Page 01 of 29

Withheld pursuant to exemption

of the Freedom of Information and Privacy Act

Behavior Analysis Capability (BAC) Risk Based Allocation Methodology

Phase I: Final Report
July 2012

Table of Contents:

~~WARNING: This document contains [illegible] information that is controlled under 49 CFR Part 1520. No part of this document [illegible] persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the [illegible] Transportation Security Administration [illegible] may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.~~

Executive Summary

Key Take-Aways:

Phase I of the risk-based allocation analysis concluded that:

(b)(3):49 U.S.C. § 114(r),(b)(5) [redacted]

Approach

The Systems Analysis Branch (SAB) within the Mission Analysis Division (MAD) was tasked with developing a risk-based methodology to determine the optimal allocation of the behavior analysis capability (BAC) across the country. The analysis focused on answering the following questions:

1. How much coverage does the current Behavior Detection Officer (BDO) allocation provide? (b)(3) [redacted] (b)(3):49 U.S.C. § 114(r),(b)(5) [redacted] are there enough Full-Time Equivalency (FTE) to observe and assess every passenger?
2. (b)(3):49 U.S.C. § 114(r),(b)(5) [redacted]
3. If additional behavior analysis capabilities (BDO or otherwise) are appropriated, where should they be allocated? (b)(3):49 U.S.C. § 114(r),(b)(5) [redacted] (b)(3):49 U.S.C. § 11 [redacted]

Phase I of this analysis focused on analyzing the above questions given the current Screening of Passengers by Observation Techniques (SPOT) parameters: BDOs work full time (8 hours per day, 5 days per week) in teams of two (b)(3):49 U.S.C. § 114(r),(b)(5) [redacted]

(b)(3):49 U.S.C. § 114(r),(b)(5) [redacted]

WARNING: [illegible] Information that is controlled under 49 CFR Part 1520. No part of this document may be [illegible] without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of [illegible] Washington, DC. Unauthorized release may result in civil penalty or other action. [illegible] agencies, public release is governed by 5 U.S.C. 552

(b)(3):49 U.S.C. § 114(r) [redacted]

(b)(3):49 U.S.C. § 114(r) [redacted]

(b)(3):49 U.S.C. § 114(r) [redacted]

CAT X, I, and II airports represent 97% of all domestic passenger traffic. (b)(3):49 U.S.C. § 114(r) [redacted]

(b)(3):49 U.S.C. § 114(r) [redacted]

(b)(3):49 U.S.C. § 114(r) [redacted]

(b)(3):49 U.S.C. § 114(r) [redacted]

[2] The detailed description of this calculation is in Section V.

WARNING: [illegible] Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released [illegible] as defined in 49 CFR 1520, except with the written permission of the Administrator [illegible] Washington, DC. Unauthorized release may result in civil [illegible] Government agencies, public release is governed by 5 U.S.C. 552.

(b)(3):49 U.S.C. § 114(r) [redacted]

Options for Implementation

The following analysis is a high level assessment of current BDO coverage, and recommends methods for allocating the behavior analysis capability to maximize security effectiveness. To make this method a valid analytical solution for BAC allocation and staffing, we recommend creating an implementation plan to outline roles and responsibilities. One potential implementation model is outlined below:

- **Mission Analysis Division, Systems Analysis Branch (SAB):** (b)(5) [redacted] (b)(3):49 U.S.C. § [redacted] (b)(3):49 U.S.C. § 114(r),(b)(5) [redacted]
- **Scheduling & Staffing (S&S):** (b)(5) [redacted] (b)(3):4 [redacted] (b)(3):49 U.S.C. § 114(r),(b)(5) [redacted] (b)(5) [redacted] (b)(5) [redacted]
- **Behavior Detection and Analysis Division (BDAD):** (b)(5) [redacted] (b)(5) [redacted]

Key Terms

Below are the definitions of key risk terms:

- **Threat:** Threat is the *intent* and *capability* of an adversary to complete a given attack.
- **Vulnerability:** Vulnerability is a combination of the countermeasures in a system and the degree of difficulty of completing an attack.
- **Consequence:** Consequence is the total direct and indirect cost of an attack. In this case it will remain *constant*, as the destruction of a single aircraft with an explosive.
- **Probability of Encounter (P(e)):** The probability that a BDO will meaningfully observe a passenger at a checkpoint where they are staffed and working. This is the best-available proxy for the likelihood that a BDO would encounter an adversary.
- **Probability of Detection:** The likelihood that a BDO will route an adversary to high risk screening.
- **Security Effectiveness:** Given that a BDO observes and meaningfully assesses an adversary (Probability of Encounter), the likelihood that the adversary will be routed to high risk screening (Probability of Detection).

