

Table of Contents

Lesson 1: Course Overview.....	1
Title Screen	1
CBP's Guiding Principles.....	1
Welcome and Introduction.....	2
Course Learning Objectives.....	2
Why Is This Important?	3
Course Structure and Time Requirements	3
CBP Directive Number 3340-049.....	4
Completing the Course	4
Lesson 2: Border Search of Electronic Information.....	5
Lesson Introduction	5
Border Search of Electronic Information Defined (contd.)	5
Border Search of Electronic Information Defined.....	5
Electronic Devices	6
Border Search of Information (BSI) Policy	7
BSI Authority and Other Searches.....	7
Commercial Shipments.....	7
Directives Not Superseded.....	7
CBP-Requested Searches.....	8
CBP Border Search Procedure.....	8
Documenting Searches.....	8
Searching in the Presence of the Individual.....	8
Lesson Summary.....	9
Lesson 3: Review and Handling of Specific Types of Information	10
Lesson Introduction	10
Sensitive or Privileged Information	10
Business Confidential Information	10
Attorney-Client Privileged Material	10
Medical Records and Work-Related Information.....	11
Lesson Summary.....	11
Lesson 4: Detention of Information	12
Lesson Introduction	12
Approval to Detain an Electronic Device	12
Time Frames for Detention.....	12
Notification of Detention	12
Destruction of Information	13
Lesson Summary.....	13
Lesson 5: Assistance by Other Federal Agencies (Excluding ICE).....	15
Lesson Introduction	15
Technical Assistance.....	15
Subject Matter Assistance.....	15
Approvals for Assistance	16
Notification to Traveler.....	16
Possible Terrorism	16

Time Frame for Assistance	16
Revocation of a Request for Assistance.....	17
Return by Agencies Providing Assistance.....	17
Retention by Agencies Providing Assistance	17
Retaining Copies.....	17
Lesson Summary.....	18
Lesson 6: Retention and Sharing of Information	19
Lesson Introduction	19
Retention with Probable Cause.....	19
Retention of Information in CBP Privacy Act-Compliant Systems	19
Sharing Information	19
Safeguarding Data During Storage and Transmission.....	20
Lesson Summary.....	20
Lesson 7: Reporting and Management Requirements	21
Lesson Introduction	21
BSI Reporting Requirements	21
BSI Reporting Requirements When Information Is Forwarded	21
Management Requirements	21
Management Requirements (contd.).....	22
Lesson Summary.....	22
Lesson 8: Course Summary	23
Conclusion	23
Additional References.....	23

Lesson 1: Course Overview

Title Screen

CBP Border Search of Electronic Information

(b)(2)High

CBP's Guiding Principles

The following are the four guiding principles that direct our organizational ethics and integrity.

Mission Statement

We are the guardians of our Nation's borders. We are America's frontline. We safeguard the American homeland at and beyond our borders. We protect the American public against terrorists and the instruments of terror. We steadfastly enforce the laws of the United States while fostering our Nation's economic security through lawful international trade and travel. We serve the American public with vigilance, integrity, and professionalism.

Core Values

Vigilance is how we ensure the safety of all Americans. We are continuously watchful and alert to deter, detect, and prevent threats to our Nation. We demonstrate courage and valor in the protection of our Nation.

Service to Country is embodied in the work we do. We are dedicated to defending and upholding the Constitution of the United States. The American people have entrusted us to protect the homeland and defend liberty.

Integrity is our cornerstone. We are guided by the highest ethical and moral principles. Our actions bring honor to ourselves and our agency.

Employee Oath of Office

“I do solemnly swear that I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion, and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.”

DHS Race and Ethnicity Guidelines

The Department of Homeland Security has adopted the Department of Justice's guidelines on the use of race or ethnicity in law enforcement activities. This statement is from the issuing memo dated June 1, 2004 and signed by the Secretary of the Department of Homeland Security.

