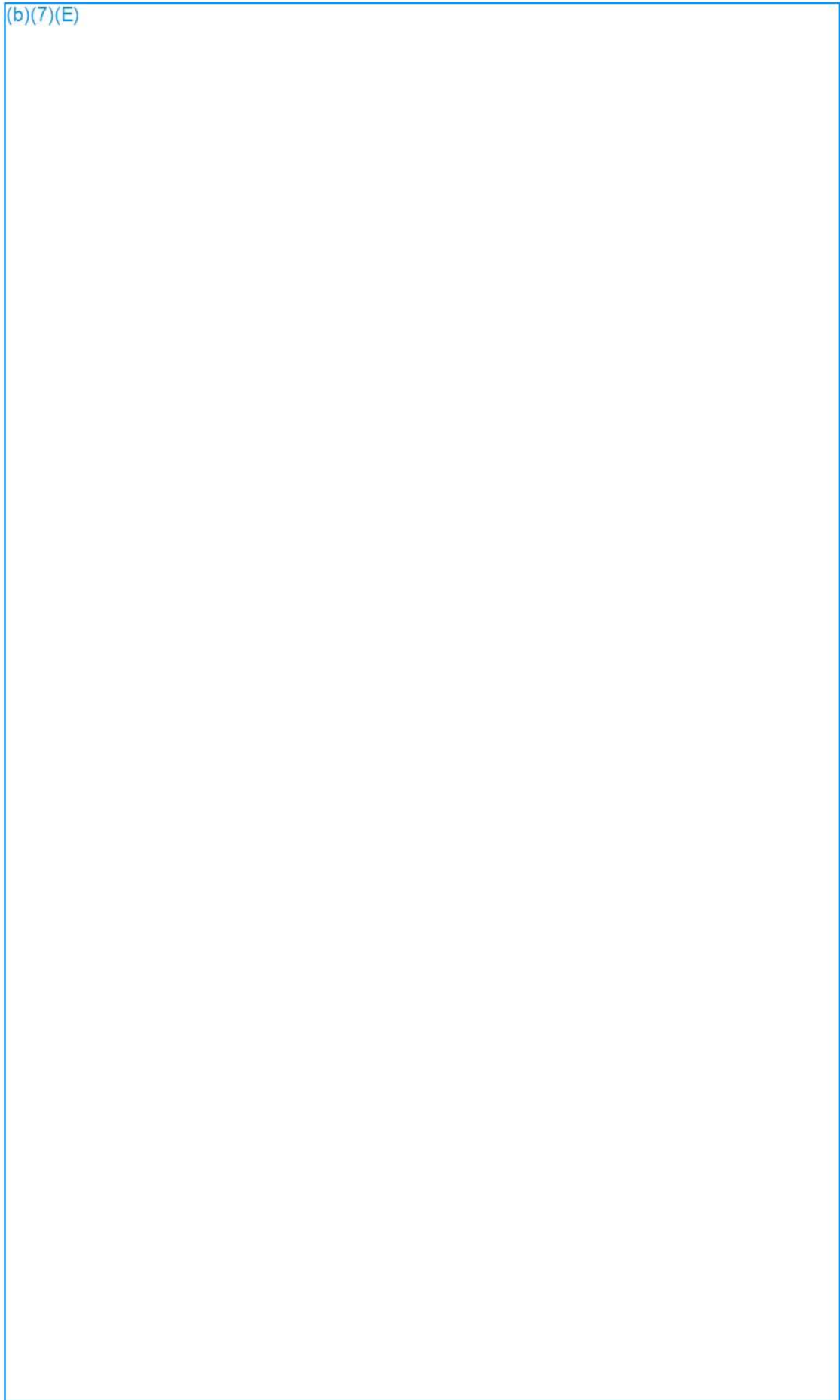


Function:Intent Sent to Activity

(b)(7)(E)



(b)(7)(E)



Function:Intent Sent to Activity

(b)(7)(E)

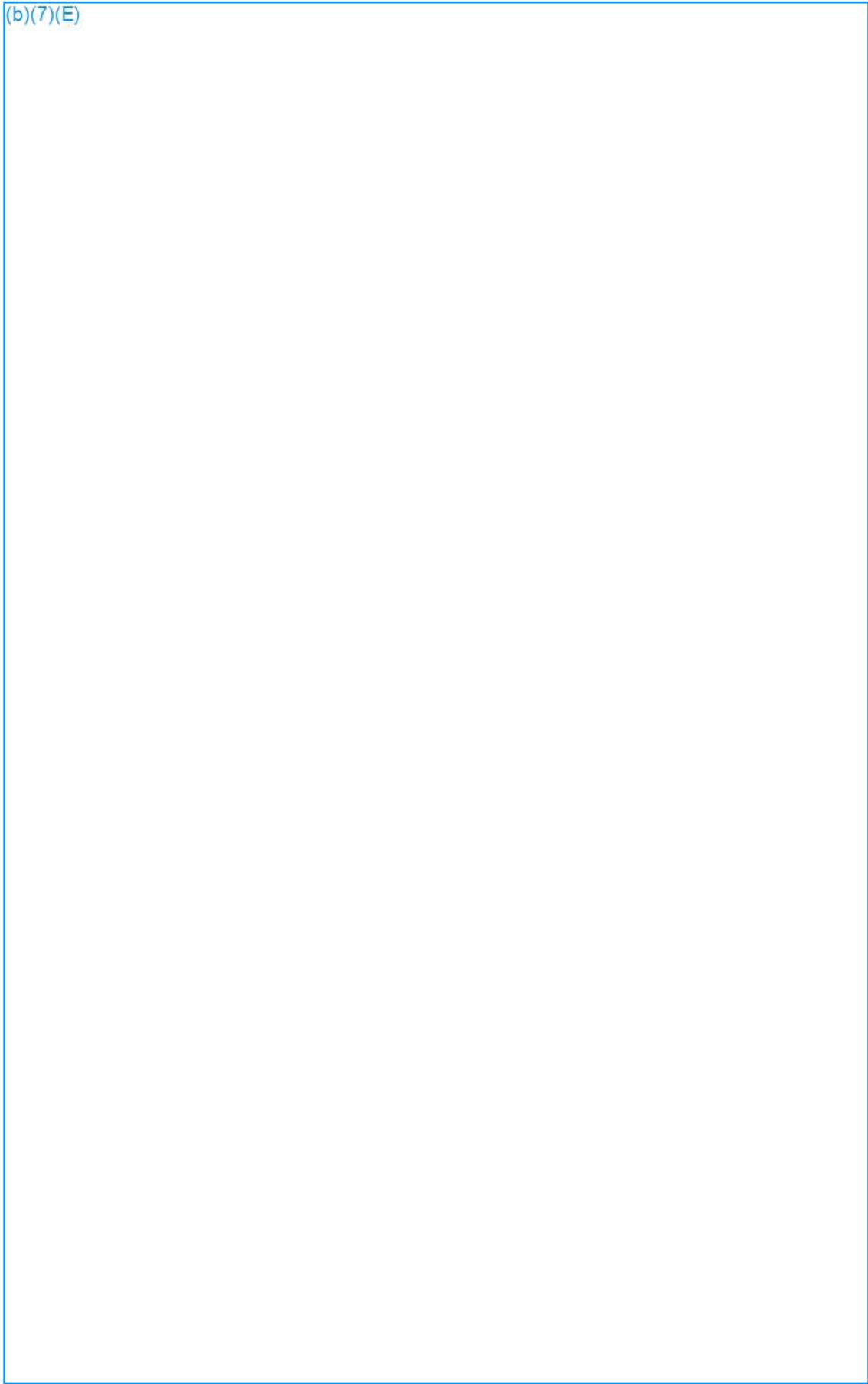


(b)(7)(E)

Use of Pending Intents

(b)(7)(E)

(b)(7)(E)

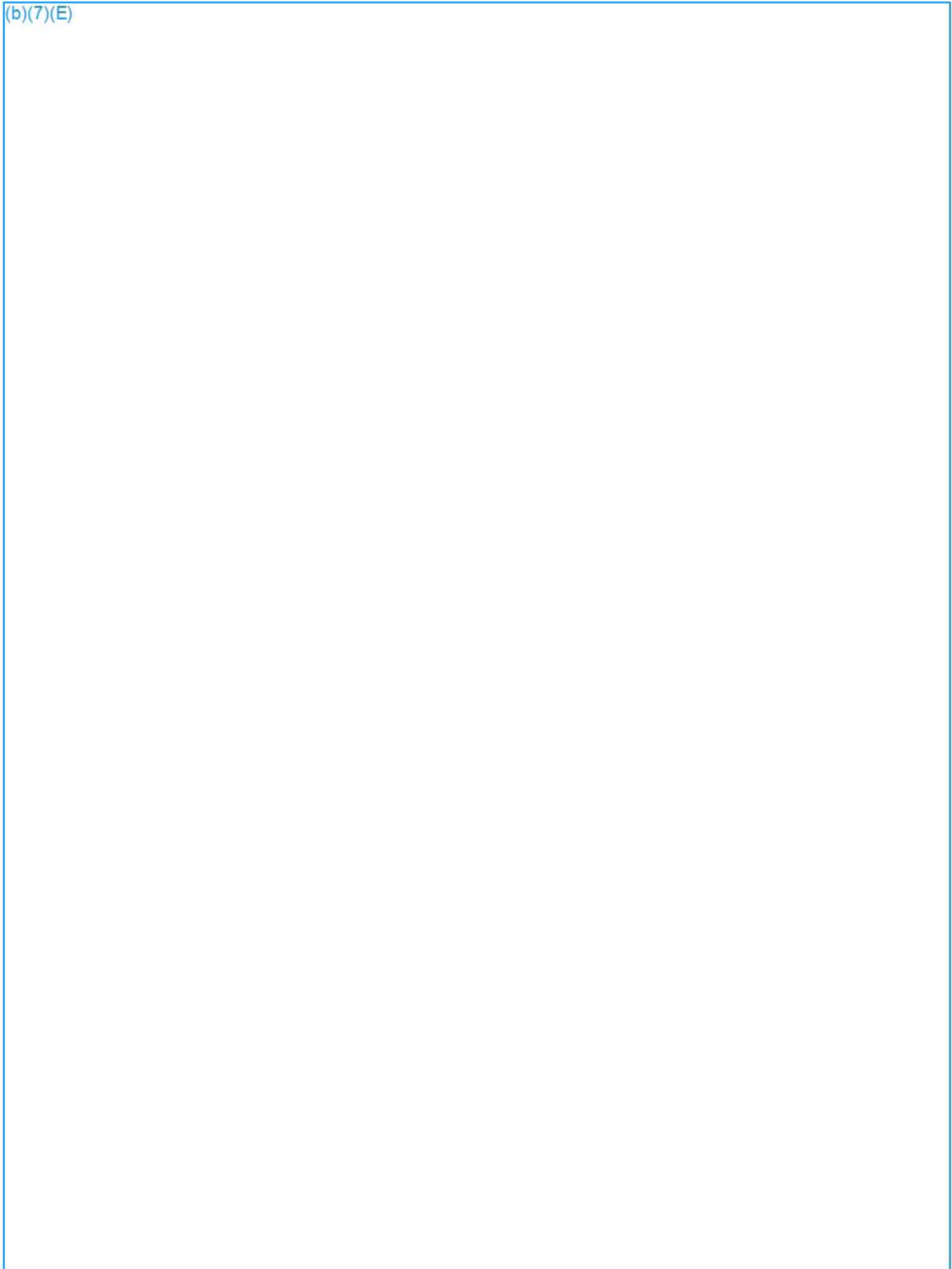


(b)(7)(E)

