

Domestic Terrorism Issue Team Solution Approach FY23-27

Sub-Issue: Threat Analysis & Mitigation

Baseline Capability: AMCIT is a specialized team of collateral duty AMO Agents certified to conduct “in-the-field” exploitations of electronic devices across the United States and Caribbean. AMCIT are trained to extract and process data from all traditional devices and non-traditional ones (e.g., Small Unmanned Vehicles (Air and Maritime), manned vehicles and navigation systems of all complexities) and provide rapid response cyber forensic services to all CBP and its partners to include (b) (7)(E)

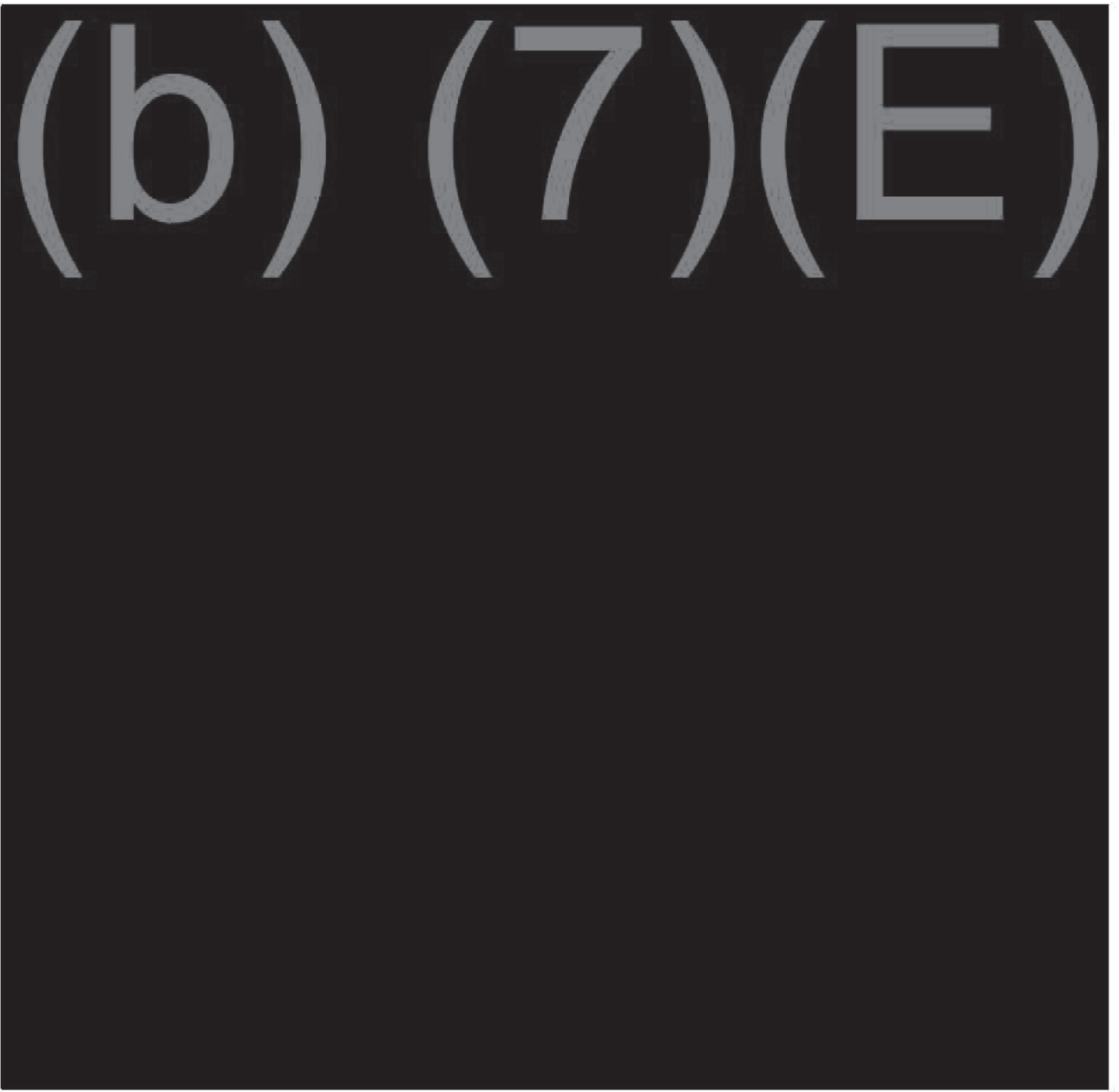
(b) (7)(E)