“Racial profiling” concerns the invidious use of race or ethnicity as a criterion in conducting stops, searches and other law enforcement activities. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity.

DHS explicitly adopts the Department of Justice's “Guidance Regarding the Use of Race by Federal Law Enforcement Agencies,” issued in June 2003. It is the policy of the Department of Homeland Security to prohibit the consideration of race or ethnicity in our daily law enforcement activities in all but the most exceptional instances, as defined in the DOJ Guidance. DHS personnel may use race or ethnicity only when a compelling governmental interest is present.

Rather than relying on race or ethnicity, it is permissible and advisable to consider an individual's connections to countries that are associated with significant terrorist activity. Of course, race- or ethnicity-based information that is specific to particular suspects or incidents or ongoing criminal activities, schemes, or enterprises may be considered, as stated in the DOJ Guidance.

Welcome and Introduction

Welcome to the U.S. Customs and Border Protection (CBP) Border Search of Electronic Information course.

This course teaches CBP procedures for searching, reviewing, retaining, and sharing information contained within electronic devices encountered at the border, to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce.

Course Learning Objectives

By the end of this course, you should be able to:

- Identify how to conduct a border search of information within an electronic device
- Identify special handling procedures for business or commercial information, attorney-client privileged material, medical records, and work-related information carried by journalists
- Identify CBP procedures for detaining an electronic device

- Identify CBP procedures for seeking assistance from other government agencies (excluding Immigration and Customs Enforcement) to further the border search of an electronic device
- Identify CBP procedures for retaining and sharing electronic information
- Identify the requirements for reporting a border search of an electronic device
- Identify supervisory responsibilities for overseeing the handling of an electronic device

Why Is This Important?

Search of electronic devices is critical to enforcing law at the border and ensuring the protection of our Nation against all threats.

Information contained within electronic devices may reveal evidence relating to terrorism and other national security matters, human and cash smuggling, contraband, child pornography, and financial and commercial crimes.

Searches of electronic devices are also used to determine admissibility under immigration laws.

Course Structure and Time Requirements

This course has eight lessons, including a course introduction and a summary. The lessons are described below.

Lesson Name	Description
Course Overview	Provides an introduction to the course topic and learning objectives for the course
Border Search of Information	Defines key terms related to border search, explains border search authority, and describes the CBP border search procedure
Review and Handling of Specific Types of Information	Describes special handling procedures for sensitive or privileged information encountered during border search of an electronic device
Detention of Information	Describes CBP procedure for detaining an electronic device
Assistance by Other Federal Agencies (Excluding ICE)	Explains CBP policy and procedure for seeking assistance with electronic information from other Federal agencies (excluding ICE)
Retention and Sharing of Information	Explains CBP policy for retaining, sharing, and safeguarding electronic information
Reporting and Management Requirements	Identifies requirements for reporting and overseeing the search of an electronic device
Course Summary	Reviews the learning objectives met by the course

CBP Directive Number 3340-049

This course is based on the CBP Directive Number 3340-049, *Border Search of Electronic Devices Containing Information*, issued August 20, 2009.

Completing the Course

You may access the lessons in any order, although it's best to proceed through the lessons in order, as lessons typically build on previous content.

There is no scored assessment.

Open each screen within each lesson and complete all knowledge checks to receive credit for the course. You will receive instructions at the end of the course to print your certificate of completion.

Lesson 2: Border Search of Electronic Information

Lesson Introduction

This lesson defines key terms and explains CBP policy and procedure for searching the information contained within electronic devices.

By the end of this lesson, you should be able to identify how to conduct a border search of information (BSI) within an electronic device.

Border Search of Electronic Information Defined (contd.)

The *Border Search of Electronic Devices Containing Information* Directive provides policy on the search of all electronic devices encountered at the border, both inbound and outbound.

Such searches are authorized, with or without suspicion, to enforce the full range of U.S. laws that CBP administers at the border subject to the requirements and limitations provided in the Directive.