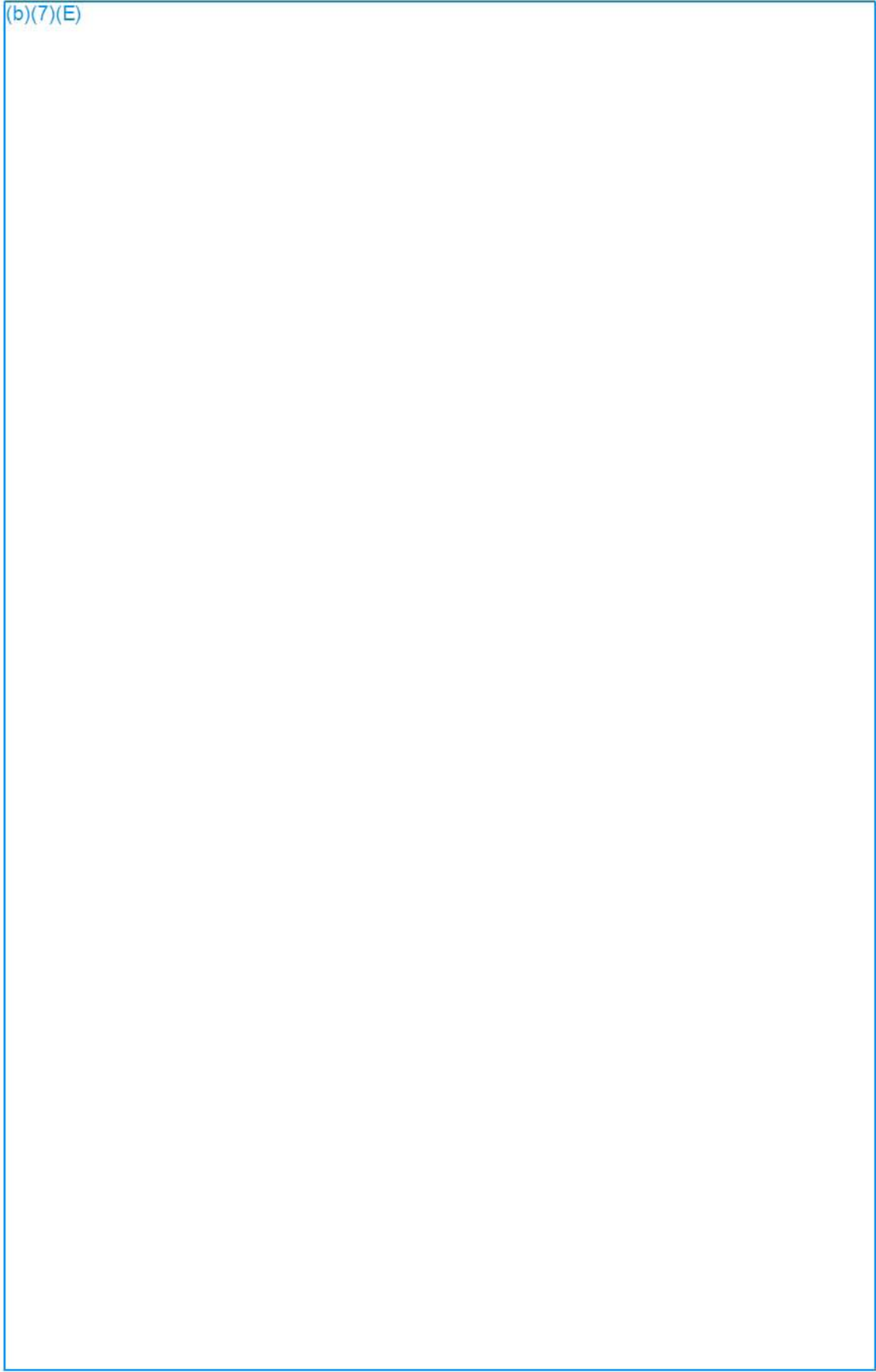
(b)(7)(E)

(b)(7)(E)

(b)(7)(E)



(b)(7)(E)

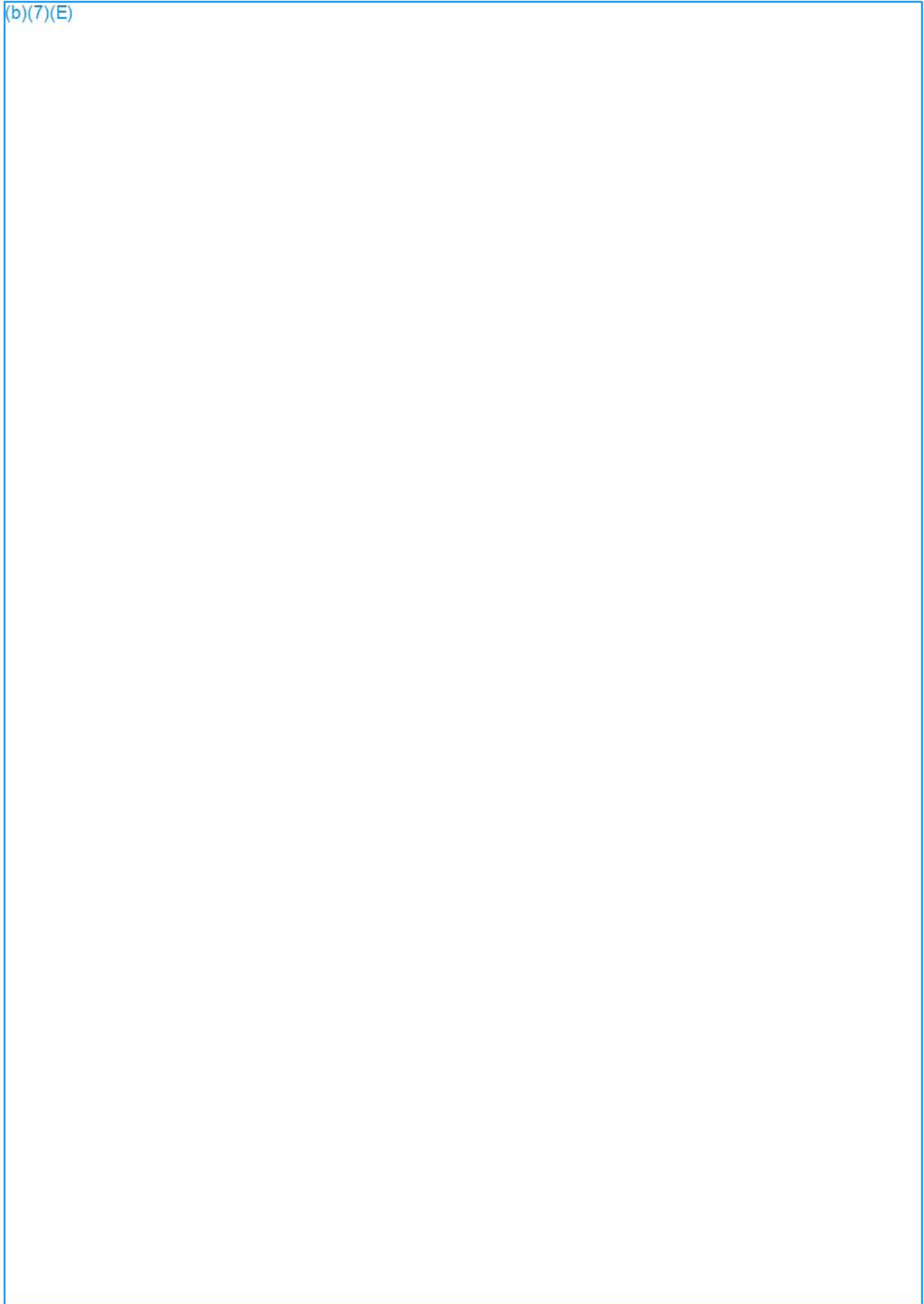


(b)(7)(E)

(b)(7)(E)

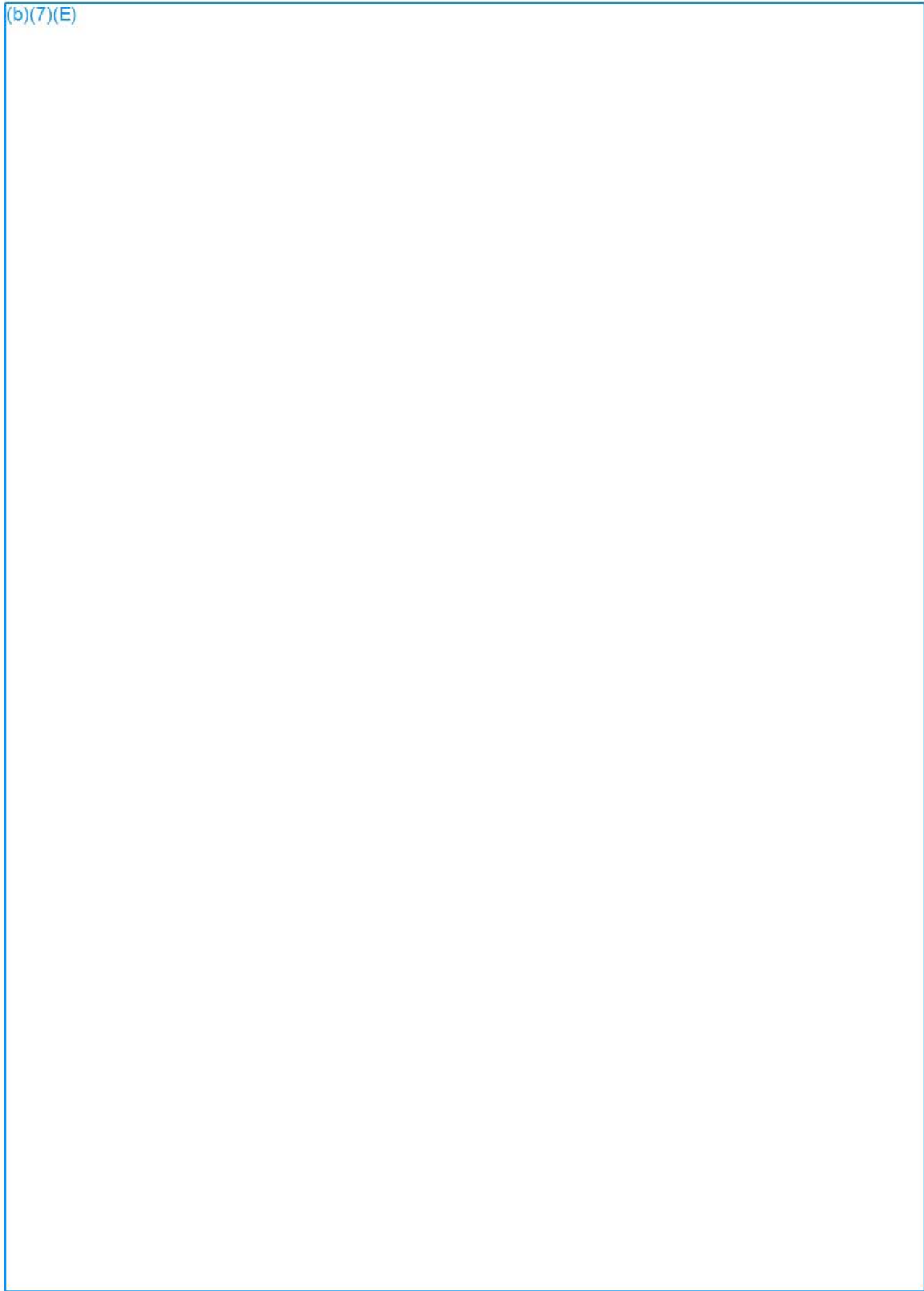


(b)(7)(E)



Line Number:24

(b)(7)(E)



(b)(7)(E)

Handled Intents (Not Called)

(b)(7)(E)

Called Intents (Not Handled)

(b)(7)(E)

Certificates and Crypto

Uses/Validates x509 Certs

No

Certificate Issues

None

Use of Crypto Algorithms

HMAC-SHA1
HmacSHA1

Use of Crypto APIs

None

Secure Random Number Generation

None

Cryptographic Key Pair Generation

None

Android Keystore Use

No

Communications

HTTPS Using RFC 2818

No

HTTPS Using TLS

No

SSL Issues

None

Opens JavaScript Bridge

yes

URLs Detected

(b)(7)(E)

FTP

No

Obfuscation/Packing/etc Findings

Packed With Proguard

No

Native Code Locations

None

Reflection

(b)(7)(E)

(b)(7)(E)

Library Calls

None

System-Level Behaviors

Changes to File Privileges

None

Access to Root

None

System Commands

None

Uses Java Classloader

yes

Uses Dex Classloader

no

Misc. Behaviors/Stats

PII Exposure

Device's Contacts

Cyclomatic Complexity

5

Downloads Supplemental .obb file

no

Masterkey Vulnerability

no

Configuration Options

(b)(7)(E)

Potentially Unwanted Functionality (Google Play Apps Only)

(b)(5)

(b)(5)

Probabilistic Metrics

Collusion

medium

Power Consumption

medium

Malware (Bayes)

No

**Privacy Policy
For the
[INSERT NAME] Mobile Application**

Overview

The overview should be a single paragraph that is used to describe the DHS Mobile Application (“DHS Mobile App”). It should include the name of the DHS component that developed the app as well as the name of the DHS Mobile App, itself. This overview should also provide a brief description of the DHS Mobile App’s purpose and function.