(b) (7)(E)

Requirement:

(b) (7)(E)

(b) (7)(E)



Solution Approach:

(b) (7)(E)



(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Instructions: Complete the following sections to outline the solution approach to closing the capability gaps of your organization associated with Domestic Terrorism mission spaces.

Sub-Issue: Information Sharing

Baseline Capability: Currently, U.S. Customs and Border Protection has numerous policies, MOUs/MOAs, and systems in place to facilitate the sharing of threat information with partners both foreign and domestic. There are broad information sharing and foreign release policies and procedures established. Many of the MOUs/MOAs are specifically written for a threat category or partner.

(b) (7)(E)

Requirement: No

Solution Approach:

(b) (7)(E)

(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Sub-Issue: Information Sharing

Baseline Capability: Office of Intelligence (OI) Security Division supports intelligence analysis and operations capabilities by providing security support for the CBP Intelligence Enterprise and the mission it supports. (b) (7)(E)

Capability Gap: (1) Lack of sufficient resources to procure, train, and maintain secure communications
(2) Lack of dedicated classified facilities to deliver classified intelligence products to deter and fight DVE
(3) CBP's gap in available secure communications facilities impedes CBP's timely execution of intelligence-based and data-driven operations

Requirement: DHS Directive 008-03 "Continuity Policy and Programs" requires the Secretary, Deputy Secretary, Component Heads, and Deputies, to participate in the Secretary-led secure communications or conferences – specifically the SLG conference – within 30 minutes of notifications. (b) (7)(E)

. The CBP Commissioner has directed the establishment of an effective strategy to address requirements for integrating secure communications architecture into all future facility construction and renovation projects. Timely access to all-source, classified information to inform CBP operational decision making has become increasingly more important in a dynamic and evolving threat environment.

Solution Approach:

(b) (7)(E)

(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Sub-Issue: Information Sharing

Baseline Capability: Office of Intelligence (OI) analysts assigned to its National Security Division's (NSD) Counterterrorism Branch conducts research and produces assessments associated with external DVE activities; and the NSD's Insider Threat Program and Analysis Branch partners with the Component's Office of Information Technology (OIT) and Professional Responsibility (OPR) to comprehensively prevent, deter, detect, and respond to internal DVE activities.

(b) (7)(E)

