The Bay Area Homeland Security Strategy and Implementation Plan
2012 – 2015

October 2013

Table of Contents

BAY AREA HOMELAND SECURITY STRATEGY SUMMARY

Background

Homeland Security is the coordinated effort to ensure the entire Bay Area region is prepared to prevent, protect against, mitigate, respond to and recover from threats and acts of terrorism and other man-made or natural catastrophes. It requires a risk management process in order to ensure the region has the right capabilities in place to manage those hazards that pose the greatest risk to the Bay Area, its people, and its critical infrastructure and key resources. The threat of catastrophic events, both natural and man-made, requires continuous attention and strategic commitment from all levels of government, the private sector and the general public. The Bay Area is committed to this effort.

The Urban Areas Security Initiative (UASI) program provides financial assistance to address the unique multi-discipline planning, organization, equipment, training, and exercise needs of high-threat, high-density urban areas, and assists those urban areas with supplemental funding to build and sustain capabilities to prevent, protect against, mitigate, respond to, and recover from threats or acts of terrorism and other major hazards. Working together, the entire Bay Area UASI has strived to integrate preparedness activities, especially preparedness planning at the strategic level. This homeland security strategy represents the latest effort in that regard.

Purpose

The purpose of the *Bay Area Homeland Security Strategy* (*"Bay Area Strategy"* or *"Strategy"*) is to ensure the Bay Area region has a comprehensive document and system that outlines the region's risks, capabilities, vision, structure, goals and objectives for homeland security. Having such a *Strategy* will ensure the Bay Area is in the best possible position to clearly track and articulate its risk and capability needs to local leaders, the State of California and the U.S. Department of Homeland Security (DHS) when seeking resources and funding to enhance homeland security and public safety across the region.

The *Strategy* is designed primarily to address terrorism risk faced by the Bay Area with an understanding that capabilities enhanced to combat terrorism often enhance the ability to also manage natural disasters, such as earthquakes, and man-made accidents, such as hazardous materials spills. The *Strategy* outlines a comprehensive system for enhancing regional capability and capacity that will guide the Bay Area's efforts to:

- Prevent and disrupt terrorist attacks
- Protect the people of the Bay Area, its critical infrastructure and key resource
- Mitigate the damage caused by acts of terrorism, natural disasters and man-made accidents
- Respond to and recover from major incidents that do occur
- Continue to strengthen our preparedness foundation to ensure our long-term success
- Guide future investments, increase capabilities and reduce risk

Finally, the *Strategy* does not alter the statutory or regulatory authority or responsibility of any agency in the Bay Area related to public safety, health, and security. Nor does the *Strategy* impose any affirmative duty for any jurisdiction or entity to take any action or inaction concerning public health, safety, or security. Rather, the *Strategy* is designed as an integration tool and guide to better coordinate and focus those often disparate authorities and resources spread across the region necessary to achieve homeland security.

Vision

The Bay Area's vision for homeland security is a secure, prepared and resilient region consistently developing regional capabilities based on an analysis of risk through collaboration and coordination.

Jurisdiction Description

The current Bay Area UASI region is comprised of twelve counties (Alameda, Contra Costa, Marin, Napa, San Francisco, San Mateo, Santa Clara, Santa Cruz, Solano, Sonoma, Monterey and San Benito) and the three major cities of Oakland, San Francisco, and San Jose.[1] In 2005, prior to the DHS led consolidation, this group initiated regional planning and collaboration efforts by developing the Regional Emergency Coordination Plan (RECP).

The Bay Area UASI is inclusive of over 100 incorporated cities and a combined total population exceeding 7.5 million people. In addition to the 7.5 million residents, the Bay Area attracts 15.9 million visitors annually who spend more than $16.6 million per day in the region. The Bay Area is one of the most culturally diverse areas in California.

Urban Area Structure

The Bay Area UASI is managed through a three-tiered governance structure. The top tier is the eleven-member Approval Authority that includes representation from each of the three major cities of Oakland, San Francisco, and San Jose and the County of Alameda, County of Contra Costa, County of Marin, County of Monterey, County of San Francisco, County of San Mateo, County of Santa Clara and County of Sonoma. An appointee from the Secretary of the California Emergency Management Agency is also a non-voting member. The Approval Authority provides policy direction to the program and is responsible for final decisions.

The eleven-member Approval Authority works collaboratively with an Advisory Group which acts as the second tier of the governance structure. Advisory Group members include one representative each from the twelve Bay Area county operational areas, the three major cities, the regional NCRIC and an appointee from the Director of the Governor's Office of Emergency

---

[1]The California Emergency Management Agency (CalEMA) divides the state's 58 counties into 3 administrative regions: Coastal, Inland, and Southern. The Bay Area UASI is part of the Coastal Region which includes: law, fire, coroners/medical examiners, emergency medical, and search and rescue mutual aid systems.

Services. The Advisory Group makes policy and programmatic recommendations to the Approval Authority and ensures there is broad representation, input and participation in the regional planning process.

Managing the day-to-day work of the Bay Area UASI is a Management Team comprised of a general manager, an assistant general manager, project managers, a chief financial officer, and finance and grants staff. The City and County of San Francisco has been designated as the fiscal agent for the grants managed by the Bay Area UASI.

Strategy Development Process

Through a series of meetings and other planning activities within the region, the *Strategy* and its goals and objectives as well as various ideas and recommendations were developed. The planning process used to develop the *Strategy* is outlined below. This process included a regional risk assessment, a capabilities assessment, and a gap analysis. From that data, strategic goals and objectives were updated along with implementation steps. The implementation steps involve a series of resource elements divided among the elements of capability: plans, organization, equipment, training and exercises (POETE) needed to achieve the objective as outlined in the figure below.
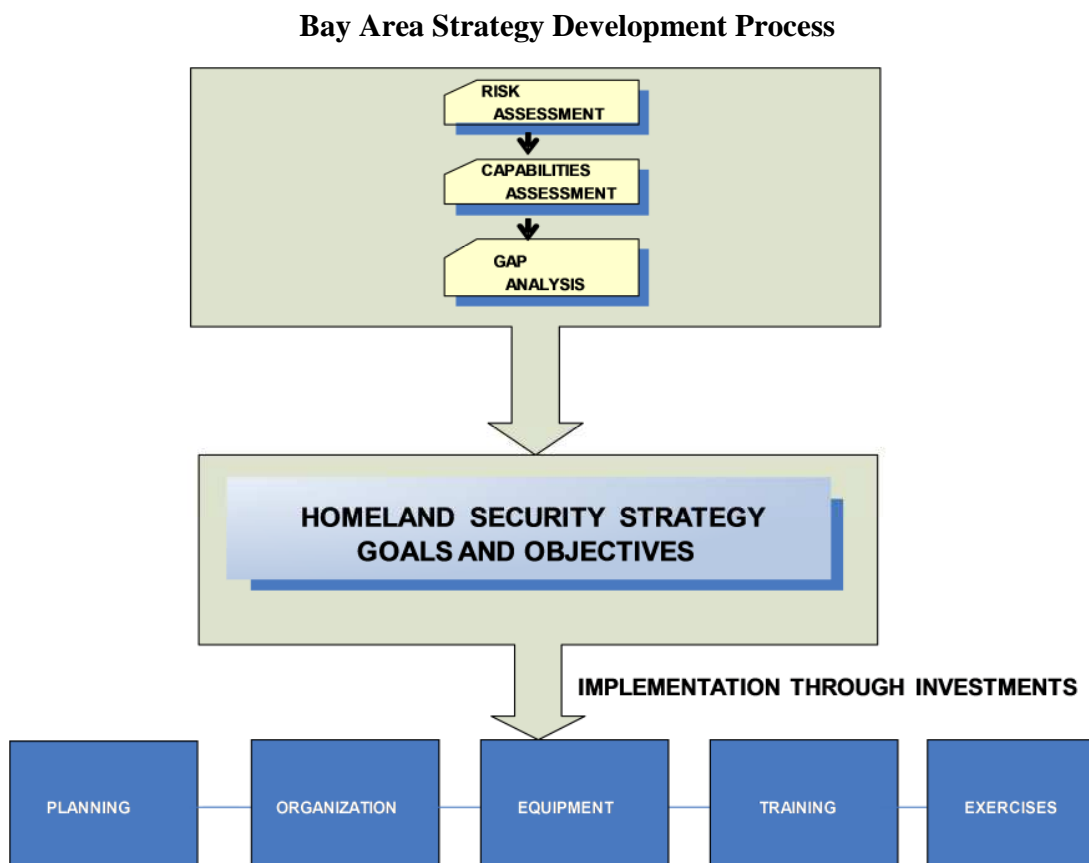
Bay Area Strategy Development Process

In 2008, the Bay Area UASI produced five major planning guidance documents: an assessment and strategic plan for regional interoperable communications; an assessment and project plan for community preparedness; a gap analysis and multi-year training and exercise program for EMS, the fire service and law enforcement; a training and exercise mandate for search and rescue; and a chemical, biological, radiological, nuclear, and/or explosive (CBRNE) assessment and strategic plan. In 2011 the region produced several region-wide response and recovery plans focusing on catastrophic disaster management. This was followed by a regional assessment and strategic plan for public information and warning. The plans from 2011 and 2012 cover:

- Mass Care and Sheltering
- Interim Housing
- Mass Fatality Management
- Donations Management
- Debris Removal
- Mass Transportation
- Volunteer Management
- Emergency Public Information and Warning

All of these plans and strategies have been reviewed and relevant key elements have been integrated into this overall regional *Bay Area Homeland Security Strategy*.

State and National Goals

The *Strategy* is built on the premise that achieving homeland security is an ongoing mission and one that must be a shared responsibility across the entire region, state and nation. This includes our local, tribal, state, and federal agencies, international partners, community organizations, businesses and individuals. Therefore, the *Strategy* supports implementation of the State of California Homeland Security Strategy and the National Security Strategy. Indeed, this *Strategy* serves as the Bay Area's focal point for implementing not only local and regional homeland security policy and priorities, but also national and state homeland security policy at the local and regional level.

The *Strategy* is also linked directly to the federally required Threat Hazard Identification and Risk Assessment (THIRA). The THIRA uses the region's risk and capabilities data described below to set regional capability targets that the region should strive towards based on terrorism, natural hazard and technological hazard scenarios that pose a significant risk to the region as a whole. These regional targets then help inform the goals, objectives and implementation steps in the *Strategy*.

Bay Area Risk Overview

Mitigating risk plays a vital role in the region's homeland security efforts. Risk is the expected negative impact of an adverse incident (whether the result of terrorism or a natural hazard) on an asset, considering both its likelihood and the magnitude of its impact. Risk can be expressed as a number or value in order to make comparisons. The Bay Area calculates risk as a function of threat, vulnerability, and consequence: **Risk = Threat x Vulnerability x Consequence.** The Bay

Area's risk environment is a complex one involving terrorism, crime, natural hazards and industrial and other accidents concerning its people, and critical infrastructure and key resources (CIKR).

In addition to its large population, there are approximately 13,000 CIKR assets in the entire Bay Area that cover all 18 *National Infrastructure Protection Plan* (*NIPP*) sectors. These assets include ███

The terrorism scenarios and natural hazards that pose the greatest risk to the Bay Area's CIKR are listed below in rank order:

Rank	Terrorism Scenarios	Natural Hazards
1	Vehicle Borne Improvised Explosive Device	Flood
2	Aircraft as a Weapon	Earthquake
3	Improvised Explosive Device	Wildfire
4	Biological Attack (Contagious)	Ice
5	Cyber Attack	Wind

From a terrorism perspective, the Bay Area's CIKR is particularly at risk from vehicle borne improvised explosive devices (VBIED), e.g., car or truck bombings against critical infrastructure. The relatively high likelihood of a VBIED attack in the Bay Area is driven by the ease and low expense of carrying out such an attack. Such a method of attack is common around the world. When combined with a conventional IED attack, over 50% of the calculated risk to the region's CIKR comes from terrorists' use of explosives. In addition to IEDs, general aviation aircraft as a weapon poses a risk given the number of general aviation airports in the region and the lower security standards imposed on general aviation as compared to commercial aviation.

The Bay Area also faces risk from natural hazards, especially floods, earthquakes and wildfires. The region rests upon one of the longest and most active earthquake fault systems in the world. This system includes the San Andreas Fault, the Hayward Fault and the Calaveras Fault. The U.S. Geological Survey estimates an 80% chance of a magnitude 6.7 or greater quake striking the Bay Area within the next 30 years. Based on the Bay Area's topography, risk from wild land fires as well as tsunamis are also of major concern.

A breakdown of the top ten CIKR sectors in the Bay Area based on the number of assets and risk to each sector (both from terrorism and natural hazards) is set forth in the table below.

Bay Area Sector Rankings

Rank	Sectors Ranked by Total Assets	Sectors Ranked by Terrorism Risk	Sectors Ranked by Natural Hazards Risk
1	Government	Transportation	Government
2	Commercial	Government	Water
3	Emergency Services	Banking	Commercial
4	Transportation	Commercial	Transportation
5	Postal	Health	Health
6	Dams	Defense Industrial Base	Energy
7	Water	Water	Emergency Services
8	Health	Monuments and Icons	Chemical
9	Banking	Energy	Communications
10	Energy	Communications	Banking

The NCRIC has further refined all of the region's assets into four priority levels (Level I being the highest and Level IV being the lowest priority) with the vast majority of the assets (over 8,100) falling within priority Level IV. Just 2% of all NCRIC identified assets fall into Level I. Such a breakdown reflects the region's goal of accounting for as many assets as possible while recognizing that a smaller subset of those assets, if attacked or otherwise incapacitated, could have a devastating impact on the region.

Capabilities Assessment

Upon updating its risk profile, the Bay Area identified those Core Capabilities that were most needed to address the highest-risk acts of terrorism faced by the region i.e., how vital each capability is to preventing, protecting against, mitigating, responding to and recovering from acts of terrorism that pose a risk to the region. While the assessment was driven by terrorism risk, most, if not all of the capabilities involved in the assessment can be used to address natural hazards as well. This "dual use" concept is one the Bay Area has used for years and will continue to use to help drive investments and strategic planning across the region.

In 2013, the region developed the first in the nation Compendium of Core Capabilities. The Bay Area Compendium of Core capabilities outlines Core Capability targets for Operational Areas and major cities in the region along with detailed measures and metrics to evaluate a jurisdiction's preparedness level in each Core Capability. Each capability target in the Compendium represents a portion or fraction of the capability targets and outcomes from the THIRA.

The compendium was used by each operational area and major city along with a regional assessment involving all jurisdictions. For the assessments, capability levels were organized into five areas or answers that determined level of ability per measure and metric in each Core Capability: Yes/Complete Success, Substantial Progress, Limited Progress, No Progress and Not Applicable.

2012-2015 BAY AREA HOMELAND SECURITY STRATEGY

Upon completing the capabilities assessments, the Core Capabilities were then plotted by terrorism risk relevance and capability gap depending on each capabilities risk relevance and the size of the gap in the capability. The Core Capabilities with the largest capability gap and highest risk relevance were ranked highest. The full findings from the 2012 Core Capabilities assessment, including current levels of ability and capability gaps, for the Bay Area are set forth in the table below.

2013 Core Capability Assessment Findings

Risk and Gap	Core Capability	Risk Relevance	Level of Ability	Gap Analysis
1	Infrastructure Systems	3	25%	Needs Extra Attention
2	Long Term Vulnerability Reduction	6	31%	Needs Attention
3	Physical Protective Measures	7	39%	Needs Attention
4	Public Information and Warning	9	26%	Needs Attention
5	Operational Communications	16	34%	Needs Attention
6	Community Resilience	1	69%	Needs Attention
7	Intelligence and Information Sharing	4	55%	Needs Attention
8	Planning	8	58%	Needs Attention
9	Situational Assessment	12	57%	Needs Attention
10	Screening, Search and Detection	14	68%	Needs Attention
11	Forensics and Attribution	2	79%	Sustain
12	Interdiction and Disruption	5	70%	Sustain
13	Risk and Disaster Resilience Assessment	10	90%	Sustain
14	Risk Management for Protection Programs	11	82%	Sustain
15	Threats and Hazard Identification	13	84%	Sustain
16	Operational Coordination	15	80%	Sustain
17	Access Control and Identity Verification	18	34%	Needs Attention
18	Critical Transportation	21	27%	Needs Attention
19	Cyber Security	20	33%	Needs Attention
20	Natural and Cultural Resources	28	30%	Sustain
21	Public Health and Medical	19	67%	Sustain
22	Fatality Management	21	61%	Sustain
23	Mass Search and Rescue	23	69%	Sustain
24	On-Scene Security and Protection	18	85%	Sustain
25	Supply Chain Integrity	26	25%	Sustain
26	Health and Social Services	25	34%	Needs Attention
27	Mass Care	29	42%	Sustain
28	Housing	31	38%	Sustain
29	Environmental Response/Health and Safety	24	82%	Sustain
30	Economic Recovery	27	38%	Sustain
31	Public and Private Services and Resources	30	49%	Sustain

BAY AREA STRATEGY SUMMARY

Summary of Goals and Objectives

After completing the risk and capabilities assessments, the region used the information to update the goals, objectives and implementation steps in the *Strategy*. Each of the *Strategy's* goals seeks to align whenever possible with either a National or State Homeland Security Priority. The eight DHS National Homeland Security Priorities represent broad and thematic goals that the nation should strive to achieve. They include Strengthen Information Sharing and Collaboration Capabilities, Strengthen Interoperable and Operable Communications Capabilities, etc. Each objective aligns with a capability or set of capabilities from the Core Capabilities[2], and the Centers for Disease Control and Prevention's (CDC's) Public Health Preparedness Capabilities for medical and health related objectives. Each objective describes the desired capability end state the region will strive to achieve.

