



HOMELAND SECURITY STRATEGIC PLANNING: THE ROAD AHEAD ALIGNING CAPABILITIES WITH RISKS

OVERVIEW

Over the last several years, significant investment has been made in the preparedness capabilities of all levels of government to prevent, protect against, respond to, and recover from catastrophic events. The nature of these investments has evolved over time, moving from basic equipment purchases to in-depth planning and tactical training and exercising. This evolution has now led states and urban areas to assess their current state of preparedness using quantifiable, risk-based metrics and to demonstrate actual capability through performance-based testing.

The lessons of the recent past have shown us that risk is dynamic; the types and magnitude of potential threats we face continually evolve as environments change and adversaries adapt. We must therefore analyze our all-hazards risk profile and the impact of past and ongoing preparedness investments to identify and quantify gaps that may exist in prevention, protection, response, and recovery capabilities. This review requires a rigorous approach that is risk-based, measurable, and repeatable, and that answers five critical preparedness questions, which in turn can effectively drive implementation of homeland security strategy:

What capability is needed?
How much capability is needed?
Where is it needed?
How much will this capability cost?
How do we validate the capability exists?

APPROACH

A rigorous process to answer these questions will enable continuous evaluation of risks and capabilities, and ensure that the right investments are being made to best manage risk in an environment of limited resources by repeatedly *identifying* capability gaps, *investing* resources to close the gaps, and *testing* through exercises to ensure actual performance. Accomplishing this requires the development of:

- a) A credible risk picture using the best risk models available and drawing upon relevant data from the state, region and federal government;
- b) A capability framework that brings into alignment risk, capability targets, and resource allocation in a way that can enable investment priorities and decision making to be driven by a balancing of risk mitigation, capability gain, and cost; and
- c) A standardized way to measure progress and improvements.

This paper describes a proposed CNA/Digital Sandbox, Inc. approach for these activities.

Creating Your Risk Management Program

STEP 1: BASELINE ANALYSIS OF RISK AND CAPABILITIES

The Baseline Analysis will create a risk/capability “portfolio” for homeland security policy makers and will give planners a starting point in identifying their homeland security program priorities and justifying federal grant and organizational budget investments (past, present, and future).

1.1 DEVELOP A RISK BASELINE

We will analyze risks to your jurisdiction from terrorist threats and natural hazards. We will use authoritative, vetted models for asset and population risk to determine how your critical infrastructure and people are at risk. For this analysis, we will work with your existing data and subject matter experts to ensure that the outputs reflect the best available information. The outputs from this process will be a full report on risk by jurisdiction, by CI/KR sector, and by threat/hazard theme. Our expert risk analysts interpret your analytic results to provide insight into the sources of risk, and the most appropriate risk mitigation measures indicated by the risk.

1.2 ANALYZE PROGRAM SPENDING AND CURRENT CAPABILITIES

We will conduct a review of existing, relevant Federal, State and local capability assessments and documentation. We will document the type, quantity and quality of information available, and then use it to identify trends and to characterize current capability levels. We will identify patterns in findings from different assessment activities and synthesize results to inform strategic priorities and program implementation. We will also analyze your historical spending (including DHS/HHS grants and other resources) across solution areas and capabilities and develop an initial spending baseline to evaluate spending relative to risk and capabilities.

1.3 DEVELOP A CAPABILITY BASELINE

We will produce a Capability Baseline report that will: identify your risk-based priority capability areas, identify trends and characterize your current capability levels, analyze historical homeland security program spending relative to risks and capabilities, and identify downstream opportunities for enhanced return on preparedness investment.

STEP 2: RISK MANAGEMENT PROGRAM INITIALIZATION

Program initialization activities will utilize the baseline analyses to support facilitated planning sessions centering on identification of strategic, risk-based priorities for homeland security initiatives. These sessions will also be used to support development of a Risk Management Program Concept of Operations (CONOPS) that will support planning, resource requests and prioritization, and performance testing and evaluation.

2.1 ESTABLISH HOMELAND SECURITY STRATEGIC PRIORITIES

We will conduct facilitated workshops at the local, regional, and/or State levels to establish risk-based homeland security strategic priorities. We will produce a final workshop report compiling the output of all the workshops. This report will support application of strategic priorities to near- and long-term decision making, including allocation of current year DHS grant funding and request for future funding from Federal, State, and local sources.