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.

Introduction and Analytic Framework

WARNING: This document [illegible] Information that is controlled under 49 CFR Part 1520. No part of this document may be [illegible] a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the [illegible] Washington, DC. Unauthorized release may result in civil penalty [illegible] government agencies, public release is governed by 5 U.S.C. 552.

Introduction

The Transportation Security Administration uses multiple layers of countermeasures to create an unpredictable, effective security checkpoint. Behavior analysis serves as an integral layer of security that uses behaviors and activities that deviate from an established environmental baseline to identify potential adversaries trying to defeat the security process. The role of the behavior analysis capability (BAC) will become even more critical in the Risk-Based Security (RBS) strategy, as the BAC is used to conduct real-time threat assessments to ensure that unknown adversaries are routed towards higher security and away from lower security.

Screening of Passengers by Observation Techniques, or SPOT, was implemented in 2006 as a means of assessing passengers and routing potentially high risk passengers to selectee screening. Selection of high risk passengers is based upon the appearance of behavioral idiosyncrasies that indicate mal-intent and fear of discovery. Since its inception, SPOT has extended to 176 airports, with just under 3,000 Behavior Detection Officers (BDOs) allocated in 2011. This number was boosted slightly above 3,000 in March, with an additional allocation of 145 BDOs.

BDOs are currently allocated using a combination of (b)(3) 49 U.S.C. § 114(r) [redacted] The responsibility for developing the allocation scheme moved between BDAD and S&S in past years. The current allocation numbers use the existing locations from the BDAD allocation, along with the following framework from S&S:

(b)(3) 49 U.S.C. § 114(r) [redacted]

3. Finally, daily SPOT hours are converted to weekly hours, and the required FTE count is determined (rounding up).

The SAB was tasked to review the current BDO distribution (b)(3) 49 U.S.C. § 114(r) [redacted] and develop a risk-based method for allocating the BAC nationwide. This would ensure that (b)(3) 49 U.S.C. § 114(r) [redacted] to maximize risk reduction and would address potential concerns around (b)(3) 49 U.S.C. § 114(r) [redacted]

Analytic Framework

The goal of this analysis is to improve overall system security effectiveness by placing BAC resources (b)(3) 49 U.S.C. § 114(r) [redacted] To do this we must first identify the adversary we are defending against. (b)(3):49 U.S.C. § 114(r) [redacted] Where should we allocate a BAC to provide the largest increase in system effectiveness?

(b)(3):49 U.S.C. § 114(r) [redacted]

~~WARNING: [redacted] document contains sensitive security information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.~~

(b)(3):49 U.S.C. § 114 (r) Adversary Analysis

WARNING: [illegible] that is controlled under 49 CFR Part 1520. No part of this document may be released [illegible] need to know, as defined in 49 CFR 1520, except with the written permission of the [illegible] Security Administration, Washington, DC. [illegible] U.S. Government agencies, public release is governed by 5 U.S.C. 552.

Key Conclusions

(b)(3) 49 U.S.C. § 114(r) [redacted]

Analytic Approach and Assumptions

(b)(3) 49 U.S.C. § 114(r) [redacted]

(b)(3) 49 U.S.C. § 114(r) [redacted] If BDOs were allocated to *fully cover* the throughput at CAT X-II airports, then they would be covering approximately 97% of the traveling population, (b)(3) 49 U.S.C. § 114(r) [redacted]

(b)(3) 49 U.S.C. § 114(r) [redacted]

[3] PACE testing measures the professional performance of TSOs. ASAP uses covert testing to evaluate TSO standard operating procedure compliance and resolution capability. A more in-depth description of these tests can be found in Section V.

WARNING: [redacted] information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons ... as defined in 49 CFR 1520, except with the written permission of the Administrator ... Washington, DC. Unauthorized release may result in civil penalty ... U.S. Government agencies, public release is governed by 5 U.S.C. 552.