The purpose of aligning each objective to a capability is to ensure the *Strategy* drives investments centered on enhancing specifically defined capabilities needed to better secure and protect the Bay Area from those acts of terrorism and other major hazards that pose the greatest risk to the region. In the end, the Bay Area's ability to prevent acts of terrorism or respond effectively to major natural disasters, such as a catastrophic earthquake, will be determined by the region having sufficient capabilities in place to deal with incidents caused by those threats and hazards. The *Strategy*'s goals, objectives and implementation steps outline in detail what the Bay Area needs to do to make sure it achieves and sustains those capabilities.

The goals and objectives are directed towards the next three years and may be reviewed and updated annually or as needed. It is likely that some of the objectives will carry over from year to year while others may be removed or updated based on the region's progress and actual needs. The goals and objectives will continue to be defined by risk analysis, identified preparedness gaps and sustainment priorities. A summary of the Bay Area's 8 goals and 31 objectives is set forth below.

---

[2] In certain cases an objective may reference both a Core Capability and a Target Capability, e.g., Objective 4.1 Improve Public and Private Services and Resources Management through *Fire Incident Response Support*. (Target Capability is in italics). This is due to the fact that certain Core Capabilities are ambiguous in their terms and require added definition, which the Target Capabilities provide, and/or the Core Capabilities are inclusive of multiple capabilities that were formally divided among the Target Capabilities List and that division is still necessary for planning purposes in the Bay Area, e.g., Objective 6.7 Improve Public and Private Services and Resources Management through *Critical Resource Logistics*. This breaking up of certain Core Capabilities along the Target Capability taxonomy reflects the reality of how the Bay Area plans and invests in these Core Capabilities.

Goal 1 Strengthen the Regional Risk Management and Planning Program

Objective 1.1 Enhance Planning, Threat and Hazard Identification, and Risk Management Capabilities: The Bay Area is able to identify and assess the threats and hazards that pose the greatest risk to the whole community. The region can prioritize and select appropriate capability-based planning investments and solutions for prevention, protection, mitigation, response, and recovery concerning those risks; monitor the outcomes of allocation decisions; and undertake corrective and sustainment actions.

Goal 2 Enhance Information Analysis and Infrastructure Protection Capabilities

Objective 2.1 Enhance Intelligence Collection, Analysis and Sharing: The Bay Area has systems and procedures to effectively collect, analyze and timely share information and intelligence across federal, state, local, tribal, territorial, regional, and private sector entities to achieve coordinated awareness of, prevention of, protection against, mitigation of, and response to a threatened or actual terrorist attack, major disaster, or other emergency. This involves sustaining and building upon the region's intelligence fusion center to include the ability to identify and systematically report suspicious activities associated with potential terrorist or criminal pre-operational planning and logistics.

Objective 2.2 Strengthen Terrorism Attribution, Interdiction and Disruption Capabilities: The Bay Area's law enforcement community (federal, state and local) and other public safety agencies can conduct forensic analysis and attribute terrorist threats and acts to help ensure that suspects involved in terrorist and criminal activities related to homeland security are successfully identified, deterred, detected, disrupted, investigated, and apprehended.

Objective 2.3 Increase Critical Infrastructure Protection: The Bay Area can assess the risk to the region's physical and cyber critical infrastructure and key resources from acts of terrorism, crime, and natural hazards and deploy a suite of actions to enhance protection and reduce the risk to the region's critical infrastructure and key resources from all hazards. This includes a risk-assessment process and tools for identifying, assessing, cataloging, and prioritizing physical and cyber assets from across the region.

Objective 2.4 Enhance Cyber Security: Cyber security programs at the County and major city level meet the Federal Information Processing Standards 200 - Minimum Security Requirements for Federal Information and Information Systems. The region and its jurisdictions can detect malicious cyber activity, conduct technical counter-measures against existing and emerging cyber-based threats, and quickly recover from cyber-attacks in order to ensure the security, reliability, integrity, and availability of its electronic systems and services.

Goal 3 Strengthen Communications Capabilities

Objective 3.1 Enhance Operational Communications Capabilities: The emergency response community in the Bay Area has the ability to provide a continuous flow of mission critical voice, data and imagery/video information among multi-jurisdictional and multidisciplinary emergency responders, command posts, agencies, and Bay Area governmental officials for the duration of an emergency response operation. The Bay Area can

9

also re-establish sufficient communications infrastructure within the affected areas of an incident, whatever the cause, to support ongoing life-sustaining activities, provide basic human needs, and transition to recovery.

Goal 4 Strengthen CBRNE Detection, Response, and Decontamination Capabilities

Objective 4.1 Improve Public and Private Services and Resources Management through Fire Incident Response Support: Fire service agencies across the Bay Area can dispatch initial fire suppression resources within jurisdictional response time objectives, and firefighting activities are conducted safely with fire hazards contained, controlled, extinguished, and investigated, with the incident managed in accordance with local and state response plans and procedures.

Objective 4.2 Strengthen Mass Search and Rescue Capabilities: Public safety personnel in the Bay Area are able to conduct search and rescue operations to locate and rescue persons in distress and initiate community-based search and rescue support-operations across a geographically dispersed area. The region is able to synchronize the deployment of local, regional, national, and international teams to support search and rescue efforts and transition to recovery.

Objective 4.3 Enhance Screening Search and Detection Capabilities: The Bay Area has systems and procedures to rapidly detect, locate and identify CBRNE materials at ports of entry, critical infrastructure locations, public events, and incidents, and can communicate CBRNE detection, identification and warning information to appropriate entities and authorities across the state and at the federal level.

Objective 4.4 Strengthen On-Scene Security and Protection through Explosive Device Response Operations: Public safety bomb squads in the Bay Area are able to conduct threat assessments; render safe explosives and/or hazardous devices; and clear an area of explosive hazards in a safe, timely, and effective manner. This involves the following steps in priority order: ensure public safety; safeguard the officers on the scene (including the bomb technician); collect and preserve evidence; protect and preserve public and private property; and restore public services.

Objective 4.5 Enhance Environmental Response/Health and Safety through WMD/HazMat Response and Decontamination Capabilities: Responders in the Bay Area are able to conduct health and safety hazard assessments and disseminate guidance and resources, including deploying HazMat response and decontamination teams, to support immediate environmental health and safety operations in the affected area(s) following a WMD or HazMat incident. Responders are also able to assess, monitor, clean up, and provide resources necessary to transition from immediate response to sustained response and short-term recovery.

Objective 4.6 Improve Environmental Response/Health and Safety through Responder Safety and Health: The Bay Area can reduce the risk of illnesses or injury to first responders, first receivers, medical facility staff members, or other skilled support personnel as a result of preventable exposure to secondary trauma, chemical/radiological release, infectious disease, or physical/emotional stress after the initial incident or during decontamination and incident follow-up.

10

Objective 4.7 Enhance On-Scene Security and Protection through Emergency Public Safety and Security Response: Public safety agencies within the Bay Area are able to keep the public and critical infrastructure safe by securing a particular incident scene and maintaining law and order following an incident or emergency to include managing the criminal justice prisoner population.

Goal 5 Enhance Medical and Public Health Preparedness

Objective 5.1 Enhance Emergency Triage and Pre-Hospital Treatment: Emergency medical services (EMS) resources across the Bay Area can effectively and appropriately be dispatched (including with law enforcement tactical teams) to provide pre-hospital triage, treatment, transport, tracking of patients, and documentation of care appropriate for the incident, while maintaining the capabilities of the EMS system for continued operations up to and including for mass casualty incidents.

Objective 5.2 Increase Medical Surge: The Bay Area is able to provide adequate medical evaluation and care during incidents that exceed the limits of the normal medical infrastructure of an affected community or the region. The healthcare system in the region is able to survive a hazard impact and maintain or rapidly recover operations that were compromised. Those injured or ill from a medical disaster and/or mass casualty event in the Bay Area are rapidly and appropriately cared for. Continuity of care is maintained for non-incident related illness or injury.

Objective 5.3 Strengthen Medical Countermeasure Dispensing: With the onset of an incident, the Bay Area is able to provide appropriate medical countermeasures (including vaccines, antiviral drugs, antibiotics, antitoxin, etc.) in support of treatment or prophylaxis (oral or vaccination) to the identified population in accordance with local, state and federal public health guidelines and/or recommendations.

Objective 5.4 Improve Medical Materiel Management and Distribution: The Bay Area is able to acquire, maintain (e.g., cold chain storage or other storage protocol), transport, distribute, and track medical materiel (e.g., pharmaceuticals, gloves, masks, and ventilators) during an incident and recover and account for unused medical materiel, as necessary, after an incident.

Objective 5.5 Strengthen Non-Pharmaceutical Interventions: Public health agencies in the Bay Area are able to recommend to the applicable lead agency (if not public health) and implement, if applicable, strategies for disease, injury, and exposure control. Strategies include the following: isolation and quarantine, restrictions on movement and travel advisory/warnings, social distancing, external decontamination, hygiene, and precautionary protective behaviors. Legal authority for those applicable measures is clearly defined and communicated to all responding agencies and the public. Logistical support is provided to maintain measures until danger of contagion has elapsed.

Objective 5.6 Improve Laboratory Testing: Laboratories in the Bay Area are able to conduct rapid and conventional detection, characterization, confirmatory testing, data reporting, investigative support, and laboratory networking to address actual or potential exposure to all-hazards. Confirmed cases and laboratory results are reported immediately to all relevant public health, food regulatory, environmental regulatory, and law enforcement agencies in support of operations and investigations.

Objective 5.7 Strengthen Public Health Surveillance and Epidemiological Investigation: Bay Area public health agencies have the ability to create, maintain, support, and strengthen

routine surveillance and detection systems and epidemiological investigation processes, as well as to expand these systems and processes in response to incidents of public health significance. This includes the ability to identify potential exposure to disease, mode of transmission, and agent.

Objective 5.8 Enhance Fatality Management: Bay Area agencies, e.g., law enforcement, public health, healthcare, emergency management, and medical examiner/coroner) are able to coordinate (to ensure the proper recovery, handling, identification, transportation, tracking, storage, and disposal of human remains and personal effects; certify cause of death; and facilitate access to mental/ behavioral health services to the family members, responders, and survivors of an incident.

Goal 6 Strengthen Emergency Planning and Citizen Preparedness Capabilities

Objective 6.1 Strengthen Emergency Public Information and Warning Capabilities: The Bay Area has an interoperable and standards-based system of multiple emergency public information and warning systems that allows Bay Area leaders and public health and safety personnel to disseminate prompt, clear, specific, accurate, and actionable emergency public information and warnings to all affected members of the community in order to save lives and property concerning known threats or hazards.

Objective 6.2 Strengthen Operational Coordination Capabilities: The Bay Area has a fully integrated response system through a common framework of the Standardized Emergency Management System, Incident Command System and Unified Command including the use of emergency operations centers (EOCs), incident command posts, emergency plans and standard operating procedures, incident action plans and the tracking of on-site resources in order to manage major incidents safely, effectively and efficiently. EOCs in the Bay Area can effectively plan, direct and coordinate information and activities internally within EOC functions, and externally with other multi-agency coordination entities, command posts and other agencies to effectively coordinate disaster response operations.

Objective 6.3 Enhance Critical Transportation Capabilities: The Bay Area can provide transportation (including infrastructure access and accessible transportation services) for response priority objectives, including the evacuation of people, including those with access and functional needs, and animals, and the delivery of vital response personnel, equipment, and services into the affected incident areas to save lives and to meet the needs of disaster survivors.

Objective 6.4 Improve Mass Care: Mass care services, including sheltering, feeding, and bulk distribution, are rapidly, effectively and efficiently provided for the impacted population, including those with access and functional needs, in a manner consistent with all applicable laws, regulations and guidelines.

Objective 6.5 Increase Community Resiliency: The Bay Area has a formal structure and process for ongoing collaboration between government and nongovernmental resources at all levels to prevent, protect/mitigate, prepare for, respond to and recover from all known threats and hazards.

Objective 6.6 Strengthen Public and Private Services and Resources Management through Volunteer Management and Donations: Volunteers and donations within the Bay Area are organized and managed throughout an emergency based upon pre-designated plans,

procedures and systems.

Objective 6.7 Improve Public and Private Services and Resources Management through Critical Resource Logistics: The Bay Area has a system to track and manage critical resources and make them appropriately available to incident managers and emergency responders from across the Bay Area to enhance emergency response operations and aid disaster victims in a cost-effective and timely manner.

Goal 7 Enhance Recovery Capabilities

Objective 7.1 Strengthen Infrastructure Systems: The Bay Area can provide accurate situation needs and damage assessments by utilizing the full range of engineering, building inspection, and code enforcement services in a way that maximizes the use of resources, aids emergency response, implements recovery operations, and restores the affected area to pre-incident conditions as quickly as possible. The Bay Area can coordinate activities between critical lifeline operations and government operations to include a process for getting the appropriate personnel and equipment to the disaster scene so that lifelines can be restored as quickly and as safely as possible to support ongoing emergency response operations, life sustainment, community functionality, and a transition to recovery

Objective 7.2 Enable Economic Recovery: During and following an incident, the Bay Area can estimate economic impact, prioritize recovery activities, minimize business disruption, and provide individuals and families with appropriate levels and types of relief with minimal delay.

Objective 7.3 Improve Environmental Response/Health and Safety: After the primary incident, the Bay Area is able to assess, monitor, perform cleanup actions, including debris and hazardous waste removal, and provide resources to prevent disease and injury through the quick identification of associated environmental hazards.

Goal 8 Enhance Homeland Security Exercise, Evaluation and Training Programs

8.1 Strengthen the Regional Exercise and Evaluation Program: The Bay Area exercise program tests and evaluates the region's enhancement and/or sustainment of the right level of capability based on the risks faced by the region with an evaluation process that feeds identified capability gaps and strengths directly into the region's risk management and planning process for remediation or sustainment.

8.2 Enhance the Regional Training Program: The Bay Area has a multi-discipline, multi-jurisdictional risk and capabilities based training program that enhances and sustains priority capabilities in order to mitigate the region's most pressing risks.

Strategy Implementation

The Bay Area UASI Management Team will have overall responsibility for managing and tracking implementation of the *Strategy* with oversight from the Bay Area UASI Approval Authority and input from the region's other stakeholders. Implementation will occur through major annual investments and projects developed at the city, county/operational area, sub-regional and regional level.

For Official Use Only   **BAY AREA STRATEGY SUMMARY**

2012-2015 BAY AREA HOMELAND SECURITY STRATEGY

The Bay Area's strategic approach to investing will be premised on two overarching principles:

- First, sustain current priority programs and capabilities in the region.
- Second, close gaps in capabilities with an emphasis on those capabilities that have the highest risk relevance and the largest capability gaps.

The Management Team is responsible for developing the region's annual planning and investment guidance, which outlines the details for planning structures and priorities to ensure the Bay Area is executing the strategy through investments. These details actualize the two guiding investment principles outlined above. It includes planning timelines, grant guidance, project templates and such other materials and policies as may be necessary to ensure a seamless and integrated planning structure and system for each year.

Evaluation of the Strategy

In order to truly understand the value of the Bay Area's homeland security investments, the region must have a consistent mechanism by which to measure the effectiveness of the homeland security activities generated (i.e., what plans were developed, personnel hired, organization and operations conducted, equipment purchased, number of people trained, and exercises conducted, etc.) by those investments. This will be done in the form of an effectiveness report to the Approval Authority, which may be shared with state and federal partners as needed.[3] Through its goals and objectives, the *Strategy* outlines the region's approach and path forward for homeland security. The effectiveness report outlines the region's progress in achieving those goals and objectives based on enhancing capabilities tied to risk management.

---

[3] In 2011, the Bay Area produced a preliminary UASI effectiveness report, which examined certain UASI investments to determine if the region had been following its strategic plans over the years and investing in priority, risk based capabilities. A more extensive follow-on report was issued in November 2012. The overall findings from both the 2011 and the 2012 report show that the region has been investing according to its plans and that priority capabilities have been enhanced to help reduce risk.

For Official Use Only   **BAY AREA STRATEGY SUMMARY**

This Page Intentionally Left Blank

SECTION 1
INTRODUCTION

1.1 Background

Homeland Security is the coordinated effort to ensure a region, state or nation is prepared to prevent, protect against, respond to and recover from threats and acts of terrorism and other man-made or natural catastrophes. It requires a risk management process in order to ensure the right capabilities are in place to manage those hazards that pose the greatest risk to the region, its people, and its critical infrastructure and key resources. The threat of catastrophic events, both natural and man-made, requires continuous attention and strategic commitment from all levels of government, the private sector and the general public.

The Northern California Bay Area is a major target of terrorist organizations and a region with an extensive history of natural disasters.   To better address these risks on a regional basis, in 2006, the U.S. Department of Homeland Security (DHS) combined three previously independent Urban Areas (Oakland, San Francisco, and San Jose) under the DHS Urban Area Security Initiative grant program and formed the Northern California Bay Area Urban Areas Security Initiative (Bay Area UASI) region for preparedness purposes.