Creating Your Risk Management Program

2.2 BUILD CONCEPT OF OPERATIONS FOR RISK MANAGEMENT PROGRAM

We will apply the results of baseline analyses and regional strategic priority identification to outline the tasks and cycle for your jurisdiction's comprehensive homeland security risk management program. With help from a working group, we will then develop a draft homeland security risk management program CONOPS. This document will frame at a conceptual level an approach to implementing a risk management program for homeland security, identifying options for how to incorporate the full suite of activities that comprise risk management, how to sequence and when to execute certain actions, and how to involve stakeholders in governance and project execution. Risk assessment, capabilities assessment, governance, strategic and operational planning, resource allocation, and performance testing will be addressed.

STEP 3: MODELING AND IN-DEPTH ANALYSIS

The Modeling and In-Depth Analysis phase will provide your jurisdiction with the tools needed to maintain a dynamic understanding of its risk, analyze capability requirements and estimate the costs associated with meeting those requirements.

3.1 ESTABLISH RISK-BASED CAPABILITY TARGETS AND IDENTIFY GAPS

Using the Risk Baseline, we will identify your priority capability areas; we will then use a capability calculation methodology to "scale" capability requirements which can be compared to existing capability levels to identify gaps. Incorporating all relevant Federal guidelines, our end product will be specific, measurable capability targets (e.g., team based targets, response time targets) for your priority capabilities.

3.2 ESTIMATE COSTS ASSOCIATED WITH CAPABILITY DEVELOPMENT AND SUSTAINMENT

We will apply life-cycle costing models to estimate costs associated with achieving and sustaining your capability targets identified in 3.1. These models account for all costs associated with acquiring and maintaining a capability over its life, including initial costs, energy costs, operating costs, repair costs, upgrade costs, and personnel costs. This information can then be used to drive your jurisdiction's homeland security strategic planning and budgeting processes.

3.3 PROVIDE ONGOING RISK ANALYSIS SERVICES

We will provide you with ongoing, subscription-based risk analysis services through Digital Sandbox's Risk Analysis Center. This will include a customized risk portal, data storage and hosted Site Profiler software applications to support your jurisdiction's ongoing CI/KR cataloging, Threat/Hazard Analysis, Security/Vulnerability Assessment, and Risk Analysis needs. Data and synthesized reports will be available providing local, regional, and State level views and will support establishment and updating of your Priority CI/KR Tier structure; periodic analysis of your CI/KR catalog to ensure data quality and completeness; transfer of data to the Federal Government's Automated Critical Asset Management System (ACAMS) as needed, and support to responses to various DHS Data Calls.

Creating Your Risk Management Program

STEP 4: INSTITUTIONALIZATION AND VALIDATION

Institutionalization and Validation will enable your to fully incorporate risk-based planning processes into your overall homeland security program. This phase will provide your jurisdiction with updated homeland security priorities and courses of action that are based on reproducible data and analysis, as well as an exercise and evaluation (E&E) CONOPS to support a comprehensive performance testing program.

4.1 REFINE REGIONAL HOMELAND SECURITY STRATEGIC PRIORITIES AND APPLY TO NEAR- AND LONG-TERM PROGRAMMATIC ACTIVITIES

We will conduct facilitated workshops to refine your risk-based homeland security strategic priorities, using capability targets and cost estimates. Workshop participants will review the results of previous analysis use this information to refine their priorities. We will support your jurisdiction in using these priorities, along with the risk and capabilities analyses, to drive requests for future DHS grant funding and final allocation of funds across your program needs. We will also support formalization of recurring strategic planning processes that draw upon dynamic risk and capabilities analyses and are aligned with DHS program cycles.

4.2 PERFORMANCE-BASED TESTING AND VALIDATION OF CAPABILITIES

We will develop a CONOPS and program plan an effective, risk- and capabilities-based exercise and evaluation program. This will include how to sequence and when to execute certain actions as part of a larger risk management program. It will also provide a process for using the results of the risk and capabilities assessment to set exercise program goals and select the specific exercise types, objectives and scenarios, and will provide cyclical schedules for planning, conducting, and evaluating exercises, and tracking of corrective actions.

MOVING FORWARD

CNA, a non-profit research and analysis organization, and their corporate partner, Digital Sandbox, have teamed to deliver this vital service. We are committed to working with jurisdictions to help them construct a robust risk-based planning and assessment architecture to serve them now and in the future. As one of the architects of the Department's risk-based methodology and its capability-based planning structure, including the initial development of the target capabilities list, we are uniquely qualified to provide this service.

As a non-profit organization, your State or urban area can contract with us directly through a cooperative agreement, can consider a sole source contract because we are unique providers of key aspects of this work, or we can respond to a request for proposal in a competitive process.

For further information, contact CNA Safety and Security at (703) 824-0007, or visit us at www.cna.org.