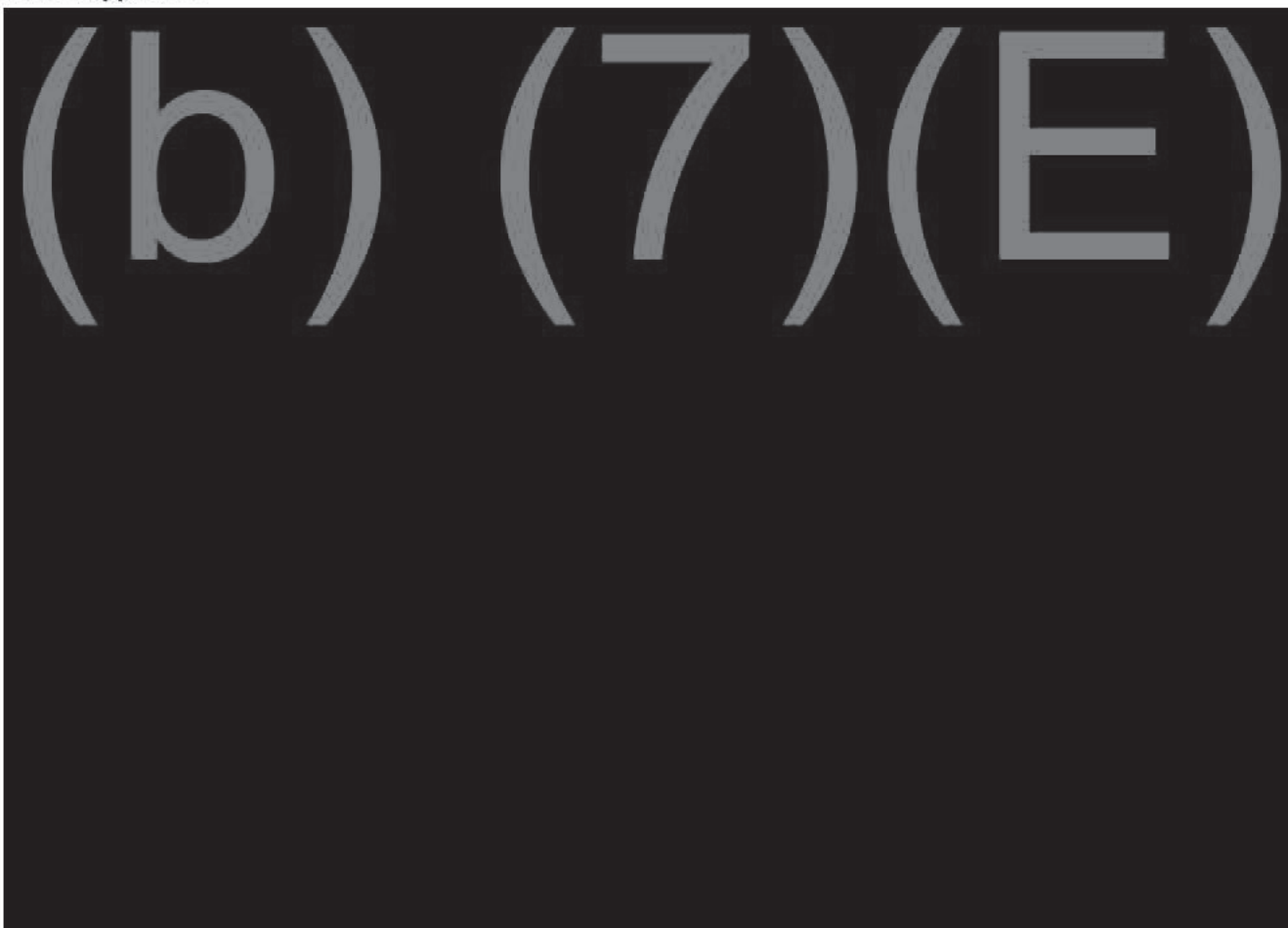
A large rectangular area of the document is redacted with a solid black box. The text "(b) (7)(E)" is visible in the top left corner of this redacted area.

Requirement: Establish external information sharing agreements with external law enforcement partners (b) (7)(E)

A rectangular area of the document is redacted with a solid black box. The text "(b) (7)(E)" is visible in the top left corner of this redacted area.

Solution Approach:

(b) (7)(E)

A large rectangular area of the document is redacted with a solid black box. The text "(b) (7)(E)" is visible in the top left corner of this redacted area.