Border Search of Electronic Information Defined

Border search of information does not pertain to:

- Actions taken to determine whether a device functions, such as turning the device on and off
- Actions taken to determine whether contraband is concealed within a device
- Review of information an individual voluntarily provides in electronic format, such as an e-ticket displayed on an electronic device

Select here for a [border search example](#).

Border Search Example

A 43-year-old male, traveling alone, arrived at Los Angeles International Airport from the Philippines - a known destination for sex tourism. When questioned, the traveler said that he had been on vacation for three weeks visiting friends in the Philippines. (b)(2)High, (b)(7)(E)

When asked about his employment, the traveler replied that he was unemployed, but had worked as a math teacher and a night auditor. (b)(2)High, (b)(7)(E)

The CBP Officer decided to search the traveler's luggage and discovered a laptop computer, an external hard drive, a memory stick, and a few CDs. In the course of this luggage search, (b)(2)High, (b)(7)(E)

(b)(2)High, (b)(7)(E) search the traveler's laptop and asked him to turn it on. When the laptop was turned on, the CBP Officer discovered numerous photographs of what appeared to be child pornography.

In the course of a border search, with or without individualized suspicion, an Officer or Agent may examine electronic devices and may review and analyze the information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

Searches of electronic devices will be documented in appropriate CBP systems of records

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

Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, etc.

Electronic Devices

Under border search authority, an electronic device is defined as “any device that may contain information,” including:

- Computers
- Disks
- Drives
- Tapes
- Mobile phones and other communication devices
- Cameras
- Music and other media players
- Any other electronic or digital devices

Select here for an [example of an electronic device](#).

Example of an Electronic Device

All electronic or digital devices that hold or transmit information may be subject to border search for CBP to enforce law at the border.

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

CBP has the authority to search GPS devices if conducted as part of a border search.

Border Search of Information (BSI) Policy

This and the following three screens describe BSI policy.

BSI policy applies to all CBP Officers, Border Patrol Agents, Air Interdiction Agents, Marine Interdiction Agents, and other employees authorized by law to perform searches at the border, the functional equivalent of the border (FEB), or the extended border.

All CBP employees performing a border search of electronic information must adhere to the policy and procedures described in this course, as specified in the *Border Search of Electronic Devices Containing Information* Directive.

Select here for an additional point about [privacy](#).

Privacy

CBP Agents, Officers, and other employees conducting a border search will protect the rights and privacy of individuals at the border from unreasonable search and seizure, while ensuring that the CBP enforcement mission is accomplished.

BSI Authority and Other Searches

The *Border Search of Electronic Devices Containing Information* Directive governs border search authority only. It does not limit CBP's authority to conduct other lawful searches at the border, such as searches based on a warrant, consent, or incident to an arrest.

This Directive does not limit CBP's ability to record impressions relating to border encounters, nor does it restrict the dissemination of information as required by applicable statutes and Executive Orders.

Commercial Shipments

The *Border Search of Electronic Devices Containing Information* Directive does not govern searches of commercial shipments of electronic devices, such as a large shipment of laptop computers transiting from the factory to the distributor.

Directives Not Superseded

This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled as defined by Directive 2210-001A or its successor.

The *Border Search of Electronic Devices Containing Information* Directive also does not supersede [Processing Foreign Diplomatic and Consular Officials](#), Directive 3340-032.

Processing Foreign Diplomatic and Consular Officials

Diplomatic and consular officials encountered at the border, the FEB, or extended border should continue to be processed as defined by Directive 3340-032 or its successor.

CBP-Requested Searches

The *Border Search of Electronic Devices Containing Information* Directive applies only to searches performed by or at the request of CBP. It does not apply to border searches performed by U.S. Immigration and Customs Enforcement (ICE).

ICE Special Agents have their own border search authority and perform border searches by ICE policy and procedure. If ICE receives an electronic device or copy of information from CBP for analysis and investigation, ICE policy applies to the item once it has been received.

CBP Border Search Procedure

CBP border searches may be performed by any individual authorized to perform or assist in such searches.