(b)(3):49 U.S.C. § 114(r) [redacted]

Range Analysis: Determining BDO Coverage Based on Workload

(b)(3):49 U.S.C. § 114(r) [redacted] TSA does not currently have a standard measure for BDO coverage at airports, so we used workload calculations to determine the number of BDOs required for 100% coverage. Because there is uncertainty surrounding BDO coverage, we used a *parametric approach* for the calculations. (b)(3):49 U.S.C. § 114(r) [redacted]. The definitions of the *best* and *worst case* scenarios are in the table below:

Variable	Definition	Best Case	Worst Case
Observation Time:	(b)(3):49 U.S.C. § 114(r) [redacted]		
Fatigue Degradation			
Traffic Inefficiency			

~~WARNING: ... Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released ... without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration ... Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.~~

(b)(3):49 U.S.C. § 114(r)

[redacted]

Calculations

(b)(3):49 U.S.C. § 114(r)

[redacted]

We calculated the answers based on the following steps:

WARNING: [illegible] Information that is controlled under 49 CFR Part 1520. No part of this document may be released [illegible] as defined in 49 CFR 1520, except with the written permission of the [illegible] Administration, Washington, DC. Unauthorized release may result in civil [illegible] Government agencies, public release is governed by 5 U.S.C. 552.

1) Calculate Teams Needed for an Hour:

A workload equation allowed us to calculate staffing requirements for BDOs at a peak hour, and therefore determine how many teams would be required for full coverage at a given hour. The equation included the "fixed workload" of observing passengers in the queue (i.e. how much time does it take to observe and assess each passenger?), as well as the "created workload" of SPOT referral screening (i.e. once a referral is identified, how long does it take to process and resolve?).

The total time requried to process a given number of passengers per hour (in this analysis we considered peak hours), was calculated using the following equation:

$$Total\ processing\ time = \frac{Fixed\ Workload\ Seconds + Created\ Workload\ Seconds}{60}$$

Where,

$$Fixed\ Workload = (Throughput * P(e)) * Average\ Encounter\ Time$$

$$Created\ Workload = (Throughput * Referral\ Rate) * Average\ Referral\ Time$$

(b)(3):49 U.S.C. § 114(r)

[redacted]

2) Calculate Teams Needed for a Year:

Because the workload calculations did not incorporate variables to determine staffing beyond an hour, we next factored in traffic inefficiency and fatigue. TSA's staffing model, ESM, takes into consideration the ebbs and flows of traffic at each checkpoint in the system nationally. However, this is beyond the purview of a high level risk analysis. Rather, the task here is to understand current BDO coverage and determine how to allocate additional BDOs using a risk-informed method. Therefore, we calculated traffic inefficiency at a very high level, using a degradation factor that considers BDO utilization.

This calculation uses hourly throughput and BDO hourly capacity to determine the average over or under-utilization. Because checkpoint traffic has peaks and valleys, the traffic inefficiency metric was used to determine the percent of time there would be either too many or too few BDOs at a checkpoint to cover the throughput. This is unavoidable due to staffing in 8-hour shifts. We used the following formula:

$$Traffic\ Inefficiency = \frac{\sum_{i=1}^{n}\left(\frac{\left\lceil \frac{Throughput\ of\ Checkpoint\ n}{(Hours\ Open * 365)} \right\rceil}{BDO\ Capacity\ per\ Hour}\right)}{Total\ Number\ of\ Checkpoints}$$

(b)(3) 49 U.S.C. § 114(r)

[redacted]

3) *Combine into a Comprehensive National-Level Model*

WARNING: ... is controlled under 49 CFR Part 1520. No part of this document may be released to persons without ... defined in 49 CFR 1520, except with the written permission of the Administrator of the ... Unauthorized release may result in civil penalty ... government agencies, public release is governed by 5 U.S.C. 552.