Information Collected

Provide the categories of individuals for whom information is collected, and for each category, list all information, including PII, SPII, and Sensitive Content that is collected by the DHS Mobile App. Details regarding the retention of information collected by the DHS Mobile App should also be addressed in this section.

Uses of Information

List each use (internal and external to the Department) of the information collected or maintained by the DHS Mobile App. Provide a detailed response that states how and why the different data elements is used.

Information Sharing

Discuss the external Departmental sharing of information (e.g., DHS to FBI). External sharing encompasses sharing with other federal, state and local government, and private sector entities.

Application Security

Discuss the technical safeguards and security controls, specific to the particular DHS Mobile App, in place to protect information that is collected and/or maintained by the DHS Mobile App.

How to Access or Correct your Information

Provide information about the processes in place for users of the DHS Mobile App to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

Analytics Tools

Discuss any analytics tools that the DHS Mobile App may use. This should include a description of any information collected through these analytic capabilities.

Privacy Policy Contact Information

Provide component privacy office contact information so that users may provide feedback and/or ask questions in regards to this DHS Mobile App Privacy Policy. This contact information may include the component privacy office’s phone number, email, and mailing address.

Department of Homeland Security
DHS Directives System
Instruction Number: 047-01-003
Revision Number: 00
Issue Date: March 30, 2016

I. Purpose

This Instruction implements the Department of Homeland Security (DHS or the Department) Directive 047-01, "Privacy Policy and Compliance," concerning DHS Mobile Applications intended for use by DHS employees and/or the public.

II. Scope

This Instruction applies throughout DHS for Mobile Applications that are developed by, on behalf of, or in coordination with the Department.

III. References

- A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note]
- B. Title 5, United States Code (U.S.C.), Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended]
- C. Title 6, U.S.C., Section 142, "Privacy officer"
- D. Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014 (FISMA)]
- E. Title 15 U.S.C., Chapter 91, "Children's Online Privacy Protection Act"
- F. Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information"
- G. DHS Directive 047-01, "Privacy Policy and Compliance" (July 25, 2011)
- H. DHS Sensitive Systems Policy Directive 4300A (March 14, 2011)
- I. DHS Privacy policy guidance and requirements issued (as updated) by the Chief Privacy Officer and published on the Privacy Office website, including:
 - 1. Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the

Department of Homeland Security (December 29, 2008)

2. Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments (December 30, 2008)

3. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS (March 2012)

IV. Definitions

A. **DHS Carwash** is the service sponsored by DHS Office of the Chief Information Officer (OCIO) that provides development teams with a continuous integration, build, test, source code management, and issue tracking environment for building DHS Mobile Apps. The shared platform provides application lifecycle management and support for mobile apps built on development frameworks. The DHS Carwash also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility.

B. **DHS Mobile Application (DHS Mobile App)** means a native software application that is developed by, on behalf of, or in coordination with DHS for use on a mobile device (e.g., phone or tablet) by DHS employees and/or the public.

C. **Fair Information Practice Principles** means the policy framework adopted by the Department in Directive 047-01, Privacy Policy and Compliance, regarding the collection, use, maintenance, disclosure, deletion, or destruction of Personally Identifiable Information, and as described in Privacy Policy Guidance Memorandum 2008-01.

D. **Location Information** means the ability of a mobile device to know a user's current location and/or location history as determined by Global Positioning System (GPS) and/or other methods.

E. **Metadata** means the information stored as the description of a unique piece of data and all the properties associated with it. For example, mobile device metadata may include the time and duration of all phone calls made from a particular mobile device, the mobile device IDs of the mobile devices involved in the phone calls, and the locations of each participant when the phone calls occurred.

F. **Mobile Device ID** means a unique serial number that is specific to a mobile device. These numbers vary in permanence, but typically a device has at least one permanent number. These numbers are used for various purposes, such as for security and fraud detection and remembering user preferences. Combining a unique device identifier with other information, such as location data, can allow the phone to be used as a tracking device.

G. **Personally Identifiable Information (PII)** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

For example, when linked or linkable to an individual, such information may include a name, Social Security number, date and place of birth, mother's maiden name, Alien Registration Number, account number, license number, vehicle identifier number, license plate number, biometric identifier (e.g., facial recognition, photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

H. **Privacy Compliance Documentation** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for Exemption from certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

I. **Privacy Compliance Review (PCR)** means both the DHS Privacy Office process to be followed and the document designed to provide a constructive mechanism to improve a DHS program's ability to comply with assurances made in existing Privacy Compliance Documentation including Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreement.

J. **Privacy Impact Assessment (PIA)** means both the DHS Privacy Office process to be followed and the document required whenever an information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer. A PIA describes what information DHS is collecting, why the information is being collected, how the information are used, stored, and shared, how the information may be accessed, how the information is protected from unauthorized use or disclosure, and how long it is retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may, in coordination with the affected component and the Office of the General Counsel,

modify or waive publication for security reasons, or to protect classified, sensitive, or private information included in a PIA.

K. **Privacy Threshold Analysis (PTA)** means both the DHS Privacy Office process to be followed and the document used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the proposed use, identifies the legal authorities for the proposed use, and describes what PII, if any, is collected (and from whom) and how that information is used. PTAs are adjudicated by the Chief Privacy Officer.

L. **Program Manager** means the responsible agency representative, who, with significant discretionary authority, is uniquely empowered to make final scope-of-work, capital investment, and performance acceptability decisions.

M. **Sensitive Content** means information that may not be PII, but raises privacy concerns because it may be related to the use of PII (e.g., location information, mobile device ID, or metadata).

N. **Sensitive Personally Identifiable Information (SPII)** means PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some types of PII, such as Social Security Number (SSNs), Alien Registration Number, and biometric identifiers, are always sensitive. Other types of PII, such as an individual's driver's license number, financial account number, citizenship or immigration status, or medical information are SPII if DHS maintains them in conjunction with other identifying information about the individual. In some instances the context surrounding the PII may determine whether it is sensitive. For example, a list of employee names by itself may not be SPII, but could be if it is a list of employees who received poor performance ratings.

O. **System Manager** means the individual identified in a System of Records Notice who is responsible for the operation and management of the system of records to which the System of Records Notice pertains.

P. **System of Records Notice (SORN)** means the statement providing the public notice of the existence and character of a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system are included.

Q. **User** means a person using a DHS Mobile App.

V. Responsibilities

- A. The **Chief Privacy Officer** is responsible for:
1. Working with Component Privacy Officers and Privacy Points of Contact (PPOCs) to provide guidance and ensure that DHS Mobile Apps are in compliance with DHS privacy policies;
 2. Reviewing and approving Privacy Compliance Documentation for DHS Mobile Apps, as appropriate; and
 3. Performing periodic PCRs of DHS Mobile Apps to ascertain compliance with DHS privacy policy.
- B. The **Chief Information Officer** is responsible for:
1. Providing web technology services, security, and technical assistance for the development of DHS Mobile Apps;
 2. Ensuring that DHS Mobile Apps comply with FISMA and DHS Sensitive Systems Policy Directive 4300A; and
 3. Performing iterative scans and tests on the source code of DHS Mobile Apps through the DHS Carwash process in order to provide insight on code security, quality, and accessibility.
- C. **Component Privacy Officers** are responsible for:
1. Coordinating with Program Managers or System Managers, as appropriate, together with the Chief Privacy Officer and counsel to complete Privacy Compliance Documentation, as necessary, for all proposed DHS Mobile Apps; and
 2. Collaborating with the Chief Privacy Officer in conducting Privacy Compliance Reviews.
- D. **Privacy Points of Contact (PPOCs)** are responsible for assuming the duties of Component Privacy Officers in Components that do not have Privacy Officers.

E. **Program Managers, or System Managers**, as appropriate, are responsible for:

1. Coordinating with the Component Privacy Officer or PPOC to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any DHS Mobile Apps;
2. Engaging and coordinating with the OCIO Carwash team to ensure that DHS Mobile Apps are sent through DHS Carwash process when proposing, developing, implementing or changing any DHS Mobile Apps;
3. Coordinating with the Component Privacy Officer or PPOC and counsel to prepare drafts of all Privacy Compliance Documentation, as necessary, when proposing, developing, implementing, or changing any DHS Mobile Apps;
4. Monitoring the design, deployment, operation, and retirement of DHS Mobile Apps to ensure that the collection and use of PII and Sensitive Content, if any, is limited to what is described in the Privacy Compliance Documentation; and
5. Coordinating with the Component Privacy Officer or PPOC and the DHS Office for Civil Rights and Civil Liberties to establish administrative, technical, and physical controls for storing and safeguarding PII and Sensitive Content consistent with DHS privacy, security, and records management requirements to ensure the protection of PII and Sensitive Content from unauthorized access, disclosure, or destruction as it relates to DHS Mobile Apps.

VI. Content and Procedures

A. **Minimum Privacy Requirements for DHS Mobile Apps**: The policies detailed below provide the baseline privacy requirements for DHS Mobile Apps. Additional privacy protections may be necessary depending on the purpose and capabilities of each individual mobile app.

1. Provide Notice
 - a. **App-Specific Privacy Policy (see Appendix A)**: DHS Mobile Apps have a Privacy Policy that is easily accessible to users through the commercial app store before installation as well as within the app, itself, after installation. This Privacy Policy should be app-specific and cannot merely reference the DHS website Privacy Policy.

The Privacy Policy should briefly describe the app's information practices to include the collection, use, sharing, disclosure, and retention of PII, SPII, and Sensitive Content. The Privacy Policy should also address: redress procedures, app security, and the Children's Online Privacy Protection Act (if applicable).

b. Privacy Statement: If a DHS Mobile App is collecting PII from users, then a Privacy Statement is provided at the point of collection. This Privacy Statement may be provided through a pop-up notification on the DHS Mobile App screens where PII is collected or via another mechanism approved by the Chief Privacy Officer.

c. Contextual Notice: DHS Mobile Apps deliver direct, contextual, self-contained notice about the uses of information through the mobile platform. Therefore, these notices should be:

(1) Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app;

(2) Provided as "just-in-time" disclosures and obtain users' affirmative express consent before a DHS Mobile App accesses Sensitive Content or other tools and applications on the mobile device for the first time (e.g., location services); and

(3) Provided with independent opt-out features so that users may customize the mobile app's features (e.g., opting out of location based services, while still choosing to utilize other app services), where appropriate.

2. Limit the Collection and/or Use of Sensitive Content

a. DHS Mobile App features cannot collect and/or use PII, SPII, or Sensitive Content, unless directly needed to achieve a DHS mission purpose; and

b. If the collection and/or use of PII, SPII, or Sensitive Content is directly necessary to achieve a DHS mission purpose, then the collection and/or use of the information is documented and justified in the mobile app's Privacy Compliance Documentation.

3. Establish Guidelines for User Submitted Information
 - a. Where feasible, use forms and check boxes to limit data collection and minimize data entry errors;
 - b. Before allowing a user to submit information to DHS, provide a “review before sending” function that allows users to correct or opt-out of sending their information to the Department; and
 - c. Unless necessary to achieve a DHS mission purpose, limit the ability of users to post information within the app that other users may access or view. This limits the potential for users to share PII, SPII, or Sensitive Content unnecessarily.
4. Ensure Mobile App Security and Privacy
 - a. Engage with the DHS Carwash throughout development to ensure the security and privacy of the mobile app;
 - b. If users submit information through a DHS Mobile App, that information is encrypted in transit and immediately transferred to a protected internal DHS system that is compliant with existing DHS IT security policy; and
 - c. Sensitive content that a DHS Mobile App accesses or uses for the benefit of the user, but that DHS does not need to collect (e.g., location information), should be locally stored within the mobile app or mobile device. This information should not be transmitted to or shared with DHS.

B. DHS Mobile App Development:

1. Program Managers and System Managers notify their Component Privacy Officers or PPOCs and the OCIO Carwash team before engaging in the development of a DHS Mobile App.
2. Component Privacy Officers or PPOCs engage with Program Managers and System Managers to ensure privacy protections outlined in Section VI. A. of this document are integrated into the development of the DHS Mobile App.
3. Before deployment, the DHS Mobile App goes through the DHS Carwash.
4. The OCIO Carwash team provides the iterative scan results of the DHS Carwash to the Program Managers and System Managers.