The combining of the three previously independent Urban Areas prompted them to review their existing governance structures. As a result, the Bay Area UASI established a new three-tiered governance structure, which included the major cities of Oakland, San Francisco, and San Jose, the twelve county operational areas, and the State of California Emergency Management Agency. This governance structure is designed to ensure integration and coordination among the diverse members of the region as each works to collectively enhance the region's preparedness and security.

The Bay Area UASI is committed to the homeland security effort. Working together, the entire Bay Area UASI has strived to integrate preparedness activities, especially preparedness planning at the strategic level. This homeland security strategy represents the latest effort in that regard. The Bay Area UASI is a recognized leader in homeland security and has made great strides in improving preparedness and security while maintaining our standards of freedom and civil liberties. The region will build on its accomplishments, but must remain vigilant and continue to meet the challenges going forward.

1.2 Bay Area Overview

The Bay Area is inclusive of over 100 incorporated cities and a combined total population exceeding 7.5 million people. In addition to the 7.5 million residents, the Bay Area attracts 15.9 million visitors annually who spend more than $16.6 million per day in the region. The Bay Area is one of the most culturally diverse regions in California. With just over 800,000 residents, San Francisco is the 4th most populous city in California and the most densely populated major city in the State. San Jose is the third largest city in California with Oakland being the eighth largest in the State.

From the beginning of the UASI program in 2003, the geographic foot print of DHS- designated UASI jurisdictions has been a combination of DHS determined risk analysis and existing state, local and regional compacts. The formula used by DHS has changed almost yearly, along with the number of eligible jurisdictions, with one of the most dramatic shifts occurring in 2006. That year, DHS combined the three previously independent UASI jurisdictions of Oakland, San Francisco, and San Jose into the current Bay Area UASI.

The current Bay Area UASI region is comprised of twelve counties (Alameda, Contra Costa, Marin, Napa, San Francisco, San Mateo, Santa Clara, Santa Cruz, Solano, Sonoma, Monterey and San Benito) and the three major cities of Oakland, San Francisco, and San Jose. In 2005, prior to the DHS led consolidation, this group initiated regional planning and collaboration efforts by developing the Regional Emergency Coordination Plan (RECP). A map of the current Bay Area UASI is set forth in Figure 1.

Figure 1: Bay Area UASI Region

2008 marked another major shift in how DHS calculates risk and determines UASI funding eligibility. That year, per the 9/11 Act passed by Congress, DHS began a new evaluation process that utilized the U.S. Census-determined Metropolitan Statistical Areas (MSA) to determine eligibility and rank those UASI jurisdictions eligible for funding. In using this approach, jurisdictions within the MSA are included in the DHS risk analysis, but are not necessarily included in the actual UASI region's geographic footprint for funding. In the case of the Bay Area UASI, the region's twelve county geographic foot print is actually **larger** than the MSA region used by DHS to calculate risk. This is rare. The Bay Area UASI includes Santa Cruz, Sonoma, Solano, Monterey and San Benito counties, which are not part of the MSA used by DHS to calculate risk and then rank and fund the Bay Area under the UASI program.

1.3 Bay Area Management

The Bay Area homeland security program is comprised of the UASI grant program, COPS Technology Grant, Interoperable Emergency Communications Grant Program (IECGP), Regional Catastrophic Preparedness Grant Program (RCPGP), and the Public Safety Interoperable Communications (PSIC) grant program. These grants serve as both terrorism and all hazards preparedness programs. Thus, this Strategy is focused on all hazards with a particular emphasis on terrorism preparedness.

17

Governed by a multi-year Memorandum of Understanding (MOU) between the participants, the Bay Area UASI is managed through a three-tiered governance structure. The Bay Area's governance structure is widely viewed as having an important, groundbreaking regional approach that has been recognized, and may be replicated, throughout the State of California and across the country as a homeland security best practice.

1.3.1 Approval Authority

The top tier is the eleven-member Approval Authority that includes representation from each of the three major cities of Oakland, San Francisco, and San Jose and the County of Alameda, County of Contra Costa, County of Marin, County of Monterey, County of San Francisco, County of San Mateo, County of Santa Clara and County of Sonoma. An Appointee from the Secretary of the California Emergency Management Agency (CalEMA) is also a non-voting member. The Approval Authority provides policy direction to the program and is responsible for final decisions.

1.3.2 Advisory Committee

The eleven-member Approval Authority works collaboratively with an Advisory Group which acts as the second tier of the governance structure. Advisory Group members include one representative each from the twelve Bay Area county operational areas, the three major cities, the regional NCRIC and an appointee from the Secretary of CalEMA. The Advisory Group makes policy and programmatic recommendations to the Approval Authority and ensures there is broad representation, input and participation in the regional planning process.

1.3.3 Management Team

Managing the day-to-day work of the Bay Area UASI is a Management Team comprised of a general manager, strategy and compliance director, several project managers, a finance manager, and grants managers. The City and County of San Francisco has been designated as the fiscal agent for the grants managed by the Bay Area.

1.3.4 Planning Hubs and Work Groups

The Bay Area also engages a variety of stakeholders throughout the region to move projects and initiatives forward and to provide essential input for decision makers of the Bay Area's homeland security efforts. Planning hubs are organized sub-regionally – North, South, East and West Bay hubs. Working groups generally organize themselves around the Strategy's goals and objectives. For example, the CBRNE Work Group manages issues related to the CBRNE goal (Goal 4 - Strengthen CBRNE Detection, Response, and Decontamination Capabilities). Work group members represent diverse interests and areas of expertise at the local, regional and state level. Each work group meets on an as needed basis to address identified projects and issues.

SECTION 2
PURPOSE

2.1 Purpose Overview

The purpose of the *Bay Area Homeland Security Strategy* is to ensure the Bay Area has a comprehensive, data driven document that outlines the Bay Area's risks, capabilities, vision, structure, goals and objectives for homeland security. Having such a document will ensure the Bay Area is in the best possible position to clearly track and articulate its risk and capability needs to local leaders, the State of California and DHS when seeking resources to reduce that risk and satisfy those capability needs. The *Strategy* is designed primarily to address terrorism risk with an understanding that capabilities enhanced to combat terrorism often enhance the ability to also manage natural disasters and man-made accidents.

The *Strategy* outlines a comprehensive system for enhancing regional capability and capacity that will guide the Bay Area UASI's efforts to:

- Prevent and disrupt terrorist attacks;
- Protect the people of the Bay Area, its critical infrastructure and key resources;
- Mitigate the damage caused by acts of terrorism, natural disasters and man-made accidents;
- Respond to and recover from major incidents and all hazards that do occur;
- Continue to strengthen our preparedness foundation to ensure our long-term success; and
- Guide future investments, increase capabilities and reduce risk.

This is an exceedingly complex mission requiring coordination, cooperation, collaboration, and focused effort from the entire region – residents, government, as well as the private and non-governmental organization sectors. The Bay Area region will apply the resources available from DHS to address unique planning, organizational, equipment, training, and exercise needs to assist in building an enhanced and sustainable capacity to prepare for all hazards. However, this *Strategy* is not a grant strategy; it is a comprehensive homeland security strategy that will be implemented through projects funded by Federal grants, general funds and such other funding opportunities that may become available.

2.2 Prior and Ongoing Planning Efforts

Prior to the 2006 consolidation of the three previously independent Urban Areas, the initial homeland security strategies were developed based upon the September 2003 regional assessments. That process included comprehensive risk, capabilities, and needs assessments. The results of the assessments provided an early insight into the requirements of each of the three Urban Areas at the time. The three strategies were revised in 2005 to align with the homeland security mission areas of prevention, protection, response and recovery, and the Target Capabilities List to enable the region to more effectively embrace the capabilities based planning process. Later, a regional strategy was developed in accordance with the consolidation of 2006. The 2006 Strategy was followed by a new 2010 Bay Area regional homeland security strategy

19

based upon a region-wide risk and capabilities assessment conducted in late 2009. The 2010 Bay Area Strategy served as a baseline for this current *2013 Bay Area Homeland Security Strategy*.

In the past, the Bay Area region has conducted assessments and developed several strategic, operational and tactical level plans that have produced valuable data to help drive the region's policies and programs. Those assessments and strategies (and future assessments and strategies) serve two purposes concerning this Strategy: first, they provide valuable data and strategic input into this regional Strategy; and second, they serve as implementation plans, policies and procedures under the umbrella of this larger region-wide *Bay Area Homeland Security Strategy*. Appendix A outlines this interrelated planning structure.

In 2008, the Bay Area UASI produced five major planning guidance documents: an assessment and strategic plan for regional interoperable communications; an assessment and project plan for community preparedness; a gap analysis and multi-year training and exercise program for EMS, the fire service and law enforcement; a training and exercise mandate for search and rescue; and a CBRNE assessment and strategic plan. In 2011, the region produced several region-wide response and recovery plans focusing on catastrophic disaster management. This was followed by a 2012 regional strategic plan for public information and warning. The plans from both years cover:

- Mass Care and Sheltering
- Interim Housing
- Mass Fatality Management
- Donations Management
- Debris Removal
- Mass Transportation
- Volunteer Management
- Emergency Public Information and Warning

All of these plans and strategies from 2008 and beyond have been reviewed and relevant key elements have been integrated into this overall regional *Bay Area Homeland Security Strategy*.

Finally, the homeland security planning and implementation process has no "end state" any more than traditional public safety has an end point. Rather, it is a constant cycle of improving plans, procedures, systems and operations designed to enhance security and preparedness for the region. The Bay Area is committed to this process and the current *Bay Area Homeland Security Strategy* is the latest product in that endeavor.

SECTION 3
VISION

The Bay Area's vision for homeland security is a secure, prepared and resilient region consistently developing regional capabilities based on risk through collaboration and coordination.

The Bay Area's vision will be implemented through a set of guiding principles that will help shape this regional *Strategy* and its implementation and maintenance. These principles are:

➢ Homeland security is a shared responsibility among all regional members at all levels of government and the private sector.

➢ Local jurisdictions and sub-regions are in the best position to know how to achieve regional goals and objectives.

➢ Each individual jurisdiction and the region as a whole will be best able to implement its vision for homeland security through regional collaboration and cooperation.

➢ The region will strive to use empirical data to drive its homeland security programs to include risk and capabilities assessment data.

➢ Every individual and family across the region has a critical role to play in homeland security from preparing for disasters to helping deter and detect terrorist plots.

➢ The region will strive to develop and share best practices in homeland security across the region and the State of California and recognizes that such best practices are often first developed at the local level.

➢ The region will responsibly leverage and manage funds to achieve the optimal result with the dollars available. This will include, wherever possible, the integration of State Homeland Security Program grants and UASI grants among others.

SECTION 4
FOCUS & MISSION

4.1 Focus and Mission Overview

To accomplish the Bay Area's vision for homeland security, this Strategy and its goals and objectives are focused and organized around managing **major/regional** threats and hazards through the five[4] mission areas of homeland security: prevention, protection, mitigation, response and recovery. Certain programs cross all mission areas; these are listed in this document under the category "common." The Strategy also reflects that day-to-day public safety policy development and implementation is the responsibility of local jurisdictions, while at the same time recognizing that such local capabilities are essential to building regional capacity for which this Strategy is designed. Each strategic goal and objective under this Strategy will be based upon and built to help the region achieve one or more of these mission areas. The five mission areas are broken down as follows:

4.1.1 Prevention

Prevention involves actions to avoid an incident or to intervene or stop a terrorist incident from occurring. It involves applying intelligence to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature of the threat; and, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators.

4.1.2 Protection

Protection involves actions to reduce the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks, major disasters, and other emergencies. It includes awareness elevation and understanding of threats and vulnerabilities to critical facilities, systems, and functions; identification and promotion of effective infrastructure sector-specific protection practices and methodologies; and information sharing among private entities within the sector, as well as between government and private entities.

---

[4] When the mission areas were first developed the mitigation mission area was not formally recognized. In 2011, PPD-8 formally adopted mitigation as a homeland security mission area. Thus, up until 2011, there were only four mission areas plus the common mission area. This change is most relevant when dealing with the Target Capabilities List, which is aligned to the four mission areas, plus common, and the new Core Capabilities List, which is aligned to the five mission areas plus common, each of which is discussed in sections 4.3 and 4.4 respectively.

SECTION 4 FOCUS AND MISSION

4.1.3 Mitigation

Mitigation involves efforts to reduce loss of life and property by lessening the impact of disasters. Mitigation is achieved through risk analysis, which results in information that provides a foundation for mitigation activities that reduce risk. Mitigation includes ongoing public education and outreach activities designed to reduce loss of life and destruction of property; complying with or exceeding floodplain management and land-use regulations; enforcing stringent building codes, seismic design standards, and wind-bracing requirements for new construction, repairs, or retrofitting of existing buildings.

4.1.4 Response

Response includes activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes.

4.1.5 Recovery

Recovery involves activities that include the development, coordination, and execution of service-and-site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; and additional measures for social, political, environmental, and economic restoration.

4.2 The National Priorities

The National Homeland Security Priorities represent broad and thematic goals that fall under the mission areas that the Nation should strive to achieve in homeland security. The National Homeland Security Priorities are:

- Implement the National Incident Management System and National Response Framework
- Implement the National Infrastructure Protection Plan
- Expand Regional Collaboration
- Strengthen Information Sharing and Collaboration Capabilities
- Strengthen CBRNE Detection, Response and Decontamination Capabilities
- Strengthen Interoperable and Operable Communications Capabilities
- Strengthen Planning and Citizen Preparedness
- Strengthen Medical Surge and Mass Prophylaxis Capabilities

4.3 The Core Capabilities

In September 2011, DHS released the new National Preparedness Goal. At the center of the new Goal is the Core Capabilities. The Core Capabilities is a list of 31 capabilities necessary to

address a wide range of hazards based on the results of a national risk assessment conducted by DHS. The Core Capabilities serve as the successor to the Target Capabilities List. A Core Capability to Target Capability Crosswalk is set forth in Appendix A. A breakdown of the Core Capabilities by mission area is set forth in Table 1 below.

Table 1: Core Capabilities by Mission Area

Common				
Planning				
Public Information and Warning				
Operational Coordination				
Prevention	**Protection**	**Mitigation**	**Response**	**Recovery**
Forensics and Attribution	Access Control and Identity Verification	Community Resilience	Critical Transportation	Economic Recovery
Intelligence and Information Sharing	Cyber Security	Long-term Vulnerability Reduction	Environmental Response/Health and Safety	Health and Social Services
Interdiction and Disruption	Intelligence and Information Sharing	Risk and Disaster Resilience Assessment	Fatality Management Services	Housing
Screening, Search, and Detection	Interdiction and Disruption	Threats and Hazard Identification	Infrastructure Systems	Infrastructure Systems
	Physical Protective Measures		Mass Care Services	Natural and Cultural Resources
	Risk Management for Protection Programs and Activities		Mass Search and Rescue Operations	
	Screening, Search, and Detection		On-scene Security and Protection	
	Supply Chain Integrity and Security		Operational Communications	
			Public and Private Services and Resources	
			Public Health and Medical Services	
			Situational Assessment	

4.4 Public Health And Medical Capabilities

Unlike the Target Capabilities, which included seven distinct medical and health related capabilities, the new Core Capabilities has one all-inclusive Public Health and Medical Services capability under the response mission area. However, in 2011, the Centers for Disease Control and Prevention (CDC) released the *Public Health Preparedness Capabilities, National Standards for State and Local Planning*. This document outlines a series of capabilities (15 in total) intended to "assist state and local planners in identifying gaps in preparedness, determining the specific jurisdictional priorities, and developing plans for building and sustaining capabilities."[5]

Many of the CDC's public health and medical related capabilities link directly to the Target Capabilities List medical and health capabilities, which the Bay Area had built most of its medical and health related objectives around. As such, for those CDC capabilities that have such a link, the Bay Area will use those CDC capabilities to develop specific medical and health related objectives in the *Strategy*. This will ensure consistency between the broader homeland security efforts in the region and the specific medical and health programs the Bay Area's public health and medical stakeholders are engaged in with the CDC.[6] Moreover, all of the efforts undertaken to enhance these medical and health capabilities can be "rolled-up" under the single Public Health and Medical Services Core Capability for reporting purposes to DHS.

A breakdown of the CDC's public health capabilities applicable to the *Strategy* are listed in Table 2.

Table 2: CDC Capabilities and Target Capabilities Crosswalk

CDC Capability	Target Capability
Public Health Laboratory Testing	Laboratory Testing
Public Health Surveillance and Epidemiological Investigation	Epidemiological Surveillance and Investigation
Medical Surge	Medical Surge
Medical Counter Measures Dispensing	Mass Prophylaxis
Medical Material Management and Distribution	Medical Supplies Management and Distribution
Non-Pharmaceutical Interventions	Isolation and Quarantine

---

[5] Centers for Disease Control and Prevention, *Public Health Preparedness Capabilities, National Standards for State and Local Planning* (2011), page 2.

[6] The Emergency Triage and Pre-hospital Treatment Target Capability is primarily focused on the emergency medical services community. As such, it is not directly accounted for in the CDC capabilities. However, the Bay Area will continue to use Emergency Triage and Pre-hospital Treatment in the *Strategy* as part of its medical and health objectives. Also, the Core Capabilities has Fatality Management Services distinct from the Public Health and Medical Services. However, the Bay Area has included Fatality Management under the medical and health goal in the *Strategy* and will continue to do so.