Domestic Terrorism Issue Team Solution Approach FY23-27

Instructions: *Complete the following sections to outline the solution approach to closing the capability gaps of your organization associated with Domestic Terrorism mission spaces.*

Sub-Issue: Policy Development & Education

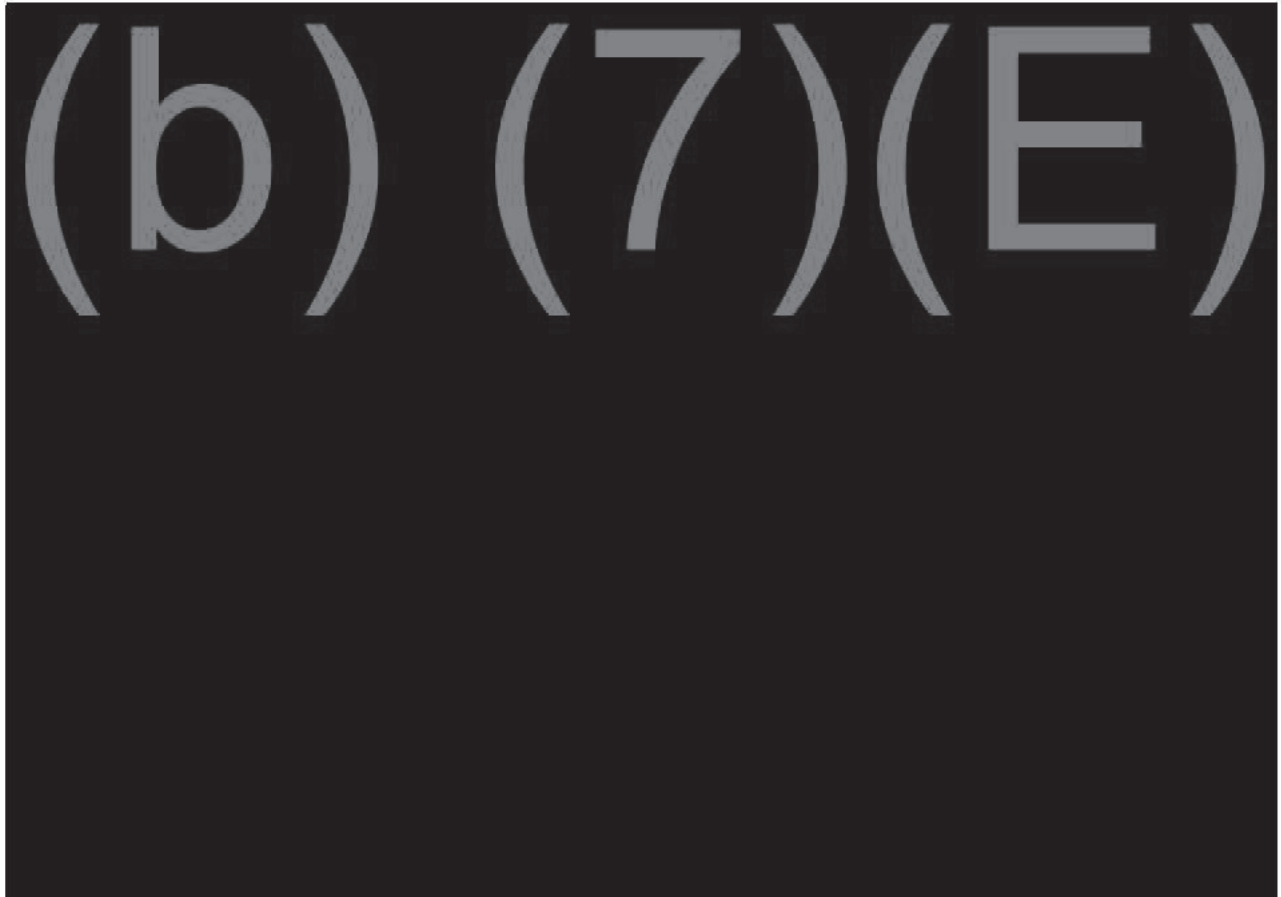
Baseline Capability: Currently, U.S. Customs and Border Protection has numerous policies, MOUs/MOAs, and systems in place to facilitate the sharing of threat information with partners both foreign and domestic. There are broad information sharing and foreign release policies and procedures established. Many of the MOUs/MOAs are specifically written for a threat category or partner.