5. Before deployment, Program Managers and System Managers in consultation with Component Privacy Officers or PPOCs complete a PTA, an App-Specific Privacy Policy, and a Privacy Statement (if necessary) for the DHS Mobile App. The PTA (a) documents a general description of the proposed use, (b) identifies the legal authorities for the proposed use and (c) describes what PII, if any, is collected, from whom PII is collected and how the PII is used. Component Privacy Officers or PPOCs compare this PTA to the DHS Carwash iterative scan results to ensure the PTA accurately describes the DHS Mobile App's collection, use, maintenance, retention, disclosure, deletion and destruction of PII, SPII, and Sensitive Content.

6. Before deployment, the DHS Mobile App's PTA, App-Specific Privacy Policy, Privacy Statement (if necessary), and results of the DHS Carwash iterative scans are submitted to the Chief Privacy Officer for a prompt review and evaluation to determine whether the DHS Mobile App contains appropriate privacy protections and whether a new or updated PIA, SORN, or other Privacy Compliance Documentation is required.

7. Once it is determined that all necessary Privacy Compliance Documentation is complete and that the DHS Mobile App contains appropriate privacy protections, the Chief Privacy Officer provides approval for the release of the DHS Mobile App.

8. DHS Mobile Apps go through the DHS Carwash any time there is a change made to the DHS Mobile App that affects or potentially affects the collection and use of PII, SPII, or Sensitive Content and consistent with the PTA review cycle. Existing DHS Mobile Apps, which were developed before the implementation of this policy, go through the DHS Carwash within 6 months of this policy's issue date. Program Managers and System Managers provide the DHS Carwash results, pertaining to their particular DHS Mobile App, to the Chief Privacy Officer for a prompt review and evaluation to ensure that the DHS Mobile App continues to contain appropriate privacy protections.

C. **Retention of PII:** Component Program Managers or System Managers, where appropriate, maintain PII collected through DHS Mobile Apps in accordance with approved records retention schedules.

D. **Privacy Compliance Reviews (PCR):** The Chief Privacy Officer, in collaboration with Component Privacy Officers or PPOCs, may conduct PCRs of DHS Mobile Apps periodically, at the sole discretion of the Chief Privacy Officer, to ascertain compliance with DHS privacy policy.

VII. Questions

Address any questions or concerns regarding these Instructions to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.



Karen L. Neuman
Chief Privacy Officer

March 30, 2016

Date

Privacy Policy
For the
[INSERT NAME] Mobile Application

Overview

The overview should be a single paragraph that is used to describe the DHS Mobile Application (“DHS Mobile App”). It should include the name of the DHS component that developed the app as well as the name of the DHS Mobile App, itself. This overview should also provide a brief description of the DHS Mobile App’s purpose and function.

Information Collected

Provide the categories of individuals for whom information is collected, and for each category, list all information, including PII, SPII, and Sensitive Content that is collected by the DHS Mobile App. Details regarding the retention of information collected by the DHS Mobile App should also be addressed in this section.

Uses of Information

List each use (internal and external to the Department) of the information collected or maintained by the DHS Mobile App. Provide a detailed response that states how and why the different data elements is used.

Information Sharing

Discuss the external Departmental sharing of information (e.g., DHS to FBI). External sharing encompasses sharing with other federal, state and local government, and private sector entities.

Application Security

Discuss the technical safeguards and security controls, specific to the particular DHS Mobile App, in place to protect information that is collected and/or maintained by the DHS Mobile App.

How to Access or Correct your Information

Provide information about the processes in place for users of the DHS Mobile App to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

Analytics Tools

Discuss any analytics tools that the DHS Mobile App may use. This should include a description of any information collected through these analytic capabilities.

Privacy Policy Contact Information

Provide component privacy office contact information so that users may provide feedback and/or ask questions in regards to this DHS Mobile App Privacy Policy. This contact information may include the component privacy office’s phone number, email, and mailing address.

Page 550

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 551

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 552

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 553

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 554

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 555

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 556

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 557

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 558

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 559

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 560

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 561

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 562

Withheld pursuant to exemption

Referred to Another Agency/Component

of the Freedom of Information and Privacy Act

Page 563

Withheld pursuant to exemption

Referred to Another Agency/Component

of the Freedom of Information and Privacy Act

Page 564

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 565

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 566

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 567

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 568

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 569

Withheld pursuant to exemption

Referred to Another Agency/Component
of the Freedom of Information and Privacy Act

Page 570

Withheld pursuant to exemption
Referred to Another Agency/Component
of the Freedom of Information and Privacy Act



PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Senior Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSCconnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	ICE Tactical Communications		
Component:	Office of the Chief Information Officer (OCIO)	Office or Program:	Operations
TAFISMA Name:	P25 Land Mobile Radio	TAFISMA Number:	ICE-06568-MAJ-06568
Type of Project or Program:	IT System	Project or program status:	Development

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	Tactical Communications Program	Title:	Chief, Tactical Communications Program
Phone:	202-732-(b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	(b)(6);(b)(7)(C)		
Phone:	202-732-(b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

ROUTING INFORMATION

Date submitted to Component Privacy Office:	Click here to enter a date.
Date submitted to DHS Privacy Office:	Click here to enter a date.
Date approved by DHS Privacy Office:	Click here to enter a date.



SPECIFIC PTA QUESTIONS

1. Please describe the purpose of the project or program:

Please provide a general description of the project and its purpose in a way a non-technical person could understand.

(b)(5)

[Redacted area]



2. Project or Program status		Existing	
Date first developed:	FY 2009	Pilot launch date:	Click here to enter a date.
Date last updated:	FY 2014	Pilot end date:	Click here to enter a date.

<p>3. From whom does the Project or Program collect, maintain, use or disseminate information? <i>Please check all that apply.</i></p>	<input type="checkbox"/> DHS Employees <input type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Members of the public <input checked="" type="checkbox"/> This program does not collect any personally identifiable information ¹
---	---

<p>4. What specific information about individuals could be collected, generated or retained? <i>Please provide a specific description of information that might be collected, generated or retained such as names, addresses, emails, etc.</i></p>	
N/A	
Does the Project or Program use Social Security Numbers (SSNs)?	No
If yes, please provide the legal authority for the collection of SSNs:	Click here to enter text.
If yes, please describe the uses of the SSNs within the Project or Program:	Click here to enter text.

<p>5. Does this system employ any of the following technologies:</p>	<input type="checkbox"/> Closed Circuit Television (CCTV) <input type="checkbox"/> Sharepoint-as-a-Service
---	---

¹ DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



<i>If project or program utilizes any of these technologies, please contact Component Privacy Officer for specialized PTA.</i>	<input type="checkbox"/> Social Media <input type="checkbox"/> Mobile Application (or GPS) <input type="checkbox"/> Web portal ² <input checked="" type="checkbox"/> None of the above
If this project is a technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input type="checkbox"/> No. Please continue to next question. <input checked="" type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.	
No log is kept.	

6. Does this project or program connect, receive, or share PII with any other DHS programs or systems⁴?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: Click here to enter text.
7. Does this project or program connect, receive, or share PII with any external (non-DHS) partners or systems?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: Click here to enter text.
Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. Please describe applicable information sharing governance in place. Click here to enter text.

² Informational and collaboration-based portals in operation at DHS and its components which collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are “members” of the portal or who seek to gain access to the portal “potential members.”

³ When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

⁴ PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as “interconnected systems” in TAFISMA.



**Homeland
Security**

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: July 7, 2012
Page 6 of 8



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Paul Simonoff
Date submitted to DHS Privacy Office:	September 3, 2015
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b)(5)	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Lindsay Lennon
Date approved by DHS Privacy Office:	September 3, 2015
PCTS Workflow Number:	1105452

DESIGNATION

Privacy Sensitive System:	No If "no" PTA adjudication is complete.
Category of System:	Choose an item. If "other" is selected, please describe: Click here to enter text.
Determination:	<input checked="" type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input type="checkbox"/> Privacy Impact Assessment (PIA) required. <input type="checkbox"/> System of Records Notice (SORN) required.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item.



	If covered by existing SORN, please list: Click here to enter text.
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
(b)(5)	



PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a new or updated Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002. This will also assess whether a new or updated System of Records Notice (SORN) is required under the Privacy Act of 1974.

Please complete this form and send it to the ICE Privacy & Records Office at ICEPrivacy@ice.dhs.gov.

Upon receipt, the ICE Privacy & Records Office will review this form. The DHS Privacy Office is the final adjudicator of the form. If a PIA is required, you will receive guidance on how to begin the PIA process.

Questions? Contact the ICE Privacy & Records Office at 202-732-3300 and ask to speak to a member of the Privacy Branch staff.



PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

SUMMARY INFORMATION

Project or Program Name:	EAGLE Directed Identification Environment (EDDIE) version 1.3.3		
Component:	Immigration and Customs Enforcement (ICE)	Office or Program:	ERO/Field Ops/LESA
TAFISMA Name:	Enforcement Integrated Database (EID) Arrest GUI for Law Enforcement	TAFISMA Number:	ICE-03529-MAJ-03529 EAGLE: ICE-06597-SUB-03529
Type of Project or Program:	IT System	Project or program status:	Modification

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	ERO/Field Ops/LESA	Title:	Project Manager
Phone:	202-732-(b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	(b)(6);(b)(7)(C)		
Phone:	202-732-(b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

ROUTING INFORMATION

Date submitted to Component Privacy Office:	November 17, 2015
Date submitted to DHS Privacy Office:	Click here to enter a date.
Date approved by DHS Privacy Office:	Click here to enter a date.



SPECIFIC PTA UPDATE QUESTIONS

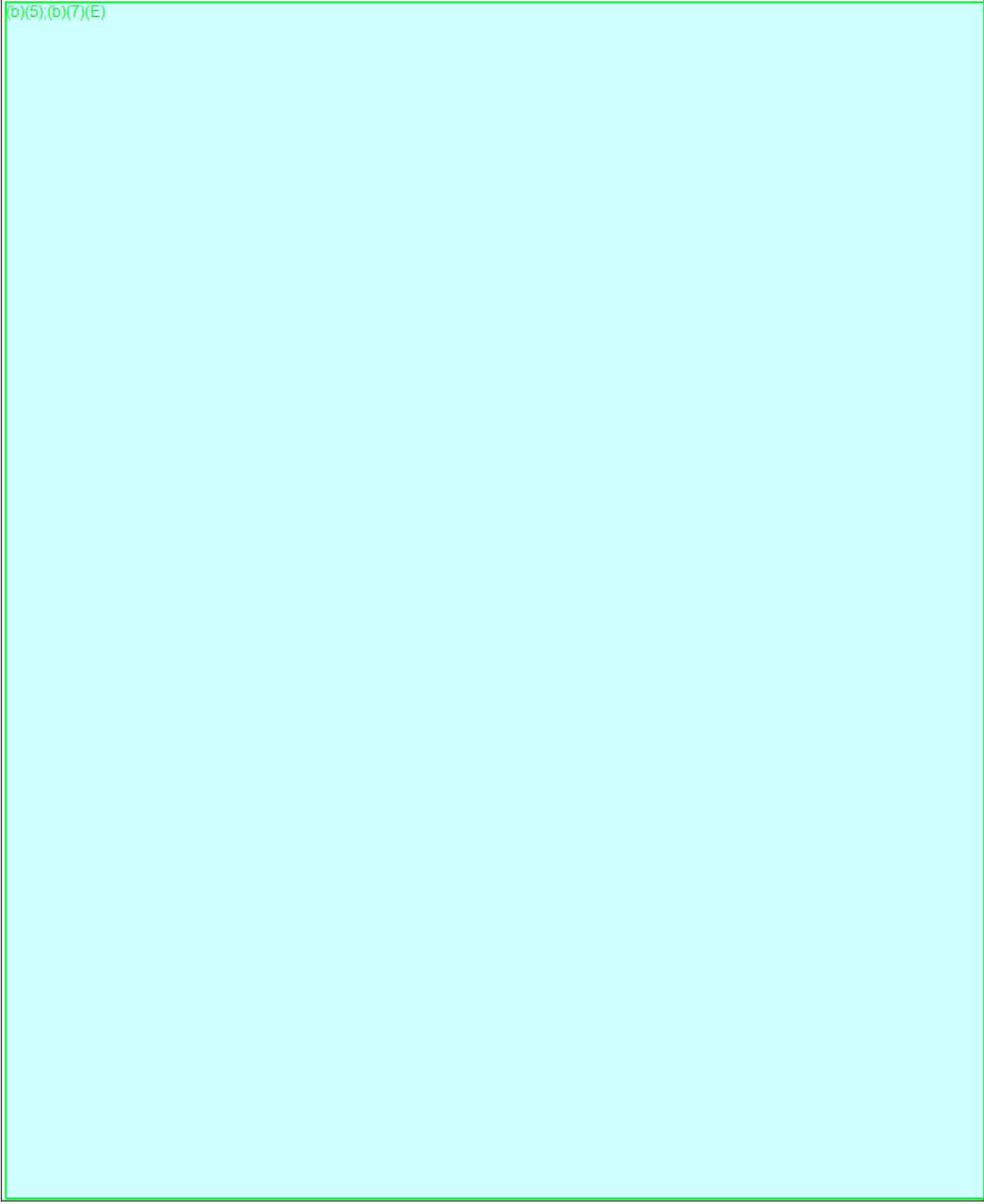
1. Describe the changes and/or upgrades planned for this system that are triggering this PTA Update:

Please provide a general description of the changes or upgrades using non-technical language and highlighting any changes involving or affecting Personally Identifiable Information (PII).