SECTION 4 FOCUS AND MISSION

4.5 The Bay Area Compendium of Core Capabilities

In June 2013, the Bay Area developed the first in the nation comprehensive set of capability measures and metrics for all 31 Core Capabilities.[7] The region developed the *Bay Area Compendium of Core Capabilities* for the specific purpose of having a consistent set of locally tailored preparedness measures and metrics that individual jurisdictions in the region can use to assess capabilities within the context of mutual aid. The need for these locally tailored measures and metrics was due to the fact that the federally developed capability targets in the *National Preparedness Goal* were too broad and generic for local assessment purposes.

The region will aggregate individual jurisdictional assessments and conduct a regional assessment to inform an overall regional picture of preparedness. Gaps and strengths identified through the assessment process will then be used to update *Strategy* goals and objectives. In addition to informing preparedness levels to update the *Strategy*, the Compendium will allow Bay Area jurisdictions and the region to:

- Have a consistent framework to assess capabilities and show trends in preparedness and performance at the local and regional level over time.
- Use the picture of preparedness and investments to help demonstrate the effectiveness of the UASI program to policy makers.
- Draw from the performance measures to set exercise performance targets and related critical tasks in order to evaluate the agencies and jurisdictions participating in an exercise.

---
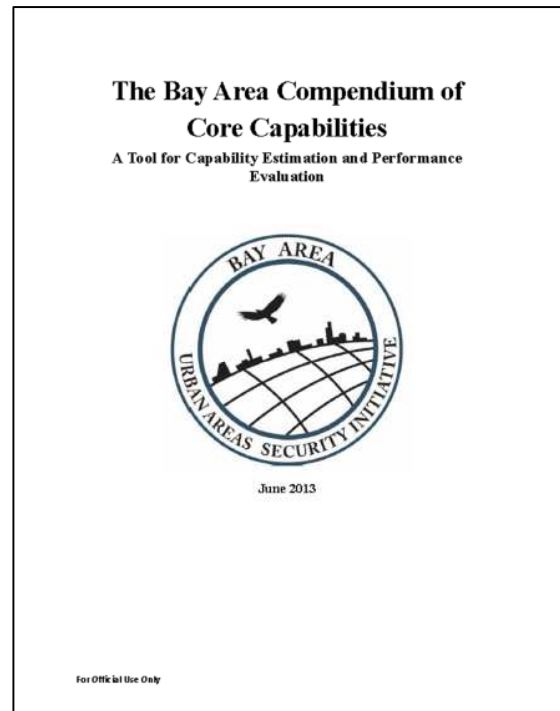
[7] For the CDC public health and medical capabilities, all measures and metrics are rolled-up under the single Public Health and Medical Core Capability. This was done to ensure that the Bay Area Compendium remains consistent with the DHS/FEMA Core Capabilities taxonomy. However, the *Strategy's* medical and health objectives are broken out aligned with the CDC public health and medical capabilities.

SECTION 4 FOCUS AND MISSION

SECTION 5
RISK OVERVIEW

5.1 Introduction

A core element of Bay Area strategic planning is utilizing risk data and risk management principles to guide planning and investments. In 2013, the Bay Area updated its risk assessment data concerning terrorism and natural hazards, the results of which are summarized here. As risk is a dynamic attribute and can shift over time, the 2013 follow-up analysis builds upon the solid baseline established in 2009, and followed-up on in each successive year, and will need to be updated again in the future.

The purpose of this section is to highlight and summarize the key findings from the 2013 risk validation analysis as outlined in the Risk Analysis Center as of August 2013. This section begins by providing details regarding the risk methodology utilized for completing the risk analysis. Although the 2013 risk analysis focused primarily on terrorism risk, the Bay Area also considered risks posed by natural hazards. In terms of terrorism events, the 2013 analysis considered sixteen terrorism (and nine natural hazard) scenarios that could potentially impact the region. The analysis goes on to determine which of those scenarios posed the greatest relative risk to the region. The focus then moves to defining the public and private sector critical assets for risk analysis and then to analyzing asset risk by each of the critical infrastructure and key resources (CIKR) sectors across the entire region as defined by the National Infrastructure Protection Plan (NIPP).

5.2 Risk Methodology

A terrorism event is defined under federal law as the "…unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.[8]" A natural event causes a hazard when it harms people or property. Such natural events may include floods, earthquakes, tornadoes, tsunamis, coastal storms, landslides, and wildfires that strike populated areas.

Risk, then, is the expected negative impact of an adverse incident (whether the result of terrorism or a natural hazard) on an asset, considering both its likelihood and the magnitude of its impact. Risk can be expressed as a number or value in order to make comparisons, and is calculated as a function of threat, vulnerability, and consequence: **Risk = Threat x Vulnerability x Consequence.**

- *Threat*: The likelihood of the occurrence of an incident, including those that are caused by nature (e.g., floods, windstorms, earthquakes) and those that are human-caused (e.g.,

---

[8] 28 C.F.R. Section 0.85

27

acts of terrorism and industrial accidents). *Likelihood* refers to the estimate of the potential of an incident or incident's occurrence as compared to other scenarios in a particular region and takes into account adversarial intent and capabilities.

- *Vulnerability*: Likelihood of the asset[9] succumbing to a terrorist attack or natural hazard. Vulnerability is a function of an asset's recognizability, resilience, and countermeasures effectiveness, such as gates, cameras, guards, etc. The higher the asset's vulnerability the greater the chance a terrorist attack will succeed or a natural hazard will cause damage to that asset. For example, a building with no gate or wall is more vulnerable to a vehicle borne improvised explosive device (more likely to succumb to the attack) than the same building is with a reinforced gate or concrete wall designed to block vehicular traffic.

- *Consequence*: Consequences of an attack can impact one or all of the following areas:

  o **Human:** The adverse impact of an incident on human health as measured by the number of fatalities and injuries the incident causes, as well as by the resulting long-term health effects.
  o **Economic:** The harm caused by an incident as measured by short-term costs of repair efforts, as well as by the long-term impact of an incident on the economic activity of the asset attacked.
  o **Mission:** The severity of the impairment of the asset that an incident inflicts. Mission interruption includes the degree of interruption, geographic scope, and mission criticality.
  o **Psychological:** The adverse impact of an incident on the morale and confidence of the population. Such adverse impacts may include a reduced sense of general well-being, concerns about personal security, and reduced confidence in the government and the economy.

Multiple kinds of risk exist, and driving the Bay Area's risk profile are the characteristics of the assets and population in the area. Further, an area may have a higher risk of one type but not necessarily of others. The Bay Area currently looks at risk in four broad categories:

- Terrorism Risk to People
- Terrorism Risk to Assets
- Natural Hazard Risk to People
- Natural Hazard Risk to Assets

Population risk takes into account not only how many people are present in a given area but also how those people are distributed within a jurisdiction or region (local population density). Population risk calculations consider residents, commuters, and international visitors in a given area. While asset risk looks at the risk to the area from attacks on or incidents involving an area's critical infrastructure, population risk gives an overview of risk to the major population-at-large.

---

[9] An asset is a piece of infrastructure such as a bridge, building, power plant, etc. An asset can also include cyber infrastructure such as networks and software.

5.3 Description of Threats and Hazards

The following is a summary of the sixteen terrorism and nine natural hazard scenarios used to help determine the Bay Area's risk profile. The terrorism scenarios are based, in part, upon actual terrorist methods used in attacks around the world such as improvised explosive devices and conventional assaults. While several of the attack scenarios listed have never been used by terrorists, e.g., an improvised nuclear device against a major U.S. city, the intent to acquire and use such weapons and tactics has been clearly articulated by certain terrorist groups.

Table 3: Terrorism Scenarios

Scenario	Description
Agro-terrorism	An attack on the agriculture/food supply chain. Largely designed to inflict economic damage.
Aircraft as a Weapon	The aircraft as a weapon scenario consists of attackers using an airplane to inflict a direct impact on a target. Damage to the asset is a result of the initial explosion of the airplane's fuel supply, as well as secondary events like fires or building collapses. Catastrophic attacks involving commercial airplanes occurred on September 11, 2001 involving financial and military targets in New York, Virginia, and Pennsylvania. A far less severe attack involving general aviation occurred on February 18, 2010 when a man flew a small plane into an IRS building in Austin, Texas.
Arson/Incendiary Attack	Arson or incendiary attacks have been used widely throughout history by terrorist groups and criminals. Attacks vary widely in scope and intensity, from the use of one small incendiary device like a Molotov cocktail to setting a fire from multiple ignition points on one site using highly flammable fuel. In 2008, the Earth Liberation Front burned down a housing development in Woodinville, Washington. The Provisional Irish Republican Army made extensive use of Molotov cocktails in its fight against British control of Ireland.
Biological Attack (Contagious)	Use of a biological agent that can be spread from human to human and results in negative health effects. This includes the intentional release of communicable infectious diseases such as pandemic flu and Bubonic Plague.
Biological Attack (Non-contagious)	Use of a biological agent that cannot be directly spread from human to human but results in negative health effects. Non-contagious biological attacks typically require direct contact or inhalation with a biological strain ─ for example, the 2001 Anthrax attacks, which killed five people.
Chemical Attack	A chemical release on a population using toxic and corrosive chemicals that generate poisonous gases, liquids, and other hazardous substance. Chemical attacks include the release of a nerve agent, blister agent, or industrial chemicals used against an asset's population. Scenario includes aerosol or other distribution of mustard gas, arsenic, mercury, Sarin, or other similar substances. This also considers the use of explosives against chlorine tanks.
Conventional Attack	Conventional attacks include attacks executed with weapons that are not weapons of mass destruction. This can include grenades, bombs, mines, missiles, small firearms, and large-caliber artillery systems. One of the most notable conventional attacks in recent history occurred in 2008 in Mumbai, India, where terrorists affiliated with Islamist group Lashkar-e-Taiba attacked multiple public sites with bombs and guns.
Cyber Attack	Computer-based attack aimed to disrupt the function of an asset or obtain sensitive information from the asset's computer systems. Attacks may involve service disruption or manipulation using destructive worms and viruses, Denial of Service exploits, and intrusions. Actors either inside or outside of the asset's organization could carry out acts of sabotage.
Food and Water Contamination	Poisoning or otherwise tampering with a food/water distribution point in such a way that causes harmful health effects. Poisoning may include the use of bacteria, viruses,

Scenario	Description
	and heavy metals. Attacks at a distribution point may spread among the population.
Hostage Taking/Assassination	Attack in which terrorists enter an asset and hold captives; also any attack targeting and killing key officials or significant persons who are present at a site.
Improvised Explosive Device (IED)	IEDs are bombs that are not of standard military construction, but may utilize components that are. Constructed using any type of explosive material, fuse, detonator, and container, they can also include biological, chemical, or other contaminants. IEDs have been used widely by terrorist groups; recent examples include use by the Taliban in Afghanistan against Coalition and Afghan forces and by the Liberation Tigers of Tamil Elam against the Sri Lankan government, most often via suicide bombers.
Maritime Attack	Use of a sea vessel to deliver explosives against a target, such as another ship or port asset directly adjacent to a waterway. In 2000, 17 military personnel were killed when such an attack targeted the USS Cole.
Nuclear Device	A nuclear device scenario involves the detonation of a weapon assembled using highly enriched uranium, most likely stolen or purchased from an unstable nuclear or former nuclear state. A device could be assembled near an UA and transported via vehicle to a densely-populated location for detonation. Such an attack has yet to occur; however, overwhelming casualties within 12 miles can be expected, with decreasing casualty rates extending over a 150-mile radius. Long-term environmental and health effects can be expected, as well as damage exceeding $100 billion.
Radiological Dispersion Device (RDD)	An attack, also called a "dirty bomb," combining radioactive materials and conventional explosives. The explosives cause damage and casualties within the blast radius and spread radiation over a larger area. Though a potentially large number of people could be exposed, the radiation levels are unlikely to cause significant deaths. However, a radiation attack would have considerable psychological effects on the public.
Sabotage/Theft	Sabotage encompasses any act intended to prevent an asset from engaging in its mission. It can affect any sector and any level of an asset, and it may be carried out by any actor to include disgruntled employees or terrorists. Sabotage is often classified solely or simultaneously as one or more other crimes, such as arson. An unidentified individual injected a glue-like substance into a remote shutdown panel at a nuclear power plant in St Lucie, Florida, in 1996. In 2006, the Salafist Group for Call and Combat vandalized and set fire to an Algerian cement plant and company vehicles.
Vehicle Borne Improvised Explosive Devices (VBIED)	VBIEDs are IEDs delivered via vehicles. A large sedan can yield up to 1,000 pounds (lbs.) of explosives in the trunk alone; a small box truck can yield over 10,000 lbs. By comparison, the truck used in the Oklahoma City bombing was carrying 4800 lbs. of explosives. This method of attack is historically common and still used by groups such as al Qaeda, which describes the attack in detail in its training manual.

SECTION 5 RISK OVERVIEW

Table 4: Natural Hazard Scenarios

| Scenario	Description
Floods	Floods, according to FEMA, are one of the most common hazards in the United States. Flood effects can be local, impacting a neighborhood or community, or very large, affecting entire river basins and multiple states. However, all floods are not alike. Some floods develop slowly, sometimes over a period of days. But flash floods can develop quickly, sometimes in just a few minutes and without any visible signs of rain. Flash floods often have a dangerous wall of roaring water that carries rocks, mud, and other debris and can sweep away most things in its path. Overland flooding occurs outside a defined river or stream, such as when a levee is breached, but still can be destructive. Flooding can also occur when a dam or levee breaks, producing effects similar to flash floods.
Earthquake	An earthquake is ground shaking caused by a sudden movement of rock in the Earth's crust. Such movements occur along faults, which are thin zones of crushed rock separating blocks of crust. When one block suddenly slips and moves relative to the other along a fault, the energy released creates vibrations called seismic waves that radiate up through the crust to the Earth's surface, causing the ground to shake. Earthquakes may last only a few seconds or may continue for up to several minutes. They can occur at any time of the day or night and at any time of the year. They are caused by stress that builds up over time as blocks of crust attempt to move but are held in place by friction along a fault. (The Earth's crust is divided into large plates that continually move over, under, alongside, or apart from one another atop the partly molten outer layer of the Earth's core.) When the pressure to move becomes stronger than the friction holding them together, adjoining blocks of crust can suddenly slip, rupturing the fault and creating an earthquake.
Wildfires	A wildfire in California may involve a fire burning uncontrolled on lands covered wholly or in part by timber, brush, grass, grain, or other flammable vegetation. It may also include any fire, controlled or uncontrolled, including a campfire, burning outside of any structure, mobile home, or living accommodation mounted on a motor vehicle. California has been extremely susceptible to such fires over the years with some of the largest wildfires in the U.S. occurring in the State.
Severe Winds	Severe winds occurring as a result of thunderstorms can be a threat to both life and property. For example, according to the National Weather Service, extreme winds, those damaging wind gusts of 58 mph or greater, within 12 miles of a location, pose an extreme likelihood (36% or greater) of causing minor to major damage in the worst situations.
Tornado	A tornado is a violent, dangerous, rotating column of air that is in contact with both the surface of the earth and a funnel shaped cumulonimbus cloud ranging in width from a few yards to more than a mile and whirling at destructively high speeds, ranging from 100 to as high as 300 miles per hour.
Hail	A hailstorm is a storm of spherical balls of ice. Hail is a product of thunderstorms or intense showers. It is generally white and translucent, consisting of liquid or snow particles encased with layers of ice. Hail can cause serious damage to cars, aircraft, skylights, glass-roofed structures, livestock and crops, etc.
Pandemic	A naturally occurring disease outbreak can cause illness and result in significant casualties. Since 1900, there have been three influenza pandemics that killed approximately 600,000 people in the United States. The 2009 H1N1 flu, first identified in Imperial and San Diego counties, killed more than 550 Californians, sent thousands more to hospitals, caused widespread fear and anxiety and the declaration of a public health emergency.

SECTION 5 RISK OVERVIEW

5.4 Critical Infrastructure and Key Resources

For the 2013 update, the Northern California Regional Intelligence Center (NCRIC) compiled a list of approximately 13,000 critical infrastructure and key resource assets in the entire Bay Area that cover all 18 *National Infrastructure Protection Plan* (NIPP) sectors. This is an increase of over 4,500 assets from 2012 and reflects the region's growing cataloging and understanding of CIKR within its area. A breakdown of those critical assets by sector is set forth in Figure 2 below. The sector with the largest number of assets is the government sector with over 5,600 assets and the sector with the fewest number of assets is nuclear with just six assets.