In the course of a border search, an Officer or Agent may examine electronic devices encountered at the border and review and analyze the information contained within those devices, with or without individualized suspicion.

Documenting Searches

Searches of electronic devices will be documented in appropriate CBP systems of records

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

Searching in the Presence of the Individual

Searches of electronic devices should be conducted in the presence of the individual whose information is being examined - unless national security, law enforcement, or other operational considerations make it inappropriate for the individual to remain present.

Allowing an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself.

Witnessing the Search

The individual will not be permitted to observe if the search could reveal law enforcement techniques or potentially compromise other operations.

Lesson Summary

This concludes the lesson Border Search of Information. Key points covered in this lesson include:

- A border search may be performed on any device containing information, with or without individualized suspicion.
- Searches of electronic devices should be conducted in the presence of a supervisor unless impractical.
- Searches of electronic devices should be conducted in the presence of the person whose information is being examined, unless inappropriate.

Lesson 3: Review and Handling of Specific Types of Information

Lesson Introduction

This lesson explains the procedures for reviewing and handling privileged or sensitive material, including business or commercial information, attorney-client privileged material, medical records, and work-related information carried by journalists.

By the end of this lesson, you should be able to identify special handling procedures for business or commercial information, attorney-client privileged material, medical records, and work-related information carried by journalists.

Sensitive or Privileged Information

During the search of an electronic device, Officers and Agents may encounter sensitive or privileged information.

Sensitive or privileged information may be handled differently based on the type of information being reviewed.

Business Confidential Information

Officers and Agents encountering business or commercial information in electronic devices should treat such information as business confidential information and protect it from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws and CBP policies may govern or restrict the handling of the information.

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

Attorney-Client Privileged Material

Officers and Agents may also encounter information that appears to be legal in nature or that an individual asserts is protected by attorney-client or attorney work-product privilege.

Legal materials are not necessarily exempt from a border search. They may be subject to the following special handling procedures:

- If an Officer suspects that the content of such material constitutes evidence of a crime or otherwise pertains to a determination within the jurisdiction of CBP, the Officer or Agent must seek advice from the **(b)(2)High, (b)(7)(E)** before conducting a search of the material.
- This consultation shall be noted in appropriate CBP systems of records.

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

Medical Records and Work-Related Information

Other possibly sensitive information, such as medical records and work-related information carried by journalists, should be handled according to applicable federal law and CBP policy.

Information that is determined to be protected by law as privileged or sensitive will be shared only with federal agencies that have mechanisms in place to protect such information.

If there are questions ...

Questions

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

Lesson Summary

This concludes the lesson Review and Handling of Specific Types of Information. Key points covered in this lesson include:

- Sensitive or privileged information encountered during a border search must be handled and protected according to applicable laws and policies.
- Questions regarding the handling of sensitive or privileged information should be directed to the CBP (b)(2)High, (b)(7)(E).

Lesson 4: Detention of Information

Lesson Introduction

This lesson describes CBP procedure for detaining information.

By the end of this lesson, you should be able to identify CBP procedure for detaining an electronic device.

Approval to Detain an Electronic Device

An Officer or Agent may detain an electronic device or copies of information contained within a device for a brief, reasonable period of time to perform a thorough border search.

The search may take place on-site or off-site and should be completed as quickly as possible. Unless extenuating circumstances exist, the detention of devices should not exceed 5 days.

Time Frames for Detention

If a border search must be continued after an individual's departure from the port or location of detention, supervisory approval is required to detain electronic devices or copies of electronic information. Approval from the (b)(2)High, (b)(7)(E) manager is required to extend the detention beyond 5 days.

Extensions of detentions exceeding 15 days must be approved by the (b)(2)High, (b)(7)(E) manager, and may be approved and re-approved in increments of no more than 7 days.

Approvals for detention and extension of detention should be noted in the appropriate CBP systems of records.