(b) (7)(E)

A large black rectangular redaction box covers the majority of the content in this section. The text "(b) (7)(E)" is visible at the top left of the redacted area.

Requirement: No

Solution Approach:

A large black rectangular redaction box covers the entire content of the "Solution Approach" section. The text "(b) (7)(E)" is visible at the top left of the redacted area.

(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Sub-Issue: Policy Development & Education

Instructions: Complete the following sections to outline the solution approach to closing the capability gaps of your organization associated with Domestic Terrorism mission spaces.

Sub-Issue: Policy Development & Education

Baseline Capability: Office of Intelligence (OI) Training Division (OITD) supports intelligence analysis and operations capabilities through foundational and advanced intelligence training. The capabilities required to counter Domestic Terrorism (DT) response are supported by existing training. Research and analysis skills required to produce DT assessments are supported by the Intelligence Foundations Course, Systems Exploitation Training, and CBP Intelligence Support to Operations Course. OITD is working with the DHS Intelligence Training Academy to produce Counterintelligence and Insider Threat Training, as well as classified work environment training, that will prepare the CBP Intelligence Enterprise workforce to identify and address DVE threats.

(b) (7)(E)

Requirement: Establish a CBP Intelligence Training Academy (ITA) and satellite training capacity capable of offering integrated, requirements-based, homeland security mission focused, intelligence tradecraft training programs at all security classification levels to the IE workforce to address all threats, all the time, especially including DT threats. IE training plays a critical role in the promulgation of CBP authorities, policy, and legal requirements to the workforce and helps to ensure safe, secure, and legally compliant operations. These initiatives address the HR 644 Trade Facilitation and Trade Enforcement Act [STAT 204] mandate to (A) develop, provide, coordinate, and implement intelligence capabilities into a cohesive intelligence enterprise to support the execution of the duties and responsibilities of U.S. Customs and Border Protection”

Solution Approach:

(b) (7)(E)

(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Sub-Issue: Policy Development & Education

Baseline Capability: CBP employees are required to complete the Department of Homeland Security's Insider Threat Awareness Training after being hired and every 2 years thereafter.

(b) (7)(E)

Requirement: Yes, Department of Homeland Security Directives System, Instruction Number 262-05-002, Revision Number 01, Issued 10/1/2019 Insider Threat Program.

Solution Approach:

(b) (7)(E)

(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Instructions: Complete the following sections to outline the solution approach to closing the capability gaps of your organization associated with Domestic Terrorism mission spaces.

Sub-Issue: Threat Analysis

Baseline Capability: U.S. Customs and Border Protection conducts threat analysis of a myriad of threat categories that relate to the agency's mission and authorities. These threats are transnational in nature.

(b) (7)(E)

Requirement: No

Solution Approach:

(b) (7)(E)