Figure 2: Distribution of Bay Area Assets by NIPP Sector
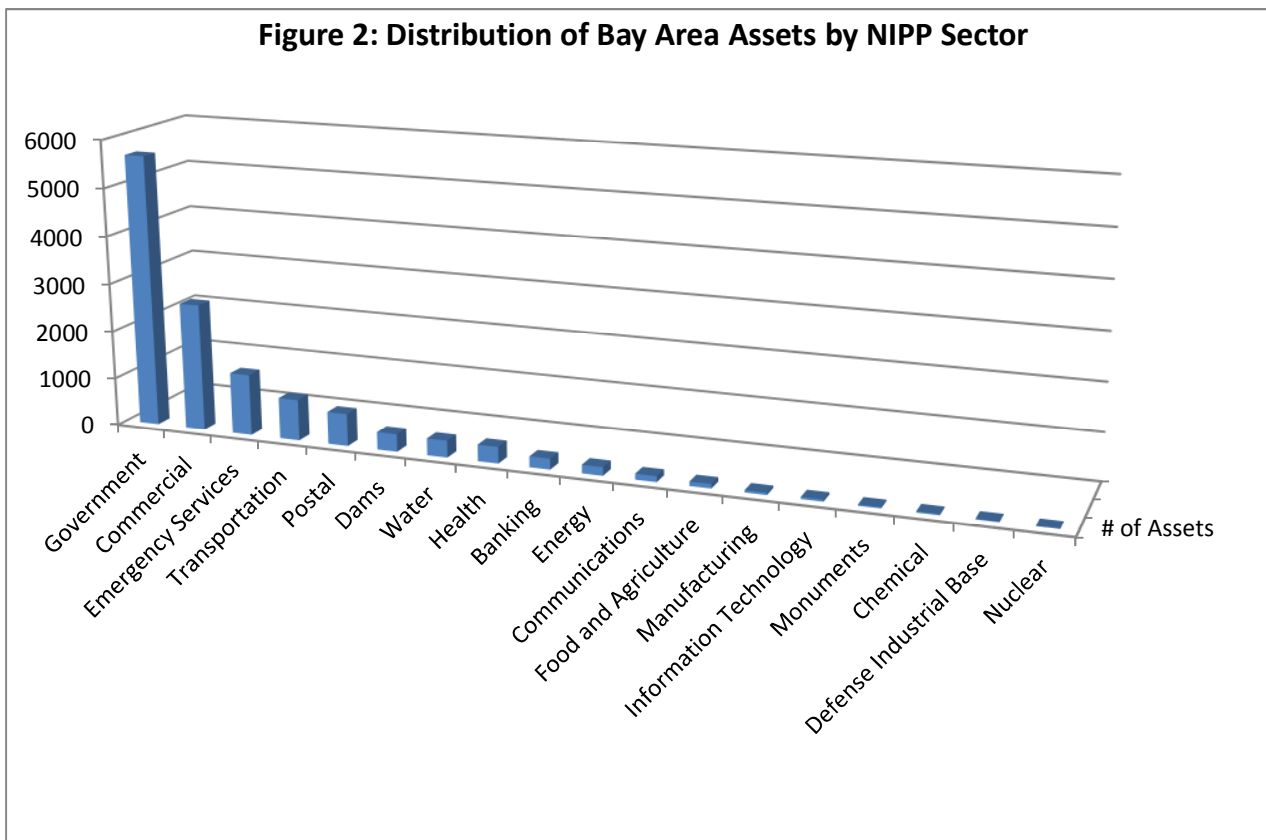
The Bay Area's assets include ██

SECTION 5 RISK OVERVIEW

The region has further refined its assets into four priority levels (Level I being the highest and Level IV being the lowest priority) with the vast majority of the assets (over 8,100) falling into priority level IV. Only 2% of the total assets fall under Level I which is consistent with the data from 2012. However, 2012 saw a decrease in the percentage of assets that fall under Level IV (74% to 63%) and a corresponding increase in the percentage of assets that fall under Levels II and III (20% to 27% and 3% to 7% respectively). Such a breakdown reflects the region's goal of accounting for as many assets as possible while recognizing that a small subset of those assets, if attacked or otherwise incapacitated, could have a devastating impact on the region. Figure 3 summarizes the distribution of assets across all four levels plus a category for assets without an assigned level.

Figure 3: Bay Area Asset Distribution by Priority

For Official Use Only   **SECTION 5 RISK OVERVIEW**
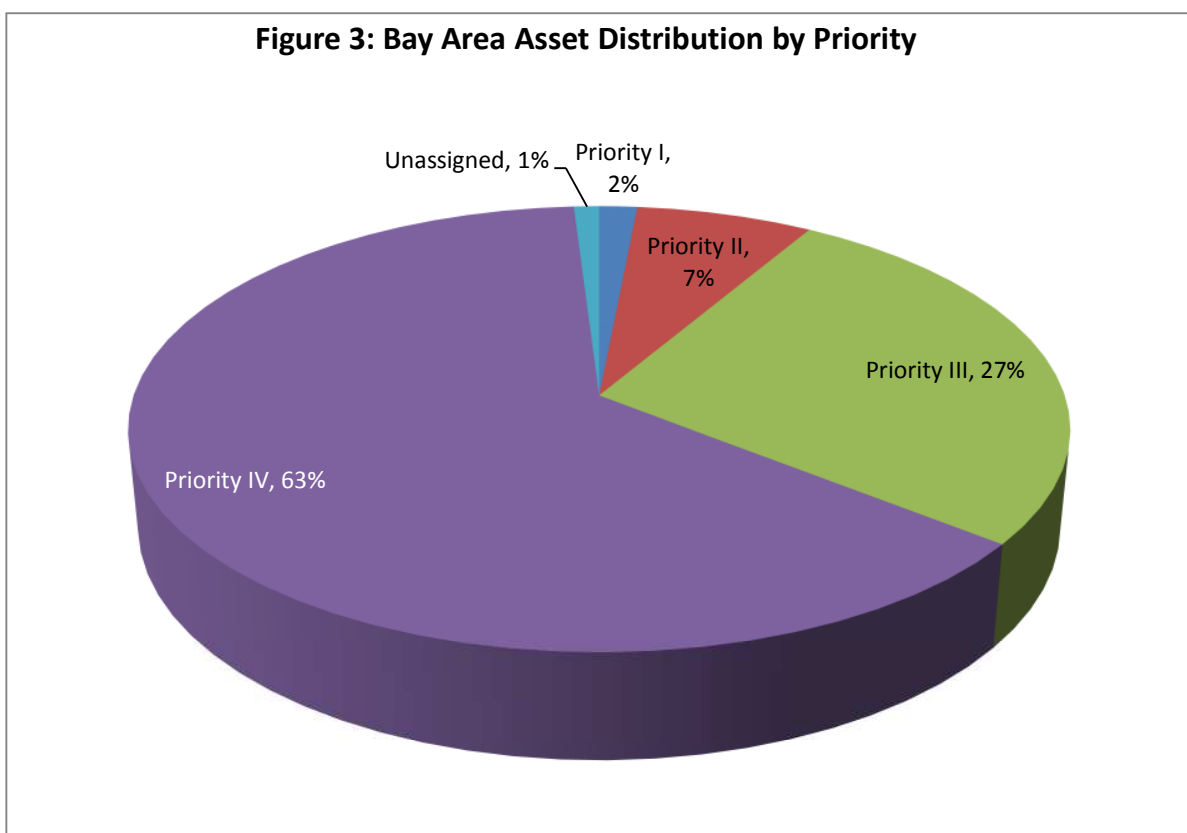
5.5 Risk Profile

The focus of the analysis was on terrorism scenarios and overall terrorism risk to the region's CIKR. However, an analysis was also done concerning natural hazards such as earthquakes, floods and wildfires, etc. This is based on the fact that while natural hazard risk plays a role in how the Bay Area will set its strategic goals and objectives, that role is contingent on a link to terrorism preparedness. Thus, the Bay Area's focus is on building capabilities that have a primary nexus to terrorism while recognizing that such capabilities may also have a "dual" purpose of enhancing all hazards preparedness. This concept of "dual use" has been recognized and encouraged by DHS for many years when developing strategies and investments.

5.5.1 Terrorism Risk

In analyzing the risk of certain attacks against the region's CIKR, the VBIED attack scenario continues to stand out as in years past and as outlined in Figure 4 below. The top four scenarios for the Bay Area region included the vehicle borne improvised explosive device (VBIED) attack, the aircraft as a weapon attack scenario, a conventional IED attack, contagious biological attack and a cyber-attack rounding out the top five.

Figure 4: Bay Area Terrorism Scenario Risk Profile

For Official Use Only   **SECTION 5 RISK OVERVIEW**
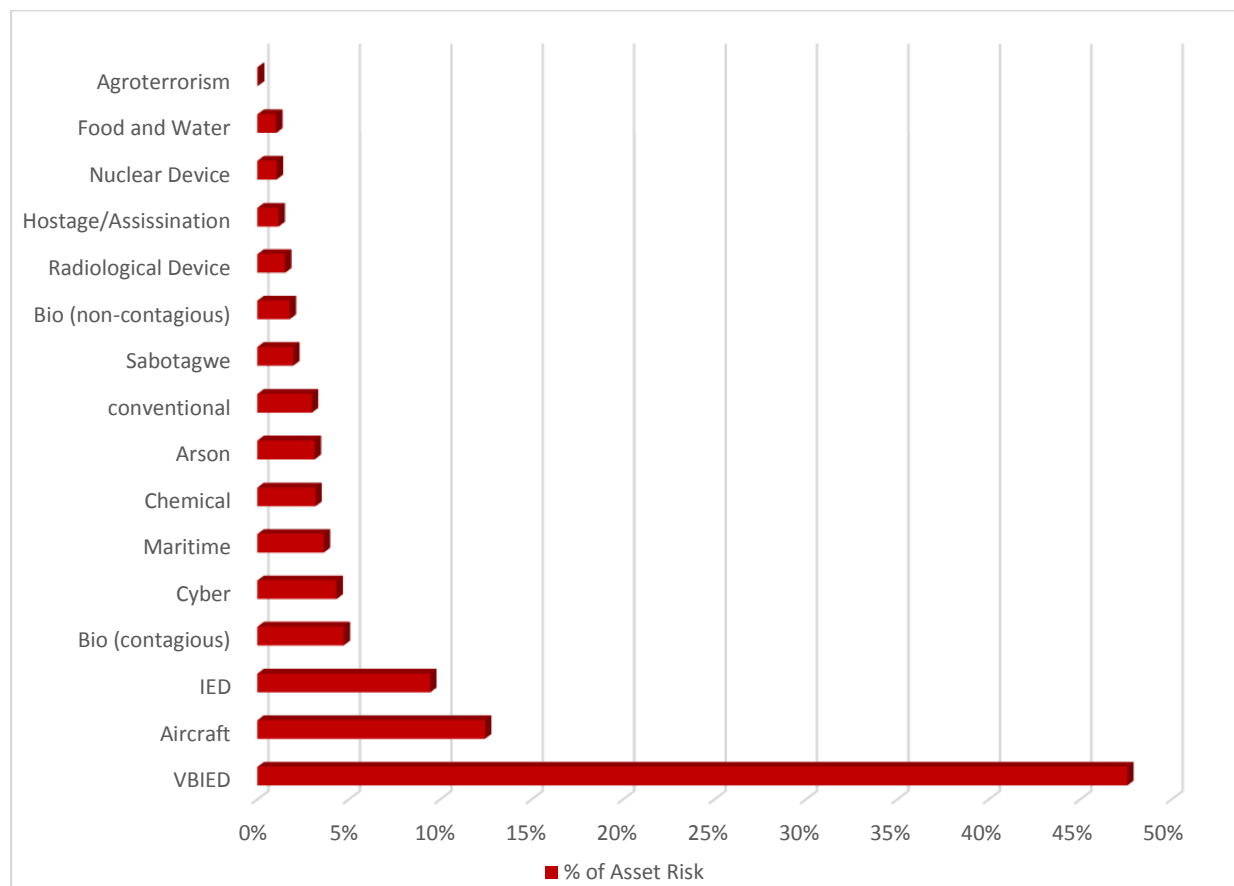
When compared to a threat/likelihood only analysis, i.e., those terrorism scenarios that are the most likely to occur in the Bay Area, the ranking of terrorism scenarios does change for the region. As outlined in Table 5 below, eight out of the sixteen scenarios have a greater likelihood of occurring than they pose an overall risk to the region, while six scenarios pose a greater risk to the region than they are likely to actually occur. Under a likelihood analysis, the top five scenarios in rank order are:

- IED
- VBIED
- Cyber-attack
- Arson
- Sabotage

The top five most likely scenarios for 2013 are consistent with those from 2012. Excluded from this list of the top five most likely scenarios for 2013 are the aircraft as a weapon and contagious biological attack scenarios each of which is in the top five for overall risk, but which have considerably lower likelihood scores than risk scores. This means that while the two scenarios are not likely to occur, in the event they did occur, the region's vulnerability to such attack methods would result in high human, economic and psychological consequences. Figure 5 summarizes risk versus likelihood for all sixteen terrorism scenarios.

Figure 5: Bay Area Terrorism Risk vs. Likelihood

35
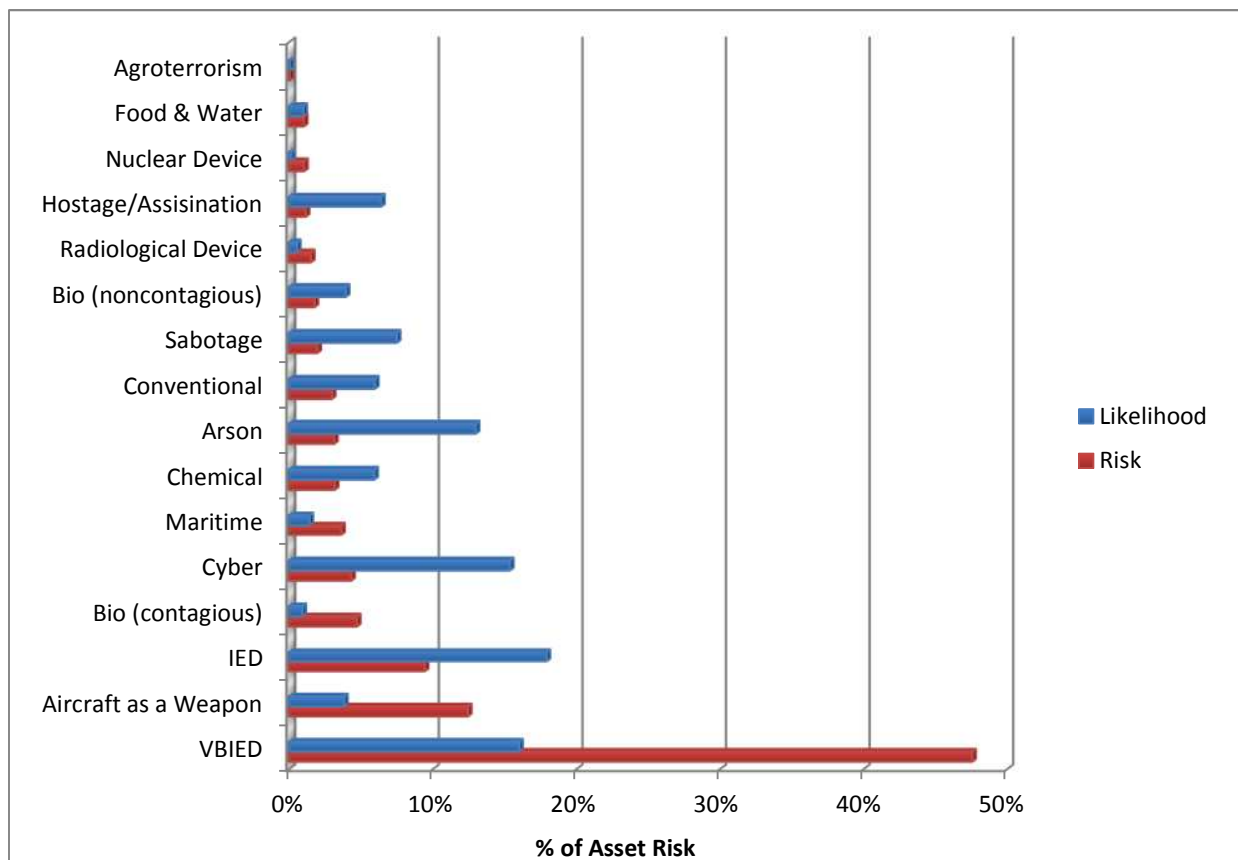
5.5.2 Natural Hazards Risk

The Bay Area's CIKR also face significant risk from natural hazards; in particular floods and earthquakes. As outlined in Figure 6 below, floods pose the greatest risk to the Bay Area's CIKR based upon their frequency, the region's vulnerability to such an event and the consequences of major flooding in terms of lives and property.