(b)(5);(b)(7)(E)



(b)(5);(b)(7)(E)

A large rectangular area of the page is redacted with a solid light blue fill. The redaction covers the majority of the page's content, leaving only the header and footer information visible.



(b)(5)

2. Project or Program status			
Date first developed:	December 17, 2014	Date last updated:	August 21, 2015
Scheduled deployment of changes/upgrades:	N/A	Degree of confidence in schedule:	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <input checked="" type="checkbox"/> Deploy date is unknown at this time
Name of system change/upgrade (e.g., EARM v 3.0):		EDDIE 1.3.3	

3. Is this project a technology/system that relates solely to infrastructure? For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?	<input type="checkbox"/> Yes (Stop here. Submit PTA Update.) <input checked="" type="checkbox"/> No (Continue with next question.)
--	---

4. Does the system currently contain PII about individuals, including ICE and DHS personnel, contractors, aliens, criminal suspects, or members of the public? (TAFISMA identifies which systems in the ICE inventory contain PII.)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
--	--

5. Are the system changes/upgrades limited to "bug fixes" only?	<input type="checkbox"/> Yes (Stop here. Submit PTA Update.) <input checked="" type="checkbox"/> No (Continue with next question.)
--	---

6. Do the changes/upgrades affect (either add or subtract) the types of individuals about whom the system collects, processes, or retains PII? Please check all that apply.
<input checked="" type="checkbox"/> No.



Yes. Information about additional types of individuals will be added.

Yes. Information will no longer be collected from one or more types of individuals.
<Please describe.>

7. Do the changes/upgrades pertain to Social Security Numbers (SSNs)?	<input type="checkbox"/> No. The project will continue to collect/use SSNs as before.
	<input checked="" type="checkbox"/> No. SSNs are not now and will not be collected or used (full or partial).
	<input type="checkbox"/> Yes. Check the applicable box below: <ul style="list-style-type: none"> <input type="checkbox"/> The SSN will no longer be collected or used. <input type="checkbox"/> Full SSNs will no longer be collected or used; instead only partial SSNs (last 4) will be used. <input type="checkbox"/> SSNs will now be collected or used. Check which: <ul style="list-style-type: none"> <input type="checkbox"/> Full <input type="checkbox"/> Partial

8. Other than the SSN, do the changes/upgrades affect (either add or subtract) the PII that is collected, created, processed, or retained in the system? *Please check all that apply.*

No.

Yes.

(b)(5);(b)(7)(E)

Yes. Data previously collected about individuals will no longer be collected.
<Please describe the data.>



<p>9. Do the changes/upgrades alter the way the PII is used, or change the reason we are maintaining it or operating the system generally?</p>	<p><input type="checkbox"/> No</p> <p><input checked="" type="checkbox"/> Yes</p> <div style="border: 1px solid green; background-color: #e0ffff; padding: 5px; margin-top: 10px;"> <p>(b)(5);(b)(7)(E)</p> </div>
---	--

<p>10. Do the changes/upgrades impact connections with other IT systems, either within or outside of ICE? For example, are system connections being added or terminated? Is the system being migrated from a stand-alone environment to the ICE network?</p>	<p><input checked="" type="checkbox"/> No</p> <p><input type="checkbox"/> Yes</p> <p><Please describe the IT connections affected and how they are affected.></p>
---	---

<p>11. Do the changes/upgrades affect how or why data about individuals will be shared within ICE, within DHS, or outside of DHS? This would include an increase or decrease in the amount of data shared, or sharing with new partners, or adding categories of new system users. <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. Changes how or why data will be shared within ICE.</p> <p><input type="checkbox"/> Yes. Changes how or why data will be shared within DHS.</p>
---	---



Yes. Changes how or why data will be shared outside of DHS.

(b)(5);(b)(7)(E)

12. Do the changes/upgrades result in the system obtaining information from any new source?

No
 Yes

<Please describe.>

13. Will the changes/upgrades add to the system new analytical capabilities or other tools that will analyze or use PII?

No
 Yes

14. What is the date of the most recent ATO for the system?

The ATO for EDDIE falls under EID. The current ATO for EID expires on July 21, 2019.

15. Will the system changes/upgrades require an update to the C&A?

No
 Yes

16. What is the FIPS 199 determination for the as-is environment:	Confidentiality:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> High
	Integrity:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> High
	Availability:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> High

Will the FIPS 199 categorizations need to be updated due to the system changes/upgrades?

No
 Yes



Privacy Threshold Analysis Update
Version date: June 5, 2015
Page 9 of 11

If yes, identify the new (or expected) FIPS 199 categorization for the future state:	Confidentiality:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High
	Integrity:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High
	Availability:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6);(b)(7)(C)
Date submitted to DHS Privacy Office:	Click here to enter a date.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b)(5)	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6);(b)(7)(C)
Date approved by DHS Privacy Office:	November 30, 2017
PCTS Workflow Number:	1154221

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA Update adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	<input type="checkbox"/> PTA Update sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required.
PIA:	(b)(5)
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, October 19, 2016, 81 FR 72080



DHS Privacy Office Comments:

Please describe rationale for privacy compliance determination above.

(b)(5)



PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a new or updated Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002. This will also assess whether a new or updated System of Records Notice (SORN) is required under the Privacy Act of 1974.

Please complete this form and send it to the ICE Privacy & Records Office at ICEPrivacy@ice.dhs.gov.

Upon receipt, the ICE Privacy & Records Office will review this form. The DHS Privacy Office is the final adjudicator of the form. If a PIA is required, you will receive guidance on how to begin the PIA process.

Questions? Contact the ICE Privacy & Records Office at 202-732-3300 and ask to speak to a member of the Privacy Branch staff.



PRIVACY THRESHOLD ANALYSIS (PTA) UPDATE

SUMMARY INFORMATION

Project or Program Name:	ENFORCE Alien Removal Module (EARM) Prosecutions Module		
Component:	Immigration and Customs Enforcement (ICE)	Office or Program:	ERO
TAFISMA Name:	EARM	TAFISMA Number:	ICE-03469-MAJ-03469
Type of Project or Program:	IT System	Project or program status:	Operational

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)			
Office:	ERO	Title:	ITPM	
Phone:	202-732-	(b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	(b)(6);(b)(7)(C)			
Phone:	202-732-	(b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

ROUTING INFORMATION

Date submitted to Component Privacy Office:	October 19, 2016
Date submitted to DHS Privacy Office:	Click here to enter a date.
Date approved by DHS Privacy Office:	Click here to enter a date.



SPECIFIC PTA UPDATE QUESTIONS

1. Describe the changes and/or upgrades planned for this system that are triggering this PTA Update:

Please provide a general description of the changes or upgrades using non-technical language and highlighting any changes involving or affecting Personally Identifiable Information (PII).

(b)(5),(b)(7)(E)



(b)(5),(b)(7)(E)

A large rectangular area of the page is completely redacted, appearing as a solid light blue color. The redaction covers the majority of the page's content.



(b)(5);(b)(7)(E)

2. Project or Program status			
Date first developed:	August 1, 2008	Date last updated:	May 18, 2017
Scheduled deployment of changes/upgrades:	May 18, 2017	Degree of confidence in schedule:	<input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <input type="checkbox"/> Deploy date is unknown at this time



Name of system change/upgrade (e.g., EARM v 5.3):	EARM-PM 1.0
3. Is this project a technology/system that relates solely to infrastructure? For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?	<input type="checkbox"/> Yes (Stop here. Submit PTA Update.) <input checked="" type="checkbox"/> No (Continue with next question.)
4. Does the system currently contain PII about individuals, including ICE and DHS personnel, contractors, aliens, criminal suspects, or members of the public? (TAFISMA identifies which systems in the ICE inventory contain PII.)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
5. Are the system changes/upgrades limited to “bug fixes” only?	<input type="checkbox"/> Yes (Stop here. Submit PTA Update.) <input checked="" type="checkbox"/> No (Continue with next question.)
6. Do the changes/upgrades affect (either add or subtract) the types of individuals about whom the system collects, processes, or retains PII? Please check all that apply.	
<input checked="" type="checkbox"/> No.	
<input type="checkbox"/> Yes. Information about additional types of individuals will be added. <Please describe the new types of individuals and the source of this information.>	
<input type="checkbox"/> Yes. Information will no longer be collected from one or more types of individuals. <Please describe.>	
7. Do the changes/upgrades pertain	<input checked="" type="checkbox"/> No. The project will continue to collect/use SSNs as before.
	<input type="checkbox"/> No. SSNs are not now and will not be collected or used (full or partial).



to Social Security Numbers (SSNs)?	<input type="checkbox"/> Yes. Check the applicable box below: <ul style="list-style-type: none"> <input type="checkbox"/> The SSN will no longer be collected or used. <input type="checkbox"/> Full SSNs will no longer be collected or used; instead only partial SSNs (last 4) will be used. <input type="checkbox"/> SSNs will now be collected or used. Check which: <ul style="list-style-type: none"> <input type="checkbox"/> Full <input type="checkbox"/> Partial
---	---

8. Other than the SSN, do the changes/upgrades affect (either add or subtract) the PII that is collected, created, processed, or retained in the system? Please check all that apply.

No.

Yes. New types of data about individuals will be created or added.

(b)(5)

Yes. Data previously collected about individuals will no longer be collected.