Notification of Detention

When a border search of information is conducted on an electronic device, the individual must be notified of the search unless the notification could hinder national security, law enforcement, or other operational considerations.

Select here to view information that should be contained in the [notification to the individual](#).

In addition, if CBP determines it is necessary to temporarily detain an electronic device to continue the search, the Officer or Agent detaining the device will issue a completed Form 6051D to the individual prior to the individual's departure.

Notification to the Individual

- The purpose and authority for the search
- How the individual may obtain more information about reporting his or her concerns about the search
- How the individual may seek redress from the agency if he or she feels aggrieved by the search

Destruction of Information

If detained information has been reviewed and there is no probable cause to seize it, or the material may not otherwise be retained in a CBP Privacy Act-compliant system, all copies of the information must be destroyed and all electronic devices must be returned to their owners. CBP will retain no copies of the information.

Electronic records may be destroyed by deleting, overwriting, or degaussing the information in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

Destruction of the information should be noted in appropriate CBP systems of records.

Copies of information are destroyed as quickly as possible after determination that they hold no value.

Destroying Copies

Copies of information that has been determined to hold no value should be destroyed within 7 days of the determination, unless circumstances require additional time. Additional time may not exceed 21 days after the determination and must be approved by a supervisor.

Destruction of the copies should be documented in the appropriate CBP systems of records.

Lesson Summary

This concludes the lesson Detention of Information. Key points covered in this lesson include:

- An Officer or Agent may detain electronic devices or copies of information to perform a thorough border search.
- Individuals will be notified that their electronic devices are being searched unless doing so could hinder national security, law enforcement, or other operational considerations.

- If there is no probable cause to seize the detained information, all copies of the information will be destroyed and all electronic devices will be returned to the individual.

Lesson 5: Assistance by Other Federal Agencies (Excluding ICE)

Lesson Introduction

This lesson explains CBP procedure for seeking assistance from other federal agencies (excluding ICE) to further the search of detained electronic information.

By the end of this lesson, you should be able to identify CBP procedures for seeking assistance from other government agencies (excluding ICE) to further the border search of an electronic device.

Technical Assistance

CBP may use other federal agency analytical resources, such as translation, decryption, and subject matter expertise, to review information contained in electronic devices or to determine the meaning, context, or value of the information contained within a device.

Officers and Agents may sometimes require technical assistance to continue the search of an electronic device or to determine the meaning of information they encounter, such as when the information is written in a foreign language or encrypted (including information that is password-protected or otherwise not readily reviewable).

In such situations, Officers and Agents may transmit electronic devices or copies of information contained within devices to seek technical assistance from other Federal agencies. Officers and Agents may seek such assistance with or without individualized suspicion.

Subject Matter Assistance

When CBP has reasonable suspicion, they can seek assistance from Subject Matter Experts in other Federal agencies to determine the meaning, context, or value of information as it relates to the laws enforced and administered by CBP.

For that purpose, Officers and Agents may transmit electronic devices or copies of information to other Federal agencies when they have reasonable suspicion of activities that violate laws that CBP enforces.

Reasonable Suspicion

While many factors may result in reasonable suspicion, the presence of an individual's name on a government-operated and government-vetted terrorist watch list is always sufficient to create reasonable suspicion.

Approvals for Assistance

Requests for translation, decryption, and subject matter assistance require supervisory approval and must be properly documented and recorded in the CBP systems of records. All transfers of the custody of the electronic device should be recorded on Form 6051D.

Notification to Traveler

When information from an electronic device is transmitted to another Federal agency for translation, decryption, or subject matter assistance, the individual is notified of the transmission.

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

Requests for translation, decryption, and subject matter assistance require supervisory approval and must be properly documented and recorded in the CBP systems of records.

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

When notification is made to the individual, the Officer or Agent will annotate the notification in CBP systems of records and on Form 6051D.

Time Frame for Assistance

Responses from assisting Federal agencies are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time.