Figure 6: Bay Area Natural Hazard Scenario Risk Profile
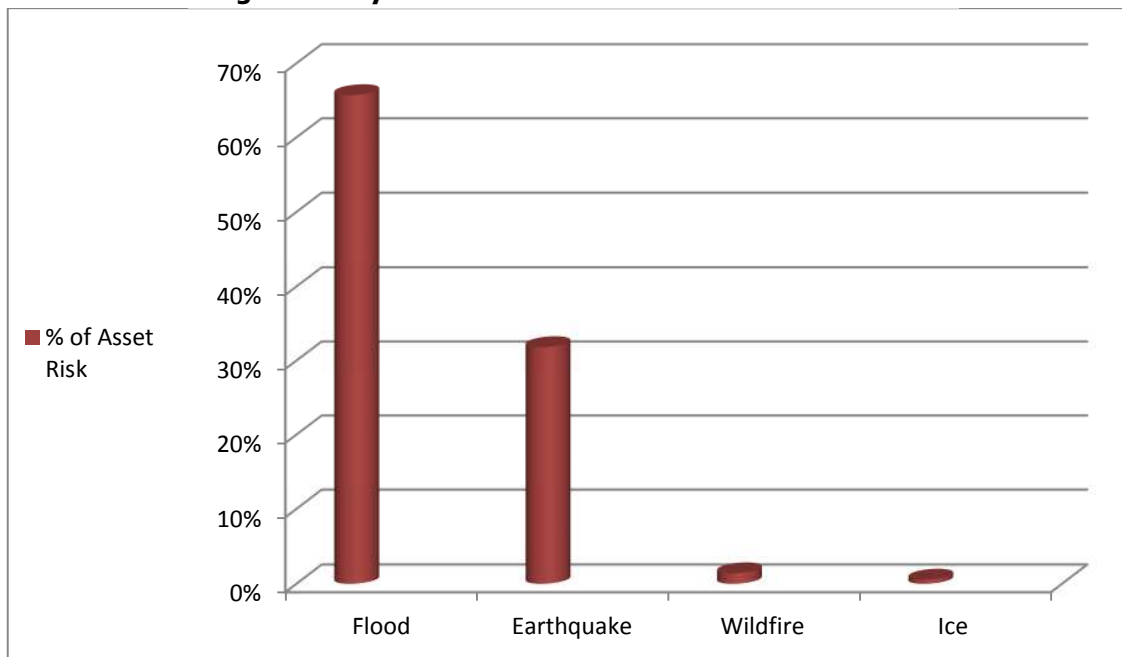
The reason flooding ranks so high in total risk is the very high frequency (likelihood) with which the hazard occurs as compared to an earthquake which is less frequent or likely, but has the potential to cause far more damage to critical infrastructure. The Bay Area rests upon one of the longest and most active earthquake fault systems in the world. This system includes the San Andreas Fault, the Hayward Fault and the Calaveras Fault. The U.S. Geological Survey estimates an 80% chance of a magnitude 6.7 or greater quake striking the Bay Area within the next 30 years.

Based on the Bay Area's topography, the risk from wild land fires is also a reality. Four wildfires in California have burned at least 200,000 acres since 2007. Though evacuations help limit casualties, significant economic loss can still occur.

5.5.3 Threat Hazard Identification and Risk Assessment (THIRA)

Among the various threats and hazards the region has identified, five scenarios have been chosen for the regional THIRA process. From the terrorism scenarios they are a VBIED and cyber attack, from the natural hazard scenarios they are fire and an earthquake, and among technical hazards the region has chosen a major oil spill. These scenarios will provide the region with a

further basis for planning and investing in the near future and may be added to or otherwise amended going forward.

5.6 Asset Risk by Sector

For 2013, the commercial, banking and transportation sectors saw a shift upward in their risk profile. This was due in large part to the more detailed information and assessment results that have been produced for commercial and other assets in the region and the growing sophistication of the region's risk data. This also resulted in a decrease in the percentage of total risk attributed to the government sector as compared to 2012.

Figure 7: Bay Area Distribution of Terrorism Risk by Sector
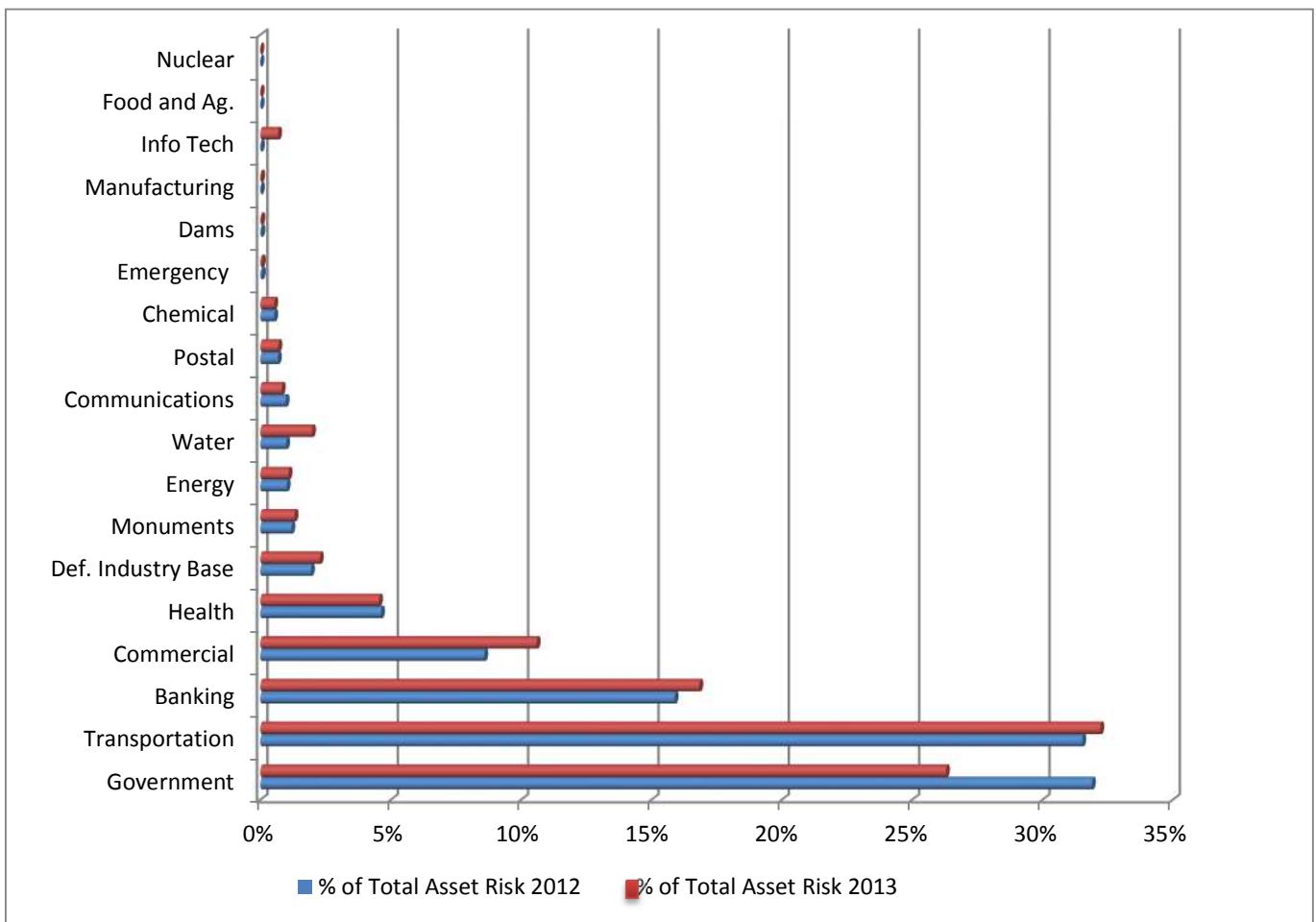
An overarching theme from the Bay Area's risk analysis process is that simply because a sector may be at high or low risk from a particular attack scenario or multiple attack scenarios, each individual asset within each sector may have a risk profile vastly different from the sector at large. This requires regional planners, asset owners and operators, and the agencies responsible for prevention, protection, mitigation, response and recovery activities to evaluate risk data both individually by site and by attack scenario in order to make more precise security investment decisions on specific assets and sectors.

SECTION 5 RISK OVERVIEW

While much of the Bay Area's infrastructure is found in the commercial, government and emergency services sectors, as outlined in Table 5 below, the terrorism asset risk in the Bay Area does not follow the sectors with the largest number of assets. This is most prevalent in the emergency services sector where the sector ranks 3rd in total number of assets (up from 4th in 2012) and yet ranks 14th in total risk. The cause of this type of discrepancy is the nature and type of assets in each sector. A small group of assets or even a single asset can have very high risk due to the likelihood of an attack, the vulnerability to attack and the human, economic, mission and psychological consequences resulting from an attack. When it comes to risk, "quality" very much outweighs "quantity."

Table 5: Bay Area CIKR Sector Rankings

Rank	Sectors Ranked by Total Assets	Sectors Ranked by Terrorism Risk
1	Government	Transportation
2	Commercial	Government
3	Emergency Services	Banking
4	Transportation	Commercial
5	Postal	Health
6	Dams	Defense Industrial Base
7	Water	Water
8	Health	Monuments
9	Banking	Energy
10	Energy	Communications
11	Communications	Postal
12	Food and Agriculture	Information Technology
13	Manufacturing	Chemical
14	Information Technology	Emergency Services
15	Monuments	Dams
16	Chemical	Manufacturing
17	Defense Industrial Base	Food and Agriculture
18	Nuclear	Nuclear

The current list of approximately 13,000 assets represents a major change from 2012 when the region accounted for approximately 8,500 assets. Thus, the Bay Area's asset list is by no means static and will certainly change as the quality of information available to the region continues to improve. For now, the current list reflects a broad representation across multiple CIKR sectors that local subject matter expertise, using best available methods, deem appropriate.

SECTION 5 RISK OVERVIEW

5.7 Capabilities Assessment

Once the 2013 risk assessment was complete, the Bay Area analyzed the relevance of the 31 Core Capabilities based on the region's risk profile. Capability relevance is defined as those capabilities most needed in order to prevent, protect against, mitigate, respond to or recover from threats and acts of terrorism that pose the greatest risk to the region's CIKR. Some of the 31 Core Capabilities are relevant to many different types of hazards affecting the spectrum of CIKR sectors, while others link closely to a few discrete scenarios.

Upon completing the risk relevance analysis, the Bay Area engaged in a two-step capabilities assessment process using the *Bay Area Compendium of Core Capabilities*. The first step involved counties and major cities conducting a local capabilities self-assessment. This was followed by a region-wide self-assessment covering all 31 of the Core Capabilities. For each assessment, capability levels were organized into five areas or answers that determined level of ability: Yes/Complete Success, Substantial Progress, Limited Progress, No Progress and Not Applicable.

Table 6: Capability Assessment Levels of Ability

Yes/Complete Success	The jurisdiction can or does fulfill all elements of the measure/metric with complete (or near complete) success. This can be documented or has been illustrated through real-world experience or multiple exercises.
Substantial Progress	The jurisdiction meets substantial elements of the measure/metric and has a specific plan in place to meet the rest. The jurisdiction does or can likely fulfill the measure/metric with some success, if required.
Limited Progress	The jurisdiction has either part of a plan or equipment in place to fulfill the measure/metric or has individuals/positions identified that have responsibility over the measure/metric, but considerable effort is still required. The jurisdiction does or can fulfill the measure/metric with partial success; it does not or cannot fulfill the measure/metric with much success.
No Progress	The jurisdiction has made no or very little progress toward the measure/metric. The jurisdiction does not or cannot currently fulfill the measure/metric.
Not Applicable	The measure/metric is not applicable to the jurisdiction.

The Core Capabilities were then plotted by terrorism risk relevance *and* capability gap depending on each capabilities risk relevance and the size of the gap in the capability. The Core Capabilities with the largest capability gap and highest risk relevance were ranked the highest priority for gap mitigation. The results from the Bay Area's 2013 Core Capabilities assessment are summarized in Table 7 below.

Table 7: Capability Assessment Results

Risk and Gap	Core Capability	Risk Relevance	Level of Ability	Gap Analysis
1	Infrastructure Systems	3	25%	Needs Extra Attention
2	Long Term Vulnerability Reduction	6	31%	Needs Attention
3	Physical Protective Measures	7	39%	Needs Attention
4	Public Information and Warning	9	26%	Needs Attention
5	Operational Communications	16	34%	Needs Attention
6	Community Resilience	1	69%	Needs Attention
7	Intelligence and Information Sharing	4	55%	Needs Attention
8	Planning	8	58%	Needs Attention
9	Situational Assessment	12	57%	Needs Attention
10	Screening, Search and Detection	14	68%	Needs Attention
11	Forensics and Attribution	2	79%	Sustain
12	Interdiction and Disruption	5	70%	Sustain
13	Risk and Disaster Resilience Assessment	10	90%	Sustain
14	Risk Management for Protection Programs	11	82%	Sustain
15	Threats and Hazard Identification	13	84%	Sustain
16	Operational Coordination	15	80%	Sustain
17	Access Control and Identity Verification	18	34%	Needs Attention
18	Critical Transportation	21	27%	Needs Attention
19	Cyber Security	20	33%	Needs Attention
20	Natural and Cultural Resources	28	30%	Sustain
21	Public Health and Medical	19	67%	Sustain
22	Fatality Management	21	61%	Sustain
23	Mass Search and Rescue	23	69%	Sustain
24	On-Scene Security and Protection	18	85%	Sustain
25	Supply Chain Integrity	26	25%	Sustain
26	Health and Social Services	25	34%	Needs Attention
27	Mass Care	29	42%	Sustain
28	Housing	31	38%	Sustain
29	Environmental Response/Health and Safety	24	82%	Sustain
30	Economic Recovery	27	38%	Sustain
31	Public and Private Services and Resources	30	49%	Sustain

The results of the capabilities assessment were then linked to those hazards that pose the greatest risk to the region, and CIKR sectors in the region at greatest risk from those hazards. The result is the matrix set forth below in Table 8, which provides a blue print for planning and investing in order reduce the risk to the listed CIKR sectors posed by the listed hazards by enhancing or sustaining the listed Core Capabilities.

Table 8: Hazards, Sectors and Capabilities Matrix

Highest Risk Hazards	Terrorists' Use of Explosives	Earthquake	Floods	Contagious Biological
Sectors at Highest Risk	Transportation	Commercial	Water	Transportation
	Government	Health	Government	Government
	Banking	Government	Transportation	Health
	Commercial	Transportation	Health	Commercial
	Health	Information Technology	Emergency Services	Banking
Most Relevant Capabilities	Planning	Planning	Planning	Planning
	Operational Communications	Operational Communications	Operational Communications	Risk Management for Protection Programs and Activities
	On-Scene Security and Protection	Community Resiliency	Community Resiliency	Intelligence and Information Sharing
	Threat and Hazard Identification	Risk and Disaster Resilience Assessment	Threat and Hazard Identification	Public Health and Medical
	Intelligence and Information Sharing	Intelligence and Information Sharing	Intelligence and Information Sharing	Intelligence Analysis and Production
	Critical Infrastructure Protection	Long Term Vulnerability Reduction	Situational Assessment	Critical Transportation
	Interdiction and Disruption	Operational Coordination	Operational Coordination	Public Information and Warning
	Mass Search and Rescue	Public and Private Services	Public and Private Services	Fatality Management
	Operational Coordination	Volunteer Management and Donations	Critical Transportation	Environmental Response
	Fatality Management	Public and Private Services	Public Information and Warning	Infrastructure Systems
	Public Health and Medical	Critical Transportation	Mass Care	Forensics and Attribution
			Mass Search and Rescue	
	Environmental Response	On-Scene Security and Protection	Fatality Management	Situational Assessment
			Public Health and Medical	
			Economic Recovery	
		Economic Recovery		
	Screening, Search and Detection	Fatality Management	Infrastructure Systems	
	Long Term Vulnerability Reduction	Situational Assessment		
	Forensics and Attribution	Mass Care		
	Physical Protective Measures	Mass Search and Rescue		
	Situational Assessment	Infrastructure Systems		
	Risk Management for Protection Programs and Activities	Public Health and Medical		
		Public Information and Warning		

SECTION 5 RISK OVERVIEW

SECTION 6
GOALS, OBJECTIVES & IMPLEMENTATION STEPS

6.1 Overview

The goals and objectives of the *Strategy* serve as the core for what the Bay Area will seek to achieve over the next three years in the mission areas of prevention, protection, mitigation, response and recovery. The goals and objectives represent the culmination of integrating risk and capabilities assessment by establishing specific implementation steps that are designed to achieve or maintain capability outcomes in those capabilities that are most relevant based on the Bay Area's risk and capability profile.

The goals and objectives are directed towards the next three years but may be reviewed and updated annually or as needed. It is likely that some of the objectives will carry over from year to year while others may be removed or updated based on the region's progress and actual needs. The goals and objectives will continue to be defined by risk analysis, identified preparedness gaps and sustainment priorities.

6.2 Organizing the Goals and Objectives

The goals and objectives represent not only the priorities of the region but also the region's implementation of State and National level policy and priorities at the regional level. As such, each goal is based on alignment with the National Homeland Security Priorities (and/or the State of California Homeland Security Strategy priorities) and each objective with a Core Capability or set of Core Capabilities, or a CDC Public Health Preparedness Capability for medical and health related objectives. The purpose of aligning each objective to a capability is to ensure the *Strategy* is designed around managing risk by enhancing capabilities through investments and other activities.

The Core Capabilities and Public Health Preparedness Capabilities were first organized under relevant National Priorities. The National Priorities were then converted, and sometimes merged, into regional goals with the capabilities converted into specific objectives under each goal. Where no equivalent National Priority exists, the Bay Area simply developed its own goal to meet its own local needs. For example, the Bay Area has developed a recovery goal, whereas the federal government has not delineated recovery as a National Priority. In addition, the federal government has listed implementing the NIPP and Strengthening Information Sharing and Collaboration as separate National Priorities. The Bay Area has combined both priorities into a single regional goal designed to enhance information analysis and infrastructure protection.

6.3 Structuring the Goals and Objectives

The goals and objectives are structured around sustaining sufficient levels of ability and closing identified capability gaps. While capabilities from the Core Capabilities Public Health Preparedness Capabilities are listed as their own objective, the objectives, like the capabilities themselves, do not operate in a vacuum. Objectives often are linked to one another with elements

of one objective sometimes found in another. This is a product of the fact that the capabilities are not isolated from each other. Rather, they overlap one another with elements of one capability present in another or even several others.