<Please describe the data.>

9. Do the changes/upgrades alter the way the PII is used, or change the reason we are maintaining it or operating the system generally?	<input type="checkbox"/> No <input checked="" type="checkbox"/> Yes <p>The Prosecutions Module allows ERO officers to track alien criminal prosecutions in a centralized manner. Although ERO officers could have entered criminal case information into EARM prior to the deployment of the Prosecutions Module, EARM was not the official database used to track criminal prosecutions.</p>
--	---



<p>10. Do the changes/upgrades impact connections with other IT systems, either within or outside of ICE? For example, are system connections being added or terminated? Is the system being migrated from a stand-alone environment to the ICE network?</p>	<p><input checked="" type="checkbox"/> No</p> <p><input type="checkbox"/> Yes</p> <p><Please describe the IT connections affected and how they are affected.></p>
---	---

<p>11. Do the changes/upgrades affect how or why data about individuals will be shared within ICE, within DHS, or outside of DHS? This would include an increase or decrease in the amount of data shared, or sharing with new partners, or adding categories of new system users. Please check all that apply.</p>	
<p><input checked="" type="checkbox"/> No.</p>	
<p><input type="checkbox"/> Yes. Changes how or why data will be shared within ICE. <Please describe the changes.></p>	
<p><input type="checkbox"/> Yes. Changes how or why data will be shared within DHS.</p>	
<p><input type="checkbox"/> Yes. Changes how or why data will be shared outside of DHS. <Please describe the changes.></p>	

<p>12. Do the changes/upgrades result in the system obtaining information from any new source?</p>	<p><input type="checkbox"/> No</p> <p><input checked="" type="checkbox"/> Yes</p> <p>ERO will now obtain information from the Public Access to Court Electronic Records (PACER) system, and manually input the information into the PM. PACER maintains information regarding aliens' criminal prosecutions.</p>
---	--



13. Will the changes/upgrades add to the system new analytical capabilities or other tools that will analyze or use PII?	<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes <Please describe.>	
14. What is the date of the most recent ATO for the system?	July 2, 2015	
15. Will the system changes/upgrades require an update to the C&A?	<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	
16. What is the FIPS 199 determination for the as-is environment:	Confidentiality:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
	Integrity:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
	Availability:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
Will the FIPS 199 categorizations need to be updated due to the system changes/upgrades?	<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	
If yes, identify the new (or expected) FIPS 199 categorization for the future state:	Confidentiality:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High
	Integrity:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High
	Availability:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6),(b)(7)(C)
Date submitted to DHS Privacy Office:	Click here to enter a date.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b)(5)	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6),(b)(7)(C)
Date approved by DHS Privacy Office:	November 30, 2017
PCTS Workflow Number:	1154220

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA Update adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	<input type="checkbox"/> PTA Update sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required.
PIA:	(b)(5) If covered by existing PIA, please list: Update to DHS/ICE/PIA-015 Enforcement Integrated Database (EID) to discuss Prosecutions Module
SORN:	System covered by existing SORN



	If covered by existing SORN, please list: DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, October 19, 2016, 81 FR 72080
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
(b)(5)	



PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSCconnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	Detainee Telephone Services Data		
Component:	Immigration and Customs Enforcement (ICE)	Office or Program:	Enforcement and Removal Operations
Xacta FISMA Name (if applicable):	N/A	Xacta FISMA Number (if applicable):	N/A
Type of Project or Program:	Program	Project or program status:	Operational
Date first developed:	September 5, 2017	Pilot launch date:	Click here to enter a date.
Date of last PTA update	September 5, 2017	Pilot end date:	Click here to enter a date.
ATO Status (if applicable)	Not started	ATO expiration date (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	Custody Management Division	Title:	Contract Officer Representative
Phone:	(202) 732-(b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Click here to enter text.		
Phone:	Click here to enter text.	Email:	Click here to enter text.



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

(b)(5)

2. Does this system employ any of the following technologies:

If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.

- Closed Circuit Television (CCTV)
- Social Media
- Web portal¹ (e.g., SharePoint)
- Contact Lists

¹ Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are “members” of the portal or “potential members” who seek to gain access to the portal.



	<input checked="" type="checkbox"/> None of these
--	---

<p>3. From whom does the Project or Program collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information²</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p>
--	--

4. What specific information about individuals is collected, generated or retained?	
<p>Detainee name and Alien number, telephone number called by detainee, facility in which detainee is housed, phone number of the relevant facility, date and time of the call, and duration of the call.</p>	
<p>4(a) Does the project, program, or system retrieve information by personal identifier?</p>	<p><input type="checkbox"/> No. Please continue to next question.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: Detainee name and Alien number</p>
<p>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes.</p>
<p>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</p>	N/A
<p>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</p>	N/A
<p>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i></p>	<p><input checked="" type="checkbox"/> No. Please continue to next question.</p> <p><input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.</p>

² DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



4(f) If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.
N/A

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems⁴?	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: <div style="border: 1px solid green; background-color: #e0ffff; padding: 5px;">(b)(5)</div>
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. N/A
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: Training is provided upon request, but system operation is not complex.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	<input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: <input checked="" type="checkbox"/> Yes. In what format is the accounting maintained: <div style="border: 1px solid green; background-color: #e0ffff; padding: 5px;">(b)(5)</div>

³ When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

⁴ PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.



9. Is there a FIPS 199 determination?⁴	<input checked="" type="checkbox"/> Unknown. <input type="checkbox"/> No. <input type="checkbox"/> Yes. Please indicate the determinations for each of the following: Confidentiality: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	---

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Michelle Ramsden
Date submitted to Component Privacy Office:	September 5, 2017
Date submitted to DHS Privacy Office:	November 27, 2017
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b)(5)	

⁴ FIPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.



(b)(5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Max Binstock
PCTS Workflow Number:	1154304
Date approved by DHS Privacy Office:	December 29, 2017
PTA Expiration Date	December 29, 2020

DESIGNATION

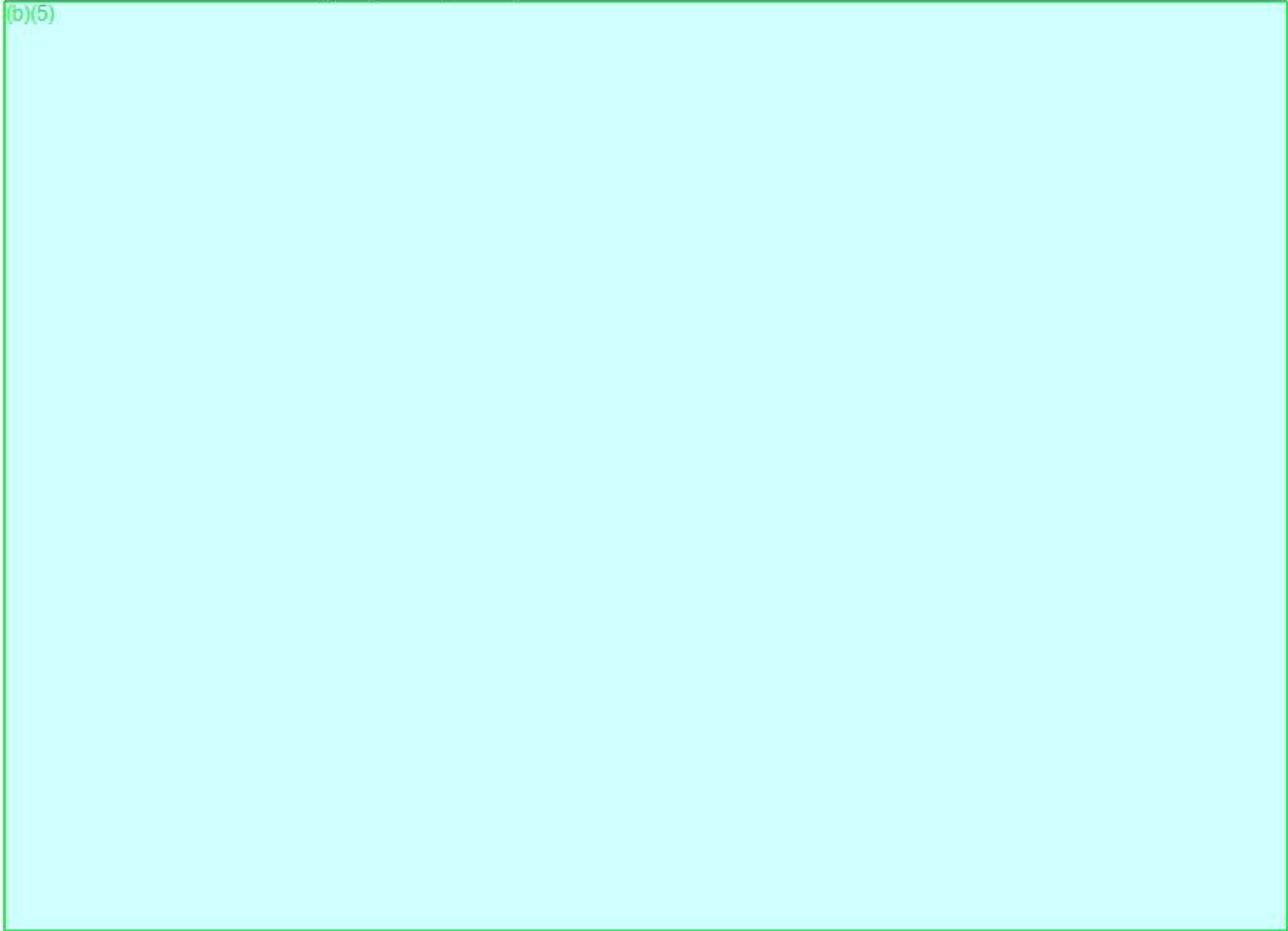
Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.
PIA:	System covered by existing PIA If covered by existing PIA, please list: DHS/ICE/PIA-015(b) Enforcement Integrated Database (EID) ENFORCE Alien Removal Module (EARM 3.0)
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, October 19, 2016, 81 FR 72080



DHS Privacy Office Comments:

Please describe rationale for privacy compliance determination above.

(b)(5)





PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.



Privacy Threshold Analysis (PTA)

Specialized Template for Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number:	I-901		
Form Title:	Fee Remittance for Certain F, J and M Nonimmigrants		
Component:	Immigration and Customs Enforcement (ICE)	Office:	Student & Exchange Visitor Program (SEVP)

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	Fee Remittance for Certain F, J and M Nonimmigrants		
OMB Control Number:	1653-0034	OMB Expiration Date:	May 31, 2018
Collection status:	Revision	Date of last PTA (if applicable):	N/A

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	Student and Exchange Visitor Program (SEVP)	Title:	Project Lead
Phone:	(703) 603- (b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	(b)(6);(b)(7)(C)		
Office:	ICE OCIO	Title:	ICE Forms Manager
Phone:	(202) 732- (b)(6);(b)(7)(C)	Email:	(b)(6);(b)(7)(C)



SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form	
a. Describe the purpose of the information collection or form.	
(b)(5)	
b. List the DHS (or component) authorities to collect, store, and use this information. <i>If this information will be stored and used by a specific DHS component, list the component-specific authorities.</i>	
Sections 1154, 1184, 1372, and 1258 of Title 8, U.S. Code	

2. Describe the IC/Form	
a. Does this form collect any Personally Identifiable Information" (PII ¹)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

¹ Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



<p>b. From which type(s) of individuals does this form collect information? <i>(Check all that apply.)</i></p>	<p><input checked="" type="checkbox"/> Members of the public</p> <p style="padding-left: 20px;"><input type="checkbox"/> U.S. citizens or lawful permanent residents</p> <p style="padding-left: 20px;"><input checked="" type="checkbox"/> Non-U.S. Persons.</p> <p><input type="checkbox"/> DHS Employees</p> <p><input type="checkbox"/> DHS Contractors</p> <p><input type="checkbox"/> Other federal employees or contractors.</p>
<p>c. Who will complete and submit this form? <i>(Check all that apply.)</i></p>	<p><input checked="" type="checkbox"/> The record subject of the form (e.g., the individual applicant).</p> <p><input type="checkbox"/> Legal Representative (preparer, attorney, etc.).</p> <p><input type="checkbox"/> Business entity.</p> <p style="padding-left: 40px;">If a business entity, is the only information collected business contact information?</p> <p style="padding-left: 80px;"><input type="checkbox"/> Yes</p> <p style="padding-left: 80px;"><input type="checkbox"/> No</p> <p><input type="checkbox"/> Law enforcement.</p> <p><input type="checkbox"/> DHS employee or contractor.</p> <p><input checked="" type="checkbox"/> Other individual/entity/organization that is NOT the record subject.</p> <p>Schools and exchange visitor program sponsors</p>
<p>d. How do individuals complete the form? <i>Check all that apply.</i></p>	<p><input type="checkbox"/> Paper. (See attached. See Appendix A)</p> <p><input type="checkbox"/> Electronic. (ex: fillable PDF)</p> <p><input checked="" type="checkbox"/> Online web form. (available and submitted via the internet)</p> <p>Access via www.fmjfee.com</p>
<p>e. What information will DHS collect on the form? <i>List all PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.</i></p>	
<p><u>Nonimmigrant PII collected:</u></p> <ul style="list-style-type: none"> Name (surname/primary name and given name) 	



- Date of birth
- Country of birth
- Country of citizenship
- Gender
- Address
- Email address
- SEVIS Identification Number (SEVIS ID)
- Passport number
- Payment
 - Credit card number (collected through the FMJfee website, but not stored after transaction occurs)

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.*

- | | |
|---|--|
| <input type="checkbox"/> Social Security number | <input type="checkbox"/> DHS Electronic Data Interchange Personal Identifier (EDIPI) |
| <input type="checkbox"/> Alien Number (A-Number) | <input type="checkbox"/> Social Media Handle/ID |
| <input type="checkbox"/> Tax Identification Number | <input type="checkbox"/> Known Traveler Number |
| <input type="checkbox"/> Visa Number | <input type="checkbox"/> Trusted Traveler Number (Global Entry, Pre-Check, etc.) |
| <input checked="" type="checkbox"/> Passport Number | <input type="checkbox"/> Driver's License Number |
| <input type="checkbox"/> Bank Account, Credit Card, or other financial account number | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Other: | |

g. List the **specific authority** to collect SSN or these other SPII elements.