Finally, we combined each previous variable and calculation into a single formula. Based on this model, we were able to determine the coverage levels associated with current allocation numbers and BDO utilization. BDO utilization includes degradation for hours paid not worked, playbook, and administrative time. The following equation was used to determine the total number of teams (b)(3):49 U.S.C. § 114(r) (b)(3):49 U.S.C. § 114(r)

$$Teams = \left(\frac{Total\ Processing\ Time}{Yearly\ Working\ Hours}\right) * Fatigue\ Degradation * Traffic\ Inefficiency * BDO\ Utilization$$

Using these calculations and assumptions, we examined the 2011 allocation numbers to determine if the current staffing provided enough FTE to screen 100% of the passengers traveling through (b)(3):49 U.S.C. § 114(r) (b)(3):49 U.S.C. § 114(r) We included a best and a worst case scenario using the assumptions described above.

The fatigue degradation and traffic inefficiency variables are both crucial elements to convert the BDO staffing requirement for a peak *hour* into a daily or yearly estimate of BDO FTE required for certain coverage levels. The final staffing equation also considers BDO utilization, or the amount of time spent performing SPOT at the checkpoint, to determine the number of teams needed to observe and assess a given throughput level.

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552

(b)(3):49 U.S.C. § 114 (r) Adversary Analysis

WARNING: [illegible] Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this [illegible] released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission [illegible] of the Transportation Security [illegible] Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.

Key Conclusions

(b)(3):49 U.S.C. § 114(r)

[redacted]

Approach and Assumptions

(b)(3):49 U.S.C. § 114(r)

[redacted]

(b)(3):49 U.S.C. § 114(r)

[redacted] e highly trained with a highly sophisticated leader, large budget, and the ability to enact complicated attack scenarios. Because they have the ability to gather information about the aviation system and to conduct trial runs, they will seek out the weakest link in the system to maximize the probability of their attack succeeding as seems to have occurred with the 9/11 example cited at the beginning of this paper.

(b)(3):49 U.S.C. § 114(r)

[redacted]

... Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released ... as defined in 49 CFR 1520, except with the written permission of the ... Washington, DC. Unauthorized release may result in civil penalty or other ... government agencies, public release is governed by 5 U.S.C. 552.

(b)(3):49 U.S.C. § 114(r) [redacted]

Calculations

Data Assessments for Threat and Vulnerability

(b)(3):49 U.S.C. § 114(r) [redacted] (b)(3):49 U.S.C. § 114(r) [redacted] To do this, we assigned each (b)(3):49 U.S.C. § 114(r) [redacted] a threat and a vulnerability score. Those scores were based on an assessment of equipment coverage, performance, and CATA scores. The data inputs and calculations are outlined below:

(b)(3):49 U.S.C. § 114(r) [redacted]

WARNING: [redacted] This document contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public release is governed by 5 U.S.C. 552.

Page 18 of 29

Withheld pursuant to exemption

(b)(3):49 U.S.C. § 114(r)

of the Freedom of Information and Privacy Act

Page 19 of 29

Withheld pursuant to exemption

(b)(3):49 U.S.C. § 114(r)

of the Freedom of Information and Privacy Act

(b)(3):49 U.S.C. § 114(r)

[redacted]

The risk percentage represents the level of risk concentrated in (b)(3):49 U.S.C. § 114(r) [redacted] out of a total of 100 possible points. This provides a relative understanding of (b)(3):49 U.S.C. § 1 [redacted] adversary risk distribution across the system, but does not measure absolute or relative security effectiveness. The final Risk equation is:

$$Risk = (Threat\ Percentage * Vulnerability\ Percentage)$$

(b)(3):49 U.S.C. § 114(r)

[redacted]

~~WARNING: [illegible] s document contains [illegible] that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without [illegible] as defined in 49 CFR 1520, except with the written permission of the Administrator of the [illegible] DC. Unauthorized release may result in civil penalty [illegible] Government agencies, public release is governed by 5 U.S.C. 552.~~

Combined Methodology

~~WARNING: [illegible] Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document [illegible] a need to know, as defined in 49 CFR 1520, except with the written permission of the [illegible] Security Administration, Washington, DC. Unauthorized release may result in civil [illegible] U.S. Government agencies, public release is governed by 5 U.S.C. 552.~~

After developing allocation methodologies to defend against (b)(3):49 U.S.C. § 114(r) [redacted] adversary types, the challenge we faced was to combine both methods to determine an overarching allocation recommendation for future BAC deployments.

To create a single allocation recommendation (b)(3):49 U.S.C. § 114(r) [redacted] (b)(3):49 U.S.C. § 114(r) [redacted] The purpose of such an assumption is to give a reasonable recommendation in a vacuum of adversary information, and this calculation could be easily updated with a more accurate assumption of the adversary breakdown based on any input we might receive from TSA Office of Intelligence.