Using the capabilities-based planning model as outlined by DHS, each goal and related objective(s) will be implemented through a series of resource elements divided among the elements of capability: plans, organization, equipment, training and exercises (POETE) as defined in Table 9 below." The POETE resource elements outline what resources are needed for the region to achieve each capability based objective. They serve as a critical strategic guide for the region and jurisdictions to develop actual projects that will result in achievement of a particular objective. As such, they are not an exhaustive list meant to limit steps necessary to achieve a goal or objective but instead operate as a roadmap.

The detail of a POETE implementation step may vary from objective to objective or even in a single objective depending on the level of detailed data available from risk and capabilities assessments. Finally, the region and jurisdictions are *not* required to generate projects for each goal and objective in a given grant or funding cycle. Rather, each grant applicant must prioritize projects based on this Strategy and their own risk and need.

Table 9: Elements of Capability[10]

Planning	Development of policies, plans, procedures, mutual aid agreements, strategies and other publications that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and actions.
Organization	Specific personnel, groups or teams, an overall organizational structure, and leadership at each level in the structure that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks. Paid and volunteer staff who meet relevant qualification and certification standards necessary to perform assigned missions and tasks.
Equipment	Major items of equipment, supplies, facilities, and systems that comply with relevant standards necessary to perform assigned missions and tasks.
Training	Content and methods of delivery that comply with training standards necessary to perform assigned missions and tasks.
Exercises	Exercises, self-assessments, peer-assessments, outside review, compliance monitoring, and actual major events that provide opportunities to demonstrate, evaluate, and improve the combined capability and interoperability of the other capability elements to perform assigned missions and tasks to standards necessary to achieve successful outcomes.

Set forth below are the 2012-2015 homeland security goals and objectives for the Bay Area UASI region.

---

[10] U.S. Department of Homeland Security, *Target Capabilities List* (September 2007).

GOAL 1	Mission Area(s)	National Priorities	Core Capabilities	State Strategy
ENHANCE REGIONAL RISK MANAGEMENT AND PLANNING PROGRAM	Common	All	Planning Threat and Hazard Identification Risk and Disaster Resilience Assessment	N/A

Risk Management

In 2009, the Bay Area began developing a regional risk management and planning program to enable the region to develop, sustain and fund programs, plans and operations based on risk and capabilities assessment data. Today, this risk management program has matured to the point where it serves as the foundation for collecting and analyzing data to support strategic, operational and tactical level planning across the region.

A risk regional management framework is one in which all available data and subject matter expertise and experience is utilized to make informed decisions on what actions should be taken based on the costs of such actions and the return on investment in terms of mitigating the identified risks. The risk management program encompasses virtually all of the region's activities from prevention, protection, mitigation, response and recovery efforts. A risk management program does not eliminate risk. It manages risk.

The Bay Area will continue to assess risk on a regular basis and in a consistent manner in order to provide a common understanding of the threats and hazards confronting the region. This information will, in turn, be used to help better understand what capabilities the region must possess to adequately address those risks. Part of this process will include the federally required threat and hazard identification and risk assessment (THIRA). While there are differences, the THIRA codifies at the federal level much of what the Bay Area has already begun at the regional level in terms of identifying scenarios and hazards that pose a significant risk to the region and the capabilities necessary to address those risks. The THIRA is very similar to the established hazard identification and risk assessment (HIRA) used to develop hazard mitigation plans at the Operational Area level.

SECTION 6 GOALS AND OBJECTIVES

Objective 1.1: Enhance Planning, Threat and Hazard Identification, and Risk Management Capabilities

The Bay Area is able to identify and assess the threats and hazards that pose the greatest risk to the whole community. The region can prioritize and select appropriate capability-based planning investments and solutions for prevention, protection, mitigation, response, and recovery concerning those risks; monitor the outcomes of allocation decisions; and undertake corrective and sustainment actions.

Objective 1.1 Implementation Steps and Resource Elements

PLANNING	
1.1-P1	Develop an actionable risk management strategy that includes short, medium, and long term risk management objectives at the regional and jurisdictional level. This will include an annual risk overview report for the region and risk-based formulas to allocate resources to include funding.
1.1-P2	Assign a lead planner from the Bay Area UASI to coordinate the risk management program.
1.1-P3	Develop data collection timelines, requirements, and avenues for receiving information on local threats, vulnerabilities, and consequence of loss from stakeholders at the regional, sub-regional and jurisdictional levels as part of an annual risk assessment.
1.1-P4	Conduct annual risk validation analysis – threats, vulnerabilities, consequences - for the region and, as necessary, for each operational area and such other entities as required across the Bay Area. Continue to expand the use of localized vulnerability and consequence of loss data in the analysis.
1.1-P5	Rank criticality of CIKR assets and potential targets from across the region.
1.1-P6	Organize and prioritize capabilities at the regional and jurisdictional level (where appropriate) based on those capabilities most directly linked to prioritized risks.
1.1-P7	Develop annual strategy implementation guidance and project templates for DHS UASI application process. Ensure project templates link projects to risk and capability gaps and *Strategy* goals and objectives.
1.1-P8	Develop an annual capability assessment and gap analysis process to determine where gaps remain among capabilities with an emphasis on those capabilities necessary to address the region's highest risks.
1.1-P9	Assign/hire planners to assist in the implementation, evaluation and updating of the *Bay Area Homeland Security Strategy* and preparedness report at the regional, sub-regional and jurisdictional levels.
1.1-P10	Produce a Bay Area annual report that outlines the annual accomplishment and major activities to ensure all appropriate stakeholders are kept informed.
1.1-P11	Conduct grant effectiveness analysis and produce grant effectiveness reports to demonstrate the value of UASI and other homeland security grants to local, state and national leaders.
1.1-P12	Bay Area UASI Management Team to provide strategic planning technical assistance to Operational Areas as needed.

1.1-P13	Update, as needed, the *Bay Area Homeland Security Strategy* based upon the latest risk and capabilities assessment data.
1.1-P14	Ensure each Operational Area has an up-to-date hazard mitigation plan, continuity of operations plan (COOP), and continuity of government (COG) plan.
ORGANIZATION	
1.1-O1	Communicate in writing with all regional stakeholders the risk management process and the intent to use risk in decision making.
1.1-O2	Develop a risk management framework or working group to outline how risk assessments and risk analysis serve the process of managing "risks" and a process for stakeholder buy-in across all four sub-regions. This may include a comprehensive stakeholder governing process and governing bodies to oversee the risk management process.
1.1-O3	Assign/hire risk analysts to conduct risk analysis and produce risk products on behalf of the region, sub-regions and jurisdictions
EQUIPMENT	
1.1-E1	Sustain capabilities and risk management software and systems for the region to conduct capabilities and risk analysis to include threats, vulnerabilities and consequence of loss analysis to support tactical, operation and strategic level planning and operations.
TRAINING	
1.1-T1	Conduct principles of risk management training for policy makers and stakeholders from across the region.
1.1-T2	Train Bay Area UASI Management Team and the NCRIC staff on the use of risk analytic tools and software planning systems.
EXERCISES	
1.1-Ex1	Ensure UASI exercise program is risk based with scenarios used and capabilities tested tied to risk.
1.1-Ex2	Conduct exercises to test COOPs and COG plans at the Operational Area and local levels.

SECTION 6 GOALS AND OBJECTIVES

GOAL 2	Mission Area(s)	National Priorities	Core Capabilities	State Strategy
ENHANCE INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION CAPABILITIES	Prevention Protection	Strengthen Information Sharing and Collaboration Capabilities Implement the *NIPP* Enhance Regional Collaboration	Long Term Vulnerability Reduction Forensics and Attribution Interdiction and Disruption Screening, Search and Detection Risk Management for Protection Programs/Activities Physical Protective Measures Intelligence and Information Sharing Access Control and Identity Verification Cyber Security	Goal 1: Enhance Information Analysis and Law Enforcement Capabilities Goal 2: Protect Critical Infrastructure and Key Resources

The National Intelligence and CIKR Protection Framework

Collecting and sharing information to protect critical infrastructure from threats and acts of terrorism is a core element of homeland security. In October 2007, to better coordinate the Nation's information sharing activities, the Federal Government released the *National Strategy for Information Sharing* (National Strategy). In 2006, DHS published the final *National Infrastructure Protection Plan* (*NIPP*) with a revised version released in 2009. Both the *NIPP* and the National Strategy represent the national level plan for information sharing and CIKR protection, the implementation of which often occurs at the local level.

The *National Strategy* is intended to ensure that those responsible for combating terrorism and protecting local communities have access to the timely and accurate information they need by:

SECTION 6 GOALS AND OBJECTIVES

- Providing a framework for enhanced information sharing among federal, state, local, and tribal officials; the private sector; and foreign partners to aid their individual missions and to help secure the U.S. homeland.

- Describing the Federal Government's approach to supporting state and major urban-area NCRICs, as well as national efforts to fight crime and make local communities safer.

- Recognizing that as information-sharing capabilities are enhanced, it is imperative that the legal rights of U.S. citizens continue to be protected, especially in the area of privacy and civil liberties.

The goal of the *NIPP* is to enhance protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. The *NIPP's* supporting CIKR Sector-Specific Plans were released in May 2007 and provide the coordinated approach to establish national priorities, goals, and requirements for protection across each of the 18 CIKR sectors at the national level.

The Nationwide Suspicious Activity Reporting Initiative

Virtually every sophisticated terrorist attack has involved some form of pre-attack planning, surveillance and logistical support functions. Most of these pre-attack activities may or may not be criminal in nature, but virtually all could appear suspicious if viewed in isolation and potentially unravel a terrorist plot if viewed in total by a NCRIC or other intelligence agency. In order for such a total view to take place, the Nationwide Suspicious Activity Reporting (SAR) Initiative was created to allow law enforcement agencies to "develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities."[11] The Bay Area's Northern California Regional Intelligence Center (NCRIC) and law enforcement agencies can play a critical role in this process by linking not only suspicious activities in the region, but fusing those regional SARs with other suspicious activities from across the country to determine if terrorist plots are underway.

California's Intelligence Structure

Consistent with the *National Strategy* and the *NIPP,* the State of California has developed the State Threat Assessment System (STAS) to "protect California's citizenry and economy from terrorism and other criminality by collaboratively producing and disseminating critical threat information to its homeland security partners." The STAS is a public safety partnership that obtains, analyzes, and shares information, and collaboratively develops and shares California-

---

[11] U.S. Department of Justice, Bureau of Justice Assistance, Nationwide SAR Initiative, accessed at http://nsi.ncirc.gov/documents/Nationwide_SAR_Initiative_Overview_2012.pdf

specific counter-terrorism intelligence products enabling law enforcement to prevent terrorism in California.

The STAS is made up primarily of the State Threat Assessment Center (STAC), which is the State NCRIC operated by the California Highway Patrol and CalEMA; the CalDoJ Intelligence Operations Center (IOC); and four Regional Threat Assessment Centers (RTAC) located in San Diego, Los Angeles, Sacramento and the Bay Area. The STAS is a partnership of these organizations with no single organization exercising command and control over the other. In 2008, California issued the STAS Strategic Business Plan Concept of Operations, which outlines the vision, mission, structure and operations of the STAS. This ConOp was updated in early 2011.

The STAC is responsible for coordinating with the RTACs and compiling the overall State Threat Assessment. It supports regional intelligence analysis by supplying the RTACs with additional analytical support. Each RTAC's geographic area of responsibility coincides with the local FBI field office for that region. The RTAC's work extensively with their local FBI led Joint Terrorism Task Force (JTTF) and Field Intelligence Group (FIG).

Operating within each RTAC is a Terrorism Liaison Officer (TLO) program made up of public safety agency officer(s) trained in understanding terrorism who serve as the bidirectional gateway for terrorism information between the members of his/her own department, the RTACs and CIKR owners and operators.

The Bay Area's Intelligence and Infrastructure Protection Structure

The NCRIC serves as the Bay Area's RTAC and NCRIC. The NCRIC helps safeguard the region by assisting public safety agencies from across the Bay Area in their mission to detect, prevent, investigate and respond to criminal and terrorist activity. The NCRIC is a cooperative federal, state and local public safety effort to centralize the intake, analysis, fusion, synthesis, and appropriate dissemination of criminal and homeland security intelligence. The NCRIC disseminates intelligence and facilitates communications between state, local, federal agencies and private sector partners, in order to help them take action on threats and public safety issues.

The NCRIC is also the region's primary infrastructure protection management entity. It embodies the Bay Area's approach to information sharing and analysis and critical infrastructure protection which is to fuse the two missions by collecting, analyzing and sharing threats to CIKR in order to review intelligence data and map threats against CIKR, determining the threatened infrastructure's vulnerability, and recommending a suite of protective measures and other resources to mitigate the risk posed by the threat.

The Bay Area will work with its partners at all levels of government and the private sector throughout the intelligence cycle to ensure that information is turned into useful intelligence while at the same time respecting the privacy and civil liberties of all of its people. This will include enhanced cooperation and coordination with the region's JTTF, the region's NCRIC, local law enforcement, and private sector security forces in and around the region's critical infrastructure and key resources.

The Bay Area's Cyber Security Framework

Since September 11, 2001, states and local jurisdictions across the U.S. have allocated significant time and resources to enhance intelligence sharing, physical security and emergency response capabilities. Too often, however, the digital world has been left as an afterthought in the homeland security enterprise. Not surprisingly, cyber based attacks against states and local governments are on the rise. To counter this increasing threat, the Bay Area has adopted a cyber security objective to build specific capabilities in cyber space, which will reduce cyber risk.

According to the National Preparedness Goal, cyber security is the ability to "protect against damage to, the unauthorized use of, and/or the exploitation of (and, if needed, the restoration of) electronic communications systems and services (and the information contained therein)." The National Institute of Science and Technology further defines cyber security as "the ability to protect or defend the use of cyberspace from cyber-attacks."

While cyber security is primarily focused on the *protection* of cyber infrastructure, cyber preparedness is a more comprehensive view of cyber space in the area of homeland security. Cyber preparedness is the capability to *prevent, protect against, mitigate, respond to, and recover from* threats and acts of terrorism and other hazards occurring in cyber space that have impacts in the cyber and/or physical world. This outline of cyber preparedness effectively mirrors the homeland security mission areas in the physical world--the only difference being their application to the cyber environment. While the Bay Area will begin its focus on cyber security, which is an element of cyber preparedness, the region's strategy is to move toward a more comprehensive cyber preparedness framework in the near future.

As called for under Executive Order 13636 issued in February 2013, the National Institute of Science and Technology (NIST) began developing a cyber security framework. While still in draft form as of October 2013, the framework is designed to provide a common language and mechanism for organizations to:

> 1) describe current cyber security posture; 2) describe their target state for cyber security; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; and 5) foster communications among internal and external stakeholders.[12]

The Bay Area will use this framework to inform its approach to cyber security and address cyber risk. Such cyber risk can come in a number of different forms in terms of the type of attacker and the method of attack employed. Tables 10 and 11 below summarize the U.S. General Accountability Office and the National Institute of Science and Technology descriptions of major cyber threat actors and attack methodologies.[13]

---

[12] National Institute of Science and Technology, *Draft Cyber Security Framework*, page 1 (August 2013).

[13] Government Accountability Office, *Department of Homeland Security's Role in Critical Infrastructure Protection Cybersecurity,* GAO-05-434 (May, 2005); and NIST *Special Publication 800-82*, *Guide to Supervisory Control and Data Acquisition and Industrial Control System Security* (June 2011).

SECTION 6 GOALS AND OBJECTIVES

Table 10: Major Cyber Threat Actors

Threat Actors	Description
Terrorists	Terrorists may use phishing schemes or spyware/malware and other attack methods to disrupt or disable critical infrastructure, or to steal funds or sensitive information.
Cyber Criminals	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent. Their goals are profit-based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat.
Foreign Governments	These actors usually involve the intelligence services of foreign governments. Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure when attacked by the U.S. to damage the ability of the US to continue its attacks.
Hacktivists	Hacktivists include individuals and groups, e.g. Anonymous, with anti-U.S. motives or other political agendas. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause.
Hackers	Hackers are often categorized as follows: • Script kiddies are unskilled attackers who do not have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages. • Worm and virus writers are attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems. • Security researcher and white hat have two sub-categories; bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security, earn money, and achieve recognition with an exploit. • Professional hacker-black hat who gets paid to write exploits or actually penetrate networks; also falls into the two sub-categories-bug hunters and exploit coders. Their goal is profit.
Bot-network	Bot-network operators are hackers; however, instead of breaking into systems

52

Operators	for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Insiders	The disgruntled organization insider is a principal source of computer crime. This could be a full or part-time employee or contractor. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes individuals who *accidentally* introduce malware or spyware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware and Malware Authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

Table 11: Major Cyber Attack Methods

Attack Methods	Description
Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources or the delaying of system operations and functions.
Telephone Denial of Service	Attacks that clog phone lines and interrupt regular phone usage and business with a flood of false call traffic.
Doxing	The collection and unauthorized release of personally identifiable information to the public. This may include all relevant personal details, such as name, address, phone numbers, date of birth, Social Security Number, social networking information, usernames, passwords, images, and anything else that is related to them in an identifying capacity.
Phishing	A digital form of social engineering that uses authentic-looking—but phony—emails to request information from users or direct them to a fake Web site that requests information.
Watering Hole Attack	Tactics that combined social engineering and malware to target specific individuals at companies or government agencies by infecting legitimate and frequently visited websites and exploiting holes in browser software systems with the goal of stealing trade or other secrets.
Virus	A hidden, self-replicating section of computer software, usually malicious

	logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.
Worms	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.
Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Super Cyber Weapons	Cyber-attack methods that are so sophisticated they require a government sponsor to develop and deploy them, e.g. the Stuxnet Virus. Such weapons are often deployed against other governments in order to conduct intelligence gathering and/or sabotage.