8 U.S.C. 1372

h. How will this information be used? What is the purpose of the collection? Describe **why** this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

The I-901 fee must be paid before going to the United States embassy or consulate for a visa interview. The nonimmigrant must present proof of payment of the fee. This payment is associated with the passport that is used to gain entry into the United States.



<p>i. Are individuals provided notice at the time of collection by DHS (<i>Does the records subject have notice of the collection or is form filled out by third party</i>)?</p>	<p><input checked="" type="checkbox"/> Yes. Please describe how notice is provided. Privacy statement is provided on the first page of the FMJfee website.</p> <p><input type="checkbox"/> No.</p>
--	--

3. How will DHS store the IC/form responses?	
<p>a. How will DHS store the original, completed IC/forms?</p>	<p><input type="checkbox"/> Paper. Please describe. Click here to enter text.</p> <p><input checked="" type="checkbox"/> Electronic. Please describe the IT system that will store the data from the form. I-901 Fee Collection Services System (I-901 System)</p> <p><input type="checkbox"/> Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository. Click here to enter text.</p>
<p>b. If electronic, how does DHS input the responses into the IT system?</p>	<p><input type="checkbox"/> Manually (data elements manually entered). Please describe.</p> <p><input checked="" type="checkbox"/> Automatically. Please describe. Data is typed into fields by individual, which is automatically captured in the I-901 System.</p>
<p>c. How would a user search the information submitted on the forms, <i>i.e.</i>, how is the information retrieved?</p>	<p><input checked="" type="checkbox"/> By a unique identifier.² <i>Please describe.</i> Name, SEVIS ID, date of birth If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. Form I-901 does not require a Privacy Act Statement, as non-U.S. Citizens or LPRs are providing their PII. However, per ICE, we have developed a Privacy Statement. See <i>Appendix A</i> for a copy of the Privacy Statement.</p>

² Generally, a unique identifier is considered any type of “personally identifiable information,” meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



	<input checked="" type="checkbox"/> By a non-personal identifier. <i>Please describe.</i> For high level data searches, non-personal identifiers such as country of birth, country of citizenship, and gender may be used.
d. What is the records retention schedule(s)? <i>Include the records schedule number.</i>	(b)(5)
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	(b)(5)
f. Is any of this information shared outside of the original program/office? <i>If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?</i>	
<input type="checkbox"/> Yes, information is shared with other DHS components or offices. Please describe. <input checked="" type="checkbox"/> Yes, information is shared <i>external</i> to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe. (b)(5) <input type="checkbox"/> No. Information on this form is not shared outside of the collecting office.	



Homeland
Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy



Please include a copy of the referenced form and Privacy Act Statement (if applicable) with this PTA upon submission.



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6);(b)(7)(C)
Date submitted to component Privacy Office:	December 7, 2017
Date submitted to DHS Privacy Office:	December 19, 2017
Have you approved a Privacy Act Statement for this form? <i>(Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.)</i>	<input checked="" type="checkbox"/> Yes. Please include it with this PTA submission. <input type="checkbox"/> No. Please describe why not. Click here to enter text. See Appendix A for a copy of the Privacy Statement.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.</i>	
(b)(5)	



PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6);(b)(7)(C)
PCTS Workflow Number:	1155365
Date approved by DHS Privacy Office:	January 2, 2018
PTA Expiration Date	January 2, 2021

DESIGNATION

Privacy Sensitive IC or Form:	Yes If "no" PTA adjudication is complete.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing SPII applies. <input checked="" type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Specialized training required. <input type="checkbox"/> Other. Click here to enter text.
DHS IC/Forms Review:	(b)(5)
Date IC/Form Approved by PRIV:	January 2, 2018
IC/Form PCTS Number:	Click here to enter text.
Privacy Act Statement:	Privacy Notice is required Please change Privacy Statement to Privacy Notice.
PTA:	No system PTA required. Click here to enter text.
PIA:	System covered by existing PIA



	<p>If covered by existing PIA, please list: DHS/ALL/PIA-053 DHS Financial Management Systems If a PIA update is required, please list: Click here to enter text.</p>
SORN:	<p>System covered by existing SORN If covered by existing SORN, please list: DHS/ICE 001 Student and Exchange Visitor Information System, January 5, 2010, 75 FR 412 If a SORN update is required, please list: Click here to enter text.</p>
<p>DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i></p>	
<p>(b)(5)</p>	

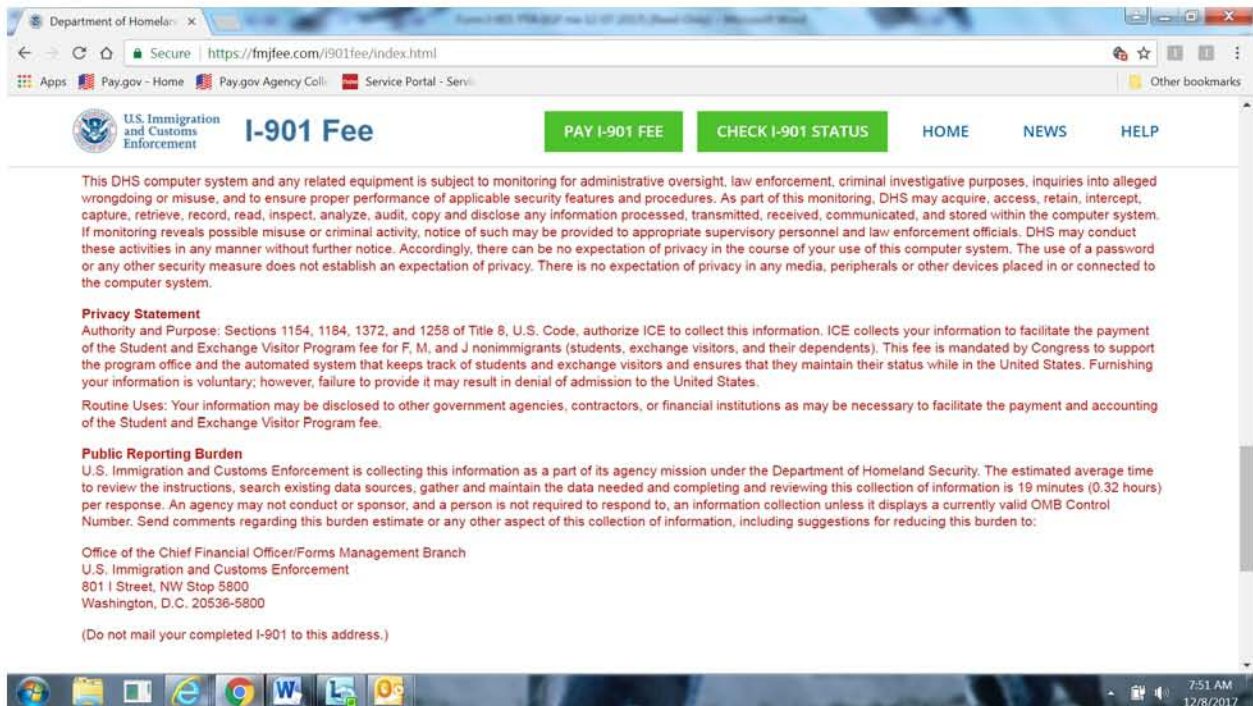


Appendix A – Privacy Statement

Privacy Statement

Authority and Purpose: Sections 1154, 1184, 1372, and 1258 of Title 8, U.S. Code, authorize ICE to collect this information. ICE collects your information to facilitate the payment of the Student and Exchange Visitor Program fee for F, M, and J nonimmigrant's (students, exchange visitors, and their dependents). This fee is mandated by Congress to support the program office and the automated system that keeps track of students and exchange visitors and ensures that they maintain their status while in the United States. Furnishing your information is voluntary; however, failure to provide it may result in denial of admission to the United States.

Routine Uses: Your information may be disclosed to other government agencies, contractors, or financial institutions as may be necessary to facilitate the payment and accounting of the Student and Exchange Visitor Program fee.





**Homeland
Security**

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

Appendix B – Form I-901

SEE NEXT PAGE



DEPARTMENT OF HOMELAND SECURITY
U.S. Immigration and Customs Enforcement

OMB No. 1653-0034
Expires 05/31/2018

I-901, FEE REMITTANCE FOR CERTAIN F, J AND M NONIMMIGRANTS

INSTRUCTIONS

This form is used to pay the fee to support the F, M, and J nonimmigrant reporting system authorized by Public Law 104-208, Subtitle D, Section 641. If you are subject to this fee and do not pay it, you will not be issued an F, M, or J nonimmigrant visa or be admitted to the United States. If you are in the United States and apply for a change of status, you are subject to this fee. If you do not pay it, your application will not be processed.

Fee payment is required if the applicant is:

- a. An alien seeking an **F-1, F-3, J-1, M-1, or M-3** visa from an embassy or consulate abroad for initial attendance at a school approved by the Department of Homeland Security (DHS) or for initial participation in an exchange visitor program designated by the Department of State (DoS). There is an exception noted below in section j.
- b. An alien who does not need a visa to enter the United States as a student or exchange visitor, who will be applying for admission at a U.S. port-of-entry to begin initial attendance at a DHS-approved school or initial participation in a DoS-designated exchange visitor program except as specified in section j below.
- c. An alien in the United States seeking a change of status to **F-1, F-3, J-1, M-1, or M-3**. There are exceptions noted below in sections j and n.
- d. A nonimmigrant who was initially granted **J-1** status as a participant in an exchange visitor program sponsored by the Federal government, as specified in section j below, and who is now transferring to another J program in the same category that is not sponsored by the Federal government.
- e. A **J-1** nonimmigrant who is applying for a change of category from within the United States. There is an exception noted below in section j.
- f. A **J-1** nonimmigrant who is applying for a reinstatement after a substantive violation, or who has been out of program status for longer than 120 days but less than 270 days during the course of his or her program. There is an exception noted below in section j.
- g. An **F-1, F-3, M-1, or M-3** nonimmigrant applying for reinstatement of student status, who has been out of student status for a period exceeding the presumptive ineligibility requirement set forth in 8 CFR 214.2(f)(16)(A) or 214.2(m)(16)(A).
- h. An **F-1, F-3, M-1, or M-3** nonimmigrant who has been absent from the United States for a period exceeding 5 months, was not working toward completion of curriculum in authorized overseas study, and now wishes to re-enter for a new F or M program of study in the United States.
- k. An **F-1, F-3, J-1, M-1, or M-3** nonimmigrant who has previously paid the fee, or whose Form I-20 or DS-2019 initial attendance was issued on or before August 31, 2004, and who is applying for a visa to return to the United States as a continuing student or a continuing participant of an exchange visitor program.
- l. An **F-1, F-3, M-1, or M-3** nonimmigrant transferring between approved schools, changing educational levels, or applying for post-completion practical training.
- m. A **J-1** nonimmigrant transferring between programs in the same exchange visitor category where no differential fee exists.
- n. A nonimmigrant applying for a change of classification from within the United States between **F-1** and **F-3** status or between **M-1** and **M-3** status.
- o. An **F-1, F-3, J-1, M-1, or M-3** nonimmigrant requesting/applying for an extension of stay in a single program.
- p. An alien reapplying for a visa from an embassy or consulate abroad after having paid the SEVIS fee for a previous **F-1, F-3, M-1, or M-3** visa that was denied, and who is applying again for the same type of program within 12 months of the initial denial.
- q. An alien reapplying for a visa from an embassy or consulate after having paid the SEVIS fee for a previous **J-1** visa that was denied, and who is applying again for the same type J-1 exchange visitor category within 12 months of the initial denial, unless there is a fee differential.
- r. A nonimmigrant who has applied for a change of status in the United States to an **F, M, or J** classification, had the initial application for the change of status denied for a reason other than failure to pay the SEVIS fee, and is applying for a motion to re-open the case within 12 months of the original denial.

Documents needed to fill out this form:

- **F-1, F-3, M-1, and M-3** status only: Form I-20 (Certificate of Eligibility for Nonimmigrant Student Status) issued to you by DHS-approved school you will attend.
- **J-1 status only:** Form DS-2019 (Certificate of Eligibility for Exchange Visitor [J-1] Status) issued to you by the designated exchange visitor program in which you will participate.