Unless otherwise approved by **(b)(2)High, (b)(7)(E)** manager, responses from an assisting agency should be received within 15 days. Select here to learn about [extending the response period](#).

Extending the Response Period

If the assisting agency is unable to respond within 15 days, **(b)(2)High, (b)(7)(E)** manager may permit extensions in increments of 7 days.

Revocation of a Request for Assistance

If at any time a CBP supervisor involved in a request for assistance is dissatisfied with the assistance, its timeliness, or anything else related to the assistance, the request may be revoked.

The CBP supervisor may require the assisting Federal agency to return all electronic devices and copies of information to CBP as quickly as possible, unless the agency retains the information under independent authority.

Revocation

All Revocations of a Request for Assistance should be documented in the appropriate CBP systems of records.

When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency.

Return by Agencies Providing Assistance

When subject matter assistance is requested of an agency, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced by CBP.

At the conclusion of the requested assistance, all information must be returned to CBP as quickly as possible. The assisting Federal agency should destroy all copies of the information unless the agency retains the information under independent authority.

If electronic devices were transmitted, they must NOT be destroyed. Electronic devices must be returned to CBP unless seized by the assisting agency based on probable cause or retained with independent authority.

Retention by Agencies Providing Assistance

All electronic devices or copies of information provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to CBP, or in accordance with retention under independent authority.

If an assisting Federal agency elects to continue to retain or seize an electronic device or information contained within the device, that agency shall assume responsibility for processing the retention or seizure.

Retaining Copies

Copies of information may be retained by an assisting Federal agency only if, and to the extent that, the agency has the independent legal authority to do so.

If an agency retains an electronic device or copy of information, the agency should advise CBP of its decision to retain the information under its own authority.

Lesson Summary

This concludes the lesson Assistance by Other Federal Agencies (Excluding ICE).

Key points covered in this lesson include:

- CBP may request assistance from other Federal agencies for translation, decryption, and subject matter expertise to further the border search.
- Responses from assisting agencies should be expeditious and should include all appropriate findings, observations, and conclusions relating to the laws that CBP enforces.
- At the conclusion of the requested assistance, all information must be returned to CBP. Copies must be destroyed by the assisting agency, unless it retains or seizes the information under independent authority.

Lesson 6: Retention and Sharing of Information

Lesson Introduction

This lesson discusses CBP procedures for retaining and sharing electronic information.

By the end of this lesson, you should be able to identify CBP procedures for retaining and sharing electronic information.

Retention with Probable Cause

Officers and Agents may seize and retain an electronic device or copies of information from the device under the following circumstance:

When the Officer or Agent determines there is probable cause to believe that the device or information contains evidence of, or is the result of, a crime that CBP is authorized to enforce.

Retention of Information in CBP Privacy Act-Compliant Systems

If there is no probable cause to seize an electronic device or copy of information, CBP may retain only information relating to immigration, customs, and other enforcement matters as long as such retention is consistent with privacy and data-protection standards of the system of records in which the information is retained.

Select here for an [example of retaining information](#).

Example of Retaining Information

Information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the following systems, among others, as appropriate and consistent with the policies governing such systems:

- A-file
- Central Index System
- TECS
- ENFORCE

Sharing Information

CBP has the authority to share copies of retained information with Federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

CBP will promptly share any terrorism-related information encountered in the course of a border search with elements of the Federal government responsible for analyzing terrorist threat information.

Safeguarding Data During Storage and Transmission

CBP will appropriately safeguard information that is retained, copied, seized, or transmitted to another Federal agency.

Appropriate safeguards include:

- Keeping materials in locked cabinets or rooms
- Documenting and tracking copies to ensure appropriate disposition
- Safeguarding during transmission, such as password protection or physical protection

Select here to learn about [loss or compromise](#).