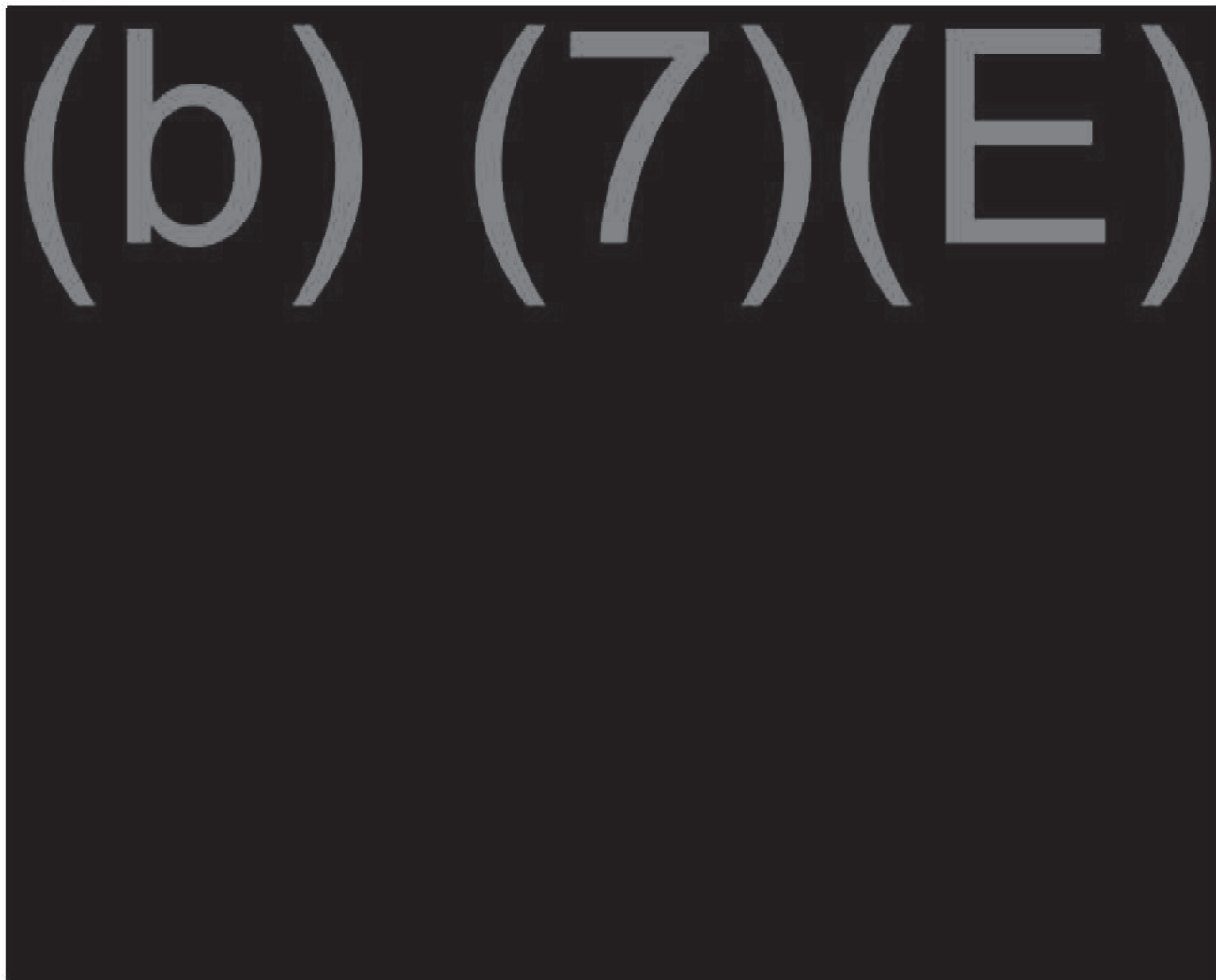
(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Sub-Issue: Threat Analysis & Mitigation