Fee payment not required if applicant is:

- i. An **F-2, J-2, or M-2** dependent.
- j. A **J-1** participant in an exchange visitor program sponsored by the Federal government. A program sponsored by the Federal government is identified by a program number of **G-1, G-2, G-3, or G-7**.



Instructions:

This form must be completed in English.

Item Number:

- 1-2. Enter your name exactly as it appears on your Form I-20 or DS-2019.
3. Enter your street address. Include apartment number and Post Office (P.O.) Box, if applicable.
4. Enter your city. Include a province as required. You may abbreviate (e.g., Toronto, ON).
5. For U.S. addresses only. If the address is in the United States, enter the 2-letter abbreviation for the state. If the address is not a state within the United States, do not fill in this section.
6. Enter your country.
7. Enter the postal code or zip code.
8. List your date of birth in mm/dd/yyyy format.
9. Check the appropriate space pertaining to your gender.
10. Enter your city (province) of birth.
11. Enter your country of birth, as listed on your Form I-20 or DS-2019.
12. Enter email address to receive SEVP official I-901 correspondence.
13. Enter your country of citizenship, as listed on your Form I-20 or DS-2019.
14. **F/M status only:** Enter the school code found on your Form I-20. Leave the Program Number blank.
J-1 status only: Enter the exchange visitor program number found on the Form DS-2019 (e.g.; P-1-00000). If your sponsor number begins with G-1, G-2, G-3, or G-7, you are exempt from fee payment. Leave the School Code blank.
15. Enter the SEVIS Identification Number listed on your Form I-20 or DS-2019, beginning with the first number after the letter "N".
16. Enter the passport number contained in your passport, if available.
17. **A. F/M status:** Check the box in subpart A which indicates that you owe \$200.00 and continue on to item number 18. Do not check any boxes in subpart B.

B. J-1 status: Do not check the box in subpart A. Check the box in subpart B that corresponds to the exchange visitor category found on your Form DS-2019. (If your sponsor number in section 2 of Form DS-2019 begins with G-1, G-2, G-3, or G-7, you are exempt from fee payment). Continue on to item number 18.

18. Enter total amount. Please send only one check or money order.

Payment by mail:

The only forms of payment that will be accepted are checks and money orders. No other form of payment will be accepted. **Do not mail cash.**

All checks and money orders must be made in U.S. dollars and drawn on a bank located in the United States.

All checks and money orders must be made payable to the "I-901 Student/Exchange Visitor Processing Fee."

Checks are accepted subject to collection. A charge of \$30.00 will be imposed if a check for payment of a fee is not honored by the bank on which it is drawn.

Write the name of the student or exchange visitor and the SEVIS identification number on the check.

Fees must be submitted in the exact amount. Failure to file forms correctly or with the correct payment will result in the return of this form to you and additional delay in processing. Fees will not be refunded.

Mail the Form I-901 and payment to:

**I-901 Student/Exchange Visitor Processing Fee
P.O. Box 970020
St. Louis, MO 63197-0020**

or

Courier the Form I-901 and payment to:

**I-901 Student/Exchange Visitor Processing Fee
1005 Convention Plaza
St. Louis, MO 63101**

All I-901 payment confirmations must be printed from www.FMJfee.com.

Payment by Internet:

The online Form I-901 is available at: www.FMJfee.com. All I-901 payment confirmations must be printed from www.FMJfee.com.



Privacy Statement

Authority and Purpose. Sections 1154, 1184, 1372, and 1258 of Title 8, U.S. Code, authorize ICE to collect this information. ICE collects your information to facilitate the payment of the Student and Exchange Visitor Program fee for F, M, and J nonimmigrant's (students, exchange visitors, and their dependents). This fee is mandated by Congress to support the program office and the automated system that keeps track of students and exchange visitors and ensures that they maintain their status while in the United States. Furnishing your information is voluntary; however, failure to provide it may result in denial of admission to the United States.

Routine Uses: Your information may be disclosed to other government agencies, contractors, or financial institutions as may be necessary to facilitate the payment and accounting of the Student and Exchange Visitor Program fee.

Public Reporting Burden

U.S. Immigration and Customs Enforcement is collecting this information as a part of its agency mission under the Department of Homeland Security. The estimated average time to review the instructions, search existing data sources, gather and maintain the data needed and completing and reviewing this collection of information is 19 minutes (0.32 hours) per response. An agency may not conduct or sponsor, and a person is not required to respond to, an information collection unless it displays a currently valid OMB Control Number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: U.S. Immigration and Customs Enforcement, Forms Management Office, 801 I Street NW, Washington D.C. 20536-5800. **Do not mail your completed I-901 to this address.**



DEPARTMENT OF HOMELAND SECURITY
U.S. Immigration and Customs Enforcement

OMB No. 1653-0034
Expires 05/31/2018

I-901, FEE REMITTANCE FOR CERTAIN F, J AND M NONIMMIGRANTS

TYPE OR PRINT IN BLUE OR BLACK INK		
1. Surname/Primary Name (<i>Last Name</i>):		
2. Given Name (<i>First and Middle Name</i>):		
3. Street Address /P.O. Box:		Apartment Number:
No. 2 Street Address /P.O. Box:		
4. City (<i>Province</i>):	5. State (<i>U.S. Address Only</i>):	6. Country:
7. Zip Code/Postal Code:	8. Date of Birth (<i>mm/dd/yyyy</i>):	9. Gender (<i>Check one</i>): Male: <input type="checkbox"/> Female: <input type="checkbox"/>
10. City (<i>Province</i>) of Birth:		
11. Country of Birth:	12. Email Address:	
13. Country of Citizenship:		
14. School Code (<i>I-20 (F/M nonimmigrant only)</i>): 214F	OR	Program Number (<i>DS-2019 (J-1 nonimmigrant only)</i>):
15. SEVIS Identification Number: N	16. Passport Number:	
17. Amount to be paid: A. F/M only: (\$200) <input type="checkbox"/> B. J-1 only: Indicate your Exchange Visitor Category (<i>Check only one of the following boxes</i>)		
Student (\$180) <input type="checkbox"/>	Research Scholar (\$180) <input type="checkbox"/>	
Trainee (\$180) <input type="checkbox"/>	Short-term scholar (\$180) <input type="checkbox"/>	
Teacher (\$180) <input type="checkbox"/>	Specialist (\$180) <input type="checkbox"/>	
Professor (\$180) <input type="checkbox"/>	Intern (\$180) <input type="checkbox"/>	
Alien Physician (\$180) <input type="checkbox"/>	Camp Counselor (\$35) <input type="checkbox"/>	
Government Visitor (\$180) <input type="checkbox"/>	Summer Work/Travel (\$35) <input type="checkbox"/>	
	AuPair (\$35) <input type="checkbox"/>	
18. Total amount \$ _____.		



The screenshot shows a web browser window with the URL <https://www.fmjfee.com/i901fee/index.html#>. The browser tabs include "Privacy Threshold Analysis (PT...", "I-901 SEVIS Fee | ICE", "Department of Homeland S...", "ice.gov", "SEVPAMS", and "SEVIS Requirements Planning". The browser's address bar shows "https://www.fmjfee.com/i901fee/index.html#". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The browser's toolbar includes "inSight Home", "G", "intranet", "admin", "training", "intel", "IT", "RIM", "privacy", "IG", "SEVP", and "DAILY".

The website header includes the U.S. Department of Homeland Security logo, the text "U.S. Immigration and Customs Enforcement", the phone number "(US) 1-703-603-3400", the email address "fmjfee.sevis@ice.dhs.gov", and the OMB number "OMB 1653-0134". The main navigation menu includes "I-901 Fee", "PAY I-901 FEE", "CHECK I-901 STATUS", "HOME", "NEWS", and "HELP". A red banner below the navigation menu says "Click Here to Request an I-901 Fee Transfer".

The main content area is divided into two sections: "APPLICANT VALIDATION" and "Payment Instructions".

APPLICANT VALIDATION

Enter the following information exactly as it appears on your Form I-20 or DS-2019.
*** Indicates that the information is required

SEVIS ID *

Last Name *

Given Name

Date of Birth * / /

Payment Instructions

Before Proceeding:

You must have a complete and accurate Form I-20 or DS-2019 if you do not have an I-20 or DS-2019 or if the information on the form is incorrect, contact your school official or program sponsor.

Do not pay for a dependent child or spouse who is on an F-2, M-2, or J-2 visa. There is no I-901 SEVIS fee due for a dependent child or spouse for these visa types.

Do not pay again if you know that you have made a mistake after you submitted your information. Instead, send an email to fmjfee.sevis@ice.dhs.gov and explain what information may need to be changed.

The footer of the website includes links for "STUDY IN THE STATES", "ACCESSIBILITY", "LAW CUSTOMER SUPPORT", and "EMPLOYMENT".



Form I-901

FORM I-901

*** indicates that the information is required

SEVIS ID: N3242343243
Date of Birth: 01/01/1970
Last Name: ESSADFAS
Given Name:

APPLICANT INFORMATION

Form Type *

Email Address *

Country of Citizenship *

Country of Birth *

ADDRESS INFORMATION

Street Address 1*

Street Address 2

Form I-901 Help

Name
Enter your name exactly as it appears on your Form I-20 or DS-2019.

Email Address
Enter the email address at which you wish to receive official SEVP I-901 correspondence.

Address
Enter your street address. Include Apartment number and Post Office (P.O.) Box, if applicable.

Enter your city. Include a province as required. You may abbreviate (e.g. Toronto, ON.)

*For U.S. addresses only. Enter the State. If your address is outside the U.S., leave the state field blank.

City *

State *

Country *

Zip / Postal Code *

SCHOOL INFORMATION

School Code *

Amount Due \$200.00

I have read the instructions on this form. I understand that I will be able to print a payment confirmation. I understand that this payment confirmation is an important document for this NON-REFUNDABLE fee. It may be needed when applying for a non-immigrant visa, admission at any United States port of entry, change of status, or other United States immigration benefits.

I Agree

[CONTINUE](#)



Form I-901 Review

FORM I-901 REVIEW

Visa Type:	F-1/M-1, F-3/M-3
SEVIS ID:	N4354353453
Date of Birth:	01/01/1970
Last Name:	EDFGASDFSDFASDF
Email Address:	gmail@gmail.com
Country Of Citizenship:	ALBANIA
Country Of Birth:	ALGERIA
School Code:	AND214F23432.234
Amount Due:	\$200.00

Street Address 1:	7 MAIN STREET
City, Province:	ROCKVILLE
State:	MD
Zip / Postal Code:	20854
Country:	UNITED STATES

Select Payment Method:

CREDIT CARD

CHECK / MONEY ORDER / WESTERN UNION

RETURN TO FORM I-901

Attention!

Please take a moment to review the information on your Form I-901. If any of the information you entered needs to be corrected, please click 'Return to Form I-901 and make the updates before submitting your payment.'





Credit Card Payment Information

PAYMENT INFORMATION

Amount Due: \$200.00



PLEASE ENTER YOUR CREDIT CARD INFORMATION:

*** Indicate that the information is required

Cardholder Name *

Card Number *

Exp Date *

CVV2 *

BILLING ADDRESS INFORMATION

Same as Form I-901 Address

Address *

City *

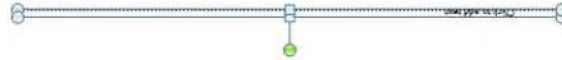
State *

Country *

Zip / Postal Code *

Attention!

Please take a moment to review the information on your Form I-901. If any of the information you entered needs to be corrected, please click "Return to Form I-901" and make the updates before submitting your payment.





I-901 Coupon

FORM I-901 REVIEW

Visa Type:	F-1/M-1, F-3/M-3
SEVIS ID:	N4354353453
Date of Birth:	01/01/1970
Last Name:	EDFGASDFSDAFASDF
Email Address:	gmail@gmail.com
Country Of Citizenship:	ALBANIA
Country Of Birth:	ALGERIA
School Code:	AND214F23432.234
Amount Due:	\$200.00

Street Address 1:	7 MAIN STREET
City, Province:	ROCKVILLE
State:	MD
Zip / Postal Code:	20854
Country:	UNITED STATES

Select Payment Method:

[REPRINT COUPON](#)

If payment is not made by credit card, the FMJfee.com website provides instructions for the student to print the Form I-901 Payment Coupon to mail along with the payment or to take to a Western Union Quick Pay agent. Check or money orders are sent to the specified lockbox.