(b)(3):49 U.S.C. § 114(r) [redacted]

~~WARNING: [illegible] document [illegible] Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without [illegible] defined in 49 CFR 1520, except with the written permission of the Administrator [illegible] Administration, Washington, DC. Unauthorized release may result in civil penalty or other [illegible] government agencies, public release is governed by 5 U.S.C. 552.~~

Allocation Stopping Points and Cost-to-Security Comparisons

Although Figure 5 would provide useful insights for determining an initial allocation of the BAO (b)(3):49 [redacted] (b)(3):49 U.S.C. § 114(r) [redacted] (b)(3):49 U.S.C. § [redacted]

(b)(3):49 U.S.C. § 114(r) [redacted]

An alternative stopping point would be used in the future, when more robust data surrounding BDO Probability of Detection is available at a statistically significant level. This methodology would calculate the relative difference in security effectiveness between (b)(3):49 U.S.C. § 114(r) [redacted] We would then calculate the level of BDO coverage needed to fill those security gaps. This methodology could be used in the long term staffing calculations.

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.~~

Constraints and Trade Space Considerations

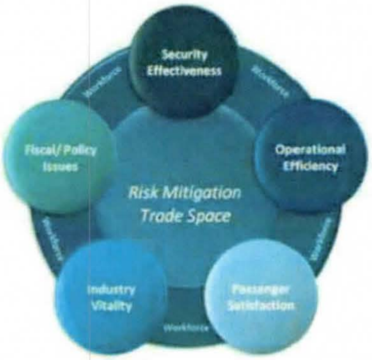
WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public release is governed by 5 U.S.C. 552.

Constraints

As previously described, this is a high-level risk analysis designed to provide insight into overall, national BDO distribution and allocations. It does not provide the detail required to determine precise FTE requirements or staffing levels, and does not analyze allocation at the [redacted]

Likewise, BDO security effectiveness values remain uncertain, so we did not calculate a robust cost-to-security ratio. Future analysis will focus more heavily on BDO effectiveness and return on investment calculations.

Trade Space Considerations and Phase II Analysis



Phase I helps us understand where risk is most concentrated in the system and how the BAC can help to compensate for that risk. [redacted] However, there are other considerations that may make this recommendation less feasible using the current SPOT CONOPs.

Cost and operational viability are two considerations that will drive allocation implementation. [redacted]

The table below shows how many BDO FTE would be needed to screen 100,000 passengers at a minimum of [redacted] P(e). [redacted]

[redacted]

defined in 49 CFR 1520, except with the written permission of the Administrator of the [illegible] Washington, DC. Unauthorized release may result in civil penalty or other [illegible] government agencies, public release is governed by 5 U.S.C. 552.

(b)(3):49 U.S.C. § 114(r)

[redacted]

WARNING: [illegible] Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to [illegible] as defined in 49 CFR 1520, except with the written permission of the [illegible] Administration, Washington, DC. Unauthorized release may result in civil [illegible] action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.

Recommendations and Conclusions

WARNING: [illegible] Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without [illegible] defined in 49 CFR 1520, except with the written permission of the [illegible] Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552.

Recommendation Option

The methodology outlined above provides a high level framework for determining where to place additional BAC resources and how to distribute them nationally to maximize security. One potential model for implementation (b)(5) [redacted]

(b)(5) [redacted]

(b)(5) [redacted]

(b)(5) [redacted]

(b)(3) 49 U.S.C. § 114(r),(b)(5) [redacted]

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the Administrator of the Transportation Security Administration, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public release is governed by 5 U.S.C. 552.~~

(b)(3):49 U.S.C. § 114(r)

Conclusions

1. (b)(3):49 U.S.C. § 114(r)

   This calculation is based on (b)(3):49 U.S.C. § 114(r) and does not consider queue configurations or staffing limitations.

(b)(3):49 U.S.C. § 114(r)

~~WARNING: [illegible] Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this document may be released to persons [illegible] defined in 49 CFR 1520, except with the written permission of the Administrator of [illegible] Washington, DC. Unauthorized release may result in civil penalty or other [illegible] government agencies, public release is governed by 5 U.S.C. 552.~~