Loss or Compromise

Any suspected loss or compromise of information that contains personal data must be immediately reported to the Port Director, (b)(2)High, (b)(7)(E)

Lesson Summary

This concludes the lesson Retention and Sharing of Information. Key points covered in this lesson include:

- Officers and Agents may seize and retain an electronic device or copy of information if the device or information contains evidence of, or is the result of, a crime that CBP is authorized to enforce.
- CBP has the authority to share copies of retained information with Federal, state, local, and foreign law enforcement agencies.
- CBP will appropriately safeguard all information at all times.

Lesson 7: Reporting and Management Requirements

Lesson Introduction

This lesson explains the reporting and management requirements for completing a border search of electronic information.

By the end of this lesson, you should be able to:

- Identify requirements for reporting a border search of an electronic device
- Identify supervisory requirements for overseeing the handling of an electronic device

BSI Reporting Requirements

The Officer or Agent performing the border search of information (BSI) is responsible for completing all reporting requirements. This responsibility includes:

- Completing Form 6051D when applicable
- Completing Document and Electronic Device Control Form (DEDCR) if an electronic device or copy of information is sent to another agency
- Creating or updating records in CBP automated systems (reports are to be created and updated in an accurate, thorough, and timely manner)

Reports must include all information related to the search through the final disposition, including supervisory approvals and extensions when appropriate.

BSI Reporting Requirements When Information Is Forwarded

If an electronic device or copy of information is forwarded within CBP, the receiving Officer or Agent is responsible for recording all information related to the search from the point of receipt through the final disposition.

Reporting requirements for this Directive are in addition to any other applicable reporting requirements.

Management Requirements

The duty supervisor is responsible for ensuring that the Officer or Agent completes a thorough inspection and that all notification, documentation, and reporting requirements are satisfied.

The appropriate CBP second-line supervisor is responsible for approving and monitoring the status of the following:

- Detention of all electronic devices or copies of information
- Transfer of any electronic device or copies of information for assistance from another Federal agency

Management Requirements (contd.)

(b)(2)High, (b)(7)(E) manager is responsible for establishing protocols to monitor the following:

- Proper documentation and recording of searches of electronic information
- Detention, transfer, and final disposition of electronic devices or copies of information in order to ensure compliance with the procedures outlined in this Directive

Lesson Summary

This concludes the lesson Reporting and Management Requirements. Key points covered in this lesson include:

- The Officer or Agent performing the border search of information is responsible for completing all reporting requirements.
- The duty supervisor ensures that Officers and Agents complete appropriate border search procedures.
- The appropriate CBP second-line supervisor approves and monitors the status of detained electronic devices or information.
- (b)(2)High, (b)(7)(E) manager establishes protocols to monitor border search procedures.

Lesson 8: Course Summary

Conclusion

Now that you have completed the Border Search of Electronic Information course, you should be able to:

- Identify how to conduct a border search of information within an electronic device
- Identify special handling procedures for business or commercial information, attorney-client privileged material, medical records, and work-related information carried by journalists
- Identify CBP procedures for detaining an electronic device
- Identify CBP procedures for seeking assistance from other government agencies (excluding ICE) to further the border search of an electronic device
- Identify CBP procedures for retaining and sharing electronic information
- Identify the requirements for reporting a border search of an electronic device
- Identify supervisory responsibilities for overseeing the handling of an electronic device

Additional References

For more information on CBP border search authority, research and review the following codes:

- 8 U.S.C. 1225, 1357, and other pertinent provisions of the immigration laws and regulations
- 19 U.S.C. 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations
- 31 U.S.C. 5317 and other pertinent provisions relating to monetary instruments
- 22 U.S.C. 401 and other laws relating to exports

Also, for further details select the following links to these directives:

- Directive 4410-001B, Guidelines for Detention and Seizures of Pornographic Materials
- Directive 1450-015, Disclosure of Business Confidential Information to Third Parties
- Directive 5240-005, Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051)
- Directive 2210-001A, Restrictions on Importation of Seditious Matter
- Directive 3340-032, Processing Foreign Diplomatic and Consular Officials
- Directive 3340-049, Border Search of Electronic Devices Containing Information