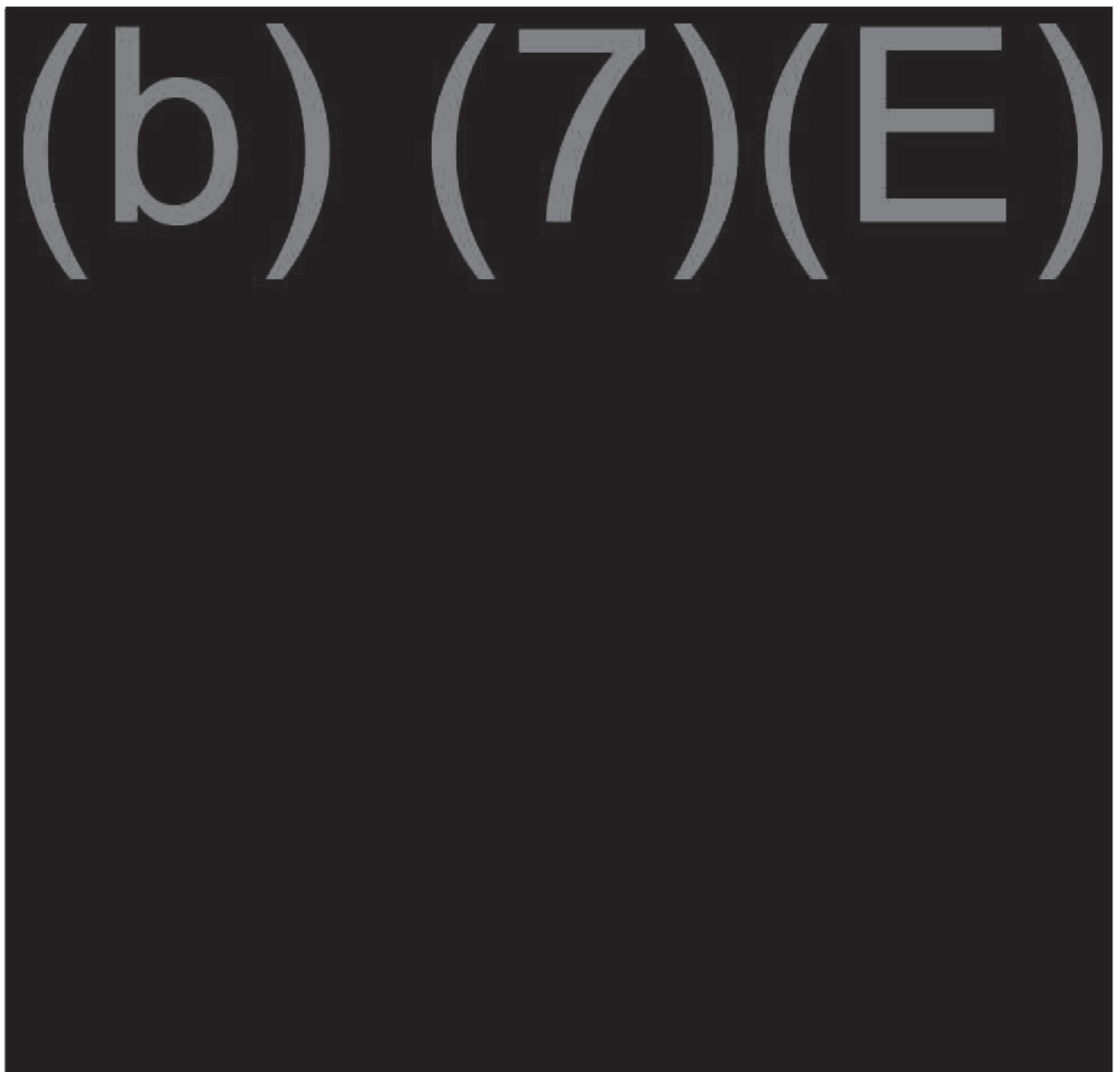
Baseline Capability: AMCIT is a specialized team of collateral duty AMO Agents certified to conduct “in-the-field” exploitations of electronic devices across the United States and Caribbean. AMCIT are trained to extract and process data from all traditional devices and non-traditional ones (e.g., Small Unmanned Vehicles (Air and Maritime), manned vehicles and navigation systems of all complexities) and provide rapid response cyber forensic services to all CBP and its partners to include (b) (7)(E)

(b) (7)(E)



Requirement:

(b) (7)(E)



Solution Approach:



(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Domestic Terrorism Issue Team Solution Approach FY23-27

Sub-Issue: Threat Analysis & Mitigation

Baseline Capability: NSD has a line of effort dedicated to identifying and triaging potential insider threat incidents, to include those incidents related to DVE activities.

(b) (7)(E)

Requirement: Yes, CBP's Insider Threat Operations Center Concept of Operations dated October 20, 2020.

Solution Approach:

(b) (7)(E)