The Bay Area has not been immune to the risk of cyber threats. In 2012 and 2013 alone, the region was the target of several high profile cyber-attacks. These include:

Alameda County System Infected by Trojan Virus

On August 24, 2012 the Alameda County Sheriff's Office IT Department identified a virus known as the "SCR" or "PE_QUERVAR" virus. The virus affected .doc, .xls, and .exe files. The virus spread rapidly through servers and altered file-type and file-names. For example, the original file name may have been window.doc, but was altered to file name window_cod.scr. Some of the infected files caused administrator lock-outs. Such root infection requires a reboot and when reverted to its original state, this alters the date of the file, which can adversely impact evidence in criminal and other proceedings.

City of Oakland Doxed

On January 28, 2012, law enforcement in Oakland conducted a raid of Occupy Oakland. Following that raid, the group "Anonymous doxed numerous elected and senior appointed officials in the city. This included Oakland Mayor Jean Quan and her husband, the City Administrator, the Police Chief, the City Attorney, and seven City Council members.

NCRIC Targeted By Spear-Phishing Attacks

On November 15, 2012 and again on December 20, 2012 the NCRIC was target by sophisticated spear-phishing attacks involving well-crafted, convincing messages from false accounts created to impersonate actual NCRIC employees. The emails demonstrated detailed institutional knowledge of the NCRIC. The November 15th attack involved a "Press Release 11.14.12" that was sent to thirteen NCRIC staff members from the NCRIC's Private Sector Outreach Coordinator. The email came from an "aol.com" account and included a backdoor Trojan, "Backdoor:Win32/Dalbot.gen."

The December 20th attack involved an email "FW: Threats to the Homeland and Agency Reaction" that was sent to eleven NCRIC staff members, including the former NCRIC Director,

supposedly from the NCRIC's then Deputy Director forwarding a document from DHS Secretary Janet Napolitano. The email used a "yahoo.com" account and involved an unknown virus.

Bay Area's Initial Cyber Security Program

Over the next 24 months, the region will begin implementation of its cyber security objective. This will include focusing on the areas of planning, organization and training. Once the initial plans, organizing structures, and training are in place, the region will then procure equipment, and conduct exercises to test the effectiveness of the region's new cyber capabilities.

The planning goals are to:

- promote the increase of cyber security defenses
- develop actionable plans for the mitigation of cyber vulnerabilities
- increase awareness of cyber threats and vulnerabilities and how to address them

Under organization, the region will address the need for improved information sharing processes and systems in order to:

- Enhance the protection of Private Sector and State/Local/Tribal/Territorial networks
- Support cyber-crime investigations
- Strengthen current cyber incident response mechanisms
- Promote private and public sector cooperation and information sharing

Information sharing initiatives include both human-to-human and automated, near real-time machine-to-machine information sharing projects and processes. The NCRIC will hire analysts to accomplish these goals.

Finally, cyber security training will be a vital part of any defense against cyber attacks. The region will develop training for employees and managers on the techniques, tactics, and procedures used by malicious threat actors to attack targets – e.g. spear phishing, SQL injections, and watering hole attacks. This training will include:

- "high-level" awareness training for all personnel on how to respond in the case of an incident, including the appropriate process to notify the IT department, what not to do when infected, and what information to convey to the appropriate responding agencies/organizations.
- Associated with the "awareness training" will be more focused cyber training for IT security professionals, law enforcement and public safety. Such training will be akin to the regular training given by Fusion Centers on drug trafficking, terrorism, and gangs.

The following regional security objectives outline the fully integrated approach the Bay Area will take to prevent and protect against risks arising out of the physical and cyber worlds.

Objective 2.1 Enhance Intelligence Collection, Analysis and Sharing

The Bay Area has systems and procedures to effectively collect, analyze and timely share information and intelligence across federal, state, local, tribal, territorial, regional, and private sector entities to achieve coordinated awareness of, prevention of, protection against, mitigation of, and response to a threatened or actual terrorist attack, major disaster, or other emergency. This involves sustaining and building upon the region's intelligence fusion center to include the ability to identify and systematically report suspicious activities associated with potential terrorist or criminal pre-operational planning and logistics.

Objective 2.1 Implementation Steps and Resource Elements

PLANNING	
2.1-P1	Ensure NCRIC planners and NCRIC fiscal agents are in place.
2.1-P2	Maintain plans and protocols to ensure connectivity between the NCRIC and other RTACs in California.
2.1-P3	The NCRIC should lead the development of and maintain operationally sound policies to comply with regulatory, statutory, privacy, and other issues that may govern the gathering and storing of intelligence/information.
2.1-P4	The NCRIC will work to ensure that jurisdictions understand and follow suspicious activity reporting guidelines.
2.1-P5	Ensure public awareness campaigns are in place, e.g. "see something, say something" at the jurisdictional level and within critical infrastructure sectors to ensure the public and private sectors report suspicious activity to appropriate authorities. Ensure the relevant information is shared with the NCRIC for action as necessary.
2.1-P6	Ensure that processes, protocols, and technical capabilities are in place at the regional and sub-regional level to allow proactive reporting and extraction of information from public, private, and law enforcement databases to the NCRIC.
2.1-P7	Develop plans and protocols to utilize social media in the acquisition of suspicious activity reports.
2.1-P8	The NCRIC will develop plans, to include MOUs, MOAs, SOPs, among Bay Area jurisdictions, outside jurisdictions, and the State of California, for the deployment of automated license plate readers (ALPRs) at fixed critical infrastructure sites as well as roaming ALPRs.
2.1-P9	Develop or maintain plans and procedures for the dissemination and routing of information and intelligence received by law enforcement agencies from outside entities and develop governance and privacy manuals.
2.1-P10	Continue to develop Terrorism Liaison Officers (TLOs) across all disciplines in the Bay Area with a particular emphasis on developing Health, Medical and Emergency Management TLOs.
2.1-P11	Develop plans and protocols for the sharing of public health and medical information between the NCRIC and the public health and medical community to include disease surveillance information.
2.1-P12	Develop plans and SOPs for intelligence sharing between the NCRIC and mass transit systems across the Bay Area.

SECTION 6 GOALS AND OBJECTIVES

2.1-P13	Ensure the private sector and public works agencies are a part of the intelligence and information sharing process across the Bay Area.
2.1-P14	Ensure the NCRIC has an up to date continuity of operations plan (COOP).
2.1-P15	Local law enforcement agencies should develop and maintain written policies, guidelines and procedures for monitoring social media to detect potential threats.
ORGANIZATION	
2.1-O1	Develop administrative structures and protocols to support TLOs and local law enforcement in getting the NCRIC necessary information which can later be disseminated by the NCRIC across the region to local partner agencies.
2.1-O2	Provide funding to support NCRIC staff including intelligence analysts.
2.1-O3	Ensure all necessary personnel possess valid and current national security clearances.
2.1-O4	Provide funding to support NCRIC staff including critical infrastructure protection teams, public health and medical personnel, public safety personnel, and support staff.
2.1-O5	Develop and manage counter-surveillance teams out of the NCRIC and within certain law enforcement agencies across the region to provide counter-surveillance capabilities at CIKR across the Bay Area.
2.1-O6	Develop local and regional public awareness and reporting campaigns for suspicious activity reporting similar to the National "If You See Something, Say Something" campaign, and IWatch in Los Angeles and Washington, DC, etc.
2.1-O7	Develop a policy and process to raise awareness of the NCRIC and its mission with policy makers, elected officials, first responders, community leaders and the general public.
2.1-O8	Develop a process for the NCRIC to receive stakeholder feedback on all parts of the intelligence cycle to include feedback on training and exercises on intelligence and infrastructure protection.
EQUIPMENT	
2.1-E1	Acquire and deploy interoperable ALPR systems at high risk critical infrastructure sites across the Bay Area to detect patterns of suspicious behavior indicative of terrorist pre-operational surveillance.
2.1-E2	Ensure surveillance detection equipment is acquired and deployed at critical infrastructure and other key sites in the Bay Area including: cameras, detectors, and sensors that can send data collected to the NCRIC either directly or indirectly for analysis.
2.1-E3	Ensure all major law enforcement agencies across the Bay Area have the technology to gather and link suspicious activity reporting within each respective law enforcement agency.
2.1-E4	Acquire equipment to allow different law enforcement database systems to be linked and compatible, allowing for rapid transmission and processing of suspicious activity information across jurisdictions and with the NCRIC.
2.1-E5	Acquire tools to conduct link analysis on suspicious activity reports to determine if a pattern of terrorist pre-operational behavior is occurring in the Bay Area.
2.1-E6	Provide and sustain information technology equipment to include computers, software and hardware for intelligence analysts.

2.1-E7	Sustain Video Teleconferencing Equipment and bridges for multi-site information sharing conferencing.
2.1-E8	Ensure terminals at the NCRIC and key law enforcement and public safety agencies across the region have access to information sharing networks, including federal classified networks where appropriate.
TRAINING	
2.1-T1	Train permanent and assigned analytical staff at the NCRIC on the intelligence cycle and on developing analytic products.
2.1-T2	All applicable training meets International Association of Law Enforcement Analytic Standards from Global Intelligence Working Group and the International Association of Law Enforcement Intelligence Analysts (GIWG/IALEIA) based standards (basic, intermediate, advanced) and such other standards as required.
2.1-T3	NCRIC staff and law enforcement personnel should receive annual awareness training on relevant privacy and security rules, and regulations (28 CFR and any other relevant State statutes and regulations).
2.1-T4	Basic and advanced intelligence analysis training is provided for intelligence operations personnel (e.g., commanders/supervisors, officers, analysts).
2.1-T5	Provide analytic staff at the NCRIC refresher training in analytical methods and practices.
2.1-T6	Personnel are trained in the process for preventing, reporting, and addressing the inappropriate disclosure of information and/or intelligence.
2.1-T7	Provide training to fire service, law enforcement and other public sector agency personnel on identifying and reporting suspicious activity to appropriate authorities.
2.1-T8	Train public and private sector, particularly security personnel at critical infrastructure sites across the Bay Area on the detection and reporting of terrorism pre-attack surveillance and logistical/operational activities against CIKR to the NCRIC.
EXERCISES	
2.1-Ex1	Conduct exercises to test and evaluate surveillance detection capabilities of security personnel at CIKR across the Bay Area.
2.1-Ex2	Conduct exercises to test the NCRIC's ability to analyze, link, and disseminate timely and actionable intelligence to law enforcement and other public safety agencies in the region.
2.1-Ex3	Hold exercises to test alternative, supplemental, and back-up mechanisms for routing information and/or intelligence to the necessary agencies in an emergency.
2.1-Ex4	Conduct exercises to test the process for preventing, reporting, and addressing the inappropriate disclosure of information and/or intelligence.

Objective 2.2 Strengthen Terrorism Attribution, Interdiction and Disruption Capabilities

The Bay Area's law enforcement community (federal, state and local) and other public safety agencies can conduct forensic analysis and attribute terrorist threats and acts to help ensure that suspects involved in terrorist and criminal activities related to homeland security are successfully identified, deterred, detected, disrupted, investigated, and apprehended.

Objective 2.2 Implementation Steps and Resource Elements

PLANNING	
2.2-P1	Develop a plan and procedures to ensure law enforcement investigators across the region receive timely threat and intelligence information from the NCRIC.
2.2-P2	Law enforcement agencies across the region have a systematic process for contacting the local JTTF when a connection to terrorism is discovered during a local criminal investigation.
2.2-P3	Ensure local, state and federal law enforcement agencies use investigative information to help the NCRIC identify potential CIKR terrorism targets.
2.2-P4	Ensure law enforcement tactical teams and HazMat response teams within each Operational Area have standard operating procedures for tactical team and HazMat team integration for critical incidents involving hazardous materials.
ORGANIZATION	
2.2-O1	All local law enforcement agencies in the region should either maintain, or have access to, special operations teams compliant with the NIMS resource types (e.g., SWAT teams) capable of interdicting and disrupting terrorist and major criminal threats.
2.2-O2	Larger jurisdictions or entities should each identify a designated liaison with the JTTF.
2.2-O3	Ensure staffing within the NCRIC is in place for the coordination of the region's interoperable law enforcement information management and sharing system(s).
EQUIPMENT	
2.2-E1	Continue to deploy interoperable law enforcement information management and sharing system across all Bay Area justice agencies to include procurement of software and computer systems, hardware and peripherals.
2.2-E2	At least one law enforcement tactical team in each planning hub has Level 1 protective ensemble models and elements that allow for the tactical team to operate in a CBRN environment.
TRAINING	
2.2-T1	Provide training for patrol officers on terrorism awareness, and protocols for passing criminal investigative information to the NCRIC and the JTTF.
2.2-T2	Train law enforcement personnel to use investigative information to identify potential vulnerabilities/target lists with the NCRIC.
2.2-T3	Provide computer-based and classroom training to TLOs, intelligence analysts, police investigators and other public safety personnel on the use of Bay Area interoperable law enforcement records management and information sharing systems.

2.2-T4	Provide training to law enforcement personnel on the use of tactical intelligence (maps, blueprints, etc.) prior to tactical level interdiction and disruption operations.
2.2-T5	Enhance and provide hostage rescue training to law enforcement.
2.2-T6	Access FEMA sponsored courses in evidence collection at WMD/HazMat and CBRNE incident sites to include Crime Scene Management for CBRNE Incidents.
2.2-T7	Provide appropriate fire service personnel training on arson investigations to include the Fire/Arson Origin and Cause Investigation (R206) and the Principles of Fire Protection: Structures and Systems (R222) courses.
2.2-T8	Provide law enforcement tactical teams training in properly "stacking" and clearing rooms and clearing other the potential threat areas during a tactical emergency response.
2.2-T9	Provide law enforcement tactical teams training on forms of cover/concealment and open area movement tactics.
2.2-T10	Provide training to law enforcement personnel on the use of tactical intelligence (maps, blueprints, etc.) prior to tactical level interdiction and disruption operations.
EXERCISES	
2.2-Ex1	Ensure UASI exercise program incorporates terrorism attribution, interdiction and disruption capabilities into appropriate regional exercises.
2.2-Ex2	NCRIC staff should participate in regional counter terrorism exercises to test its ability to support law enforcement interdiction operations.

Objective 2.3 Increase Critical Infrastructure Protection

The Bay Area can assess the risk to the region's physical and cyber critical infrastructure and key resources from acts of terrorism, crime, and natural hazards and deploy a suite of actions to enhance protection and reduce the risk to the region's critical infrastructure and key resources from all hazards. This includes a risk-assessment process and tools for identifying, assessing, cataloging, and prioritizing physical and cyber assets from across the region.

Objective 2.3 Implementation Steps and Resource Elements

PLANNING	
2.3-P1	Develop a methodology to prioritize CIKR at the regional, sub-regional and jurisdictional level.
2.3-P2	Identify and catalogue by NIPP sector and sub-sector all high risk CIKR present at the regional, sub-regional and jurisdictional level in a secure web-based system.
2.3-P3	Ensure all high risk CIKR at the regional, sub-regional and jurisdictional level undergoes a site vulnerability assessment.
2.3-P4	Within the NCRIC, develop a plan to collect, analyze and map suspicious activity reports against CIKR that may be indicators of terrorist pre-attack surveillance.
2.3-P5	Fully integrate mass transit and maritime ports across the Bay Area region into the security planning and communication and notification process at the NCRIC and the Bay Area UASI.

60

2.3-P6	Work with the private sector and other owners and operators of high risk CIKR to encourage their developing COOPs.
2.3-P7	Evaluate the methods of conducting a potential study of interdependencies of CIKR in the Bay Area.
ORGANIZATION	
2.3-O1	Develop and utilize sector coordinating council(s) for high risk infrastructure in the Bay Area.
2.3-O2	Ensure the NCRIC has CIKR protection analysts that fully integrate the intelligence/prevention and protection missions.
EQUIPMENT	
2.3-E1	Acquire devices that utilize biometric characteristics (fingerprints, palm prints, retinal scanning, etc.) to authorize access to CIKR facilities and/or systems.
2.3-E2	Acquire Geospatial/Geographical Information Systems including application software as well as integrated hardware for implementation.
2.3-E3	Deploy physical security enhancement equipment to high risk CIKR.
2.3-E4	Deploy CBRNE detection equipment in and around high risk CIKR across the Bay Area.
TRAINING	
2.3-T1	Develop and implement risk and vulnerability assessment training at the NCRIC and jurisdictional level.
EXERCISES	
2.3-Ex1	Develop and conduct exercise programs to test CIKR protection plans to include CIKR protection measures and technology across the Bay Area to evaluate the effectiveness of protection capabilities.

Objective 2.4 Enhance Cyber Security

Cyber security programs at the County and major city level meet the Federal Information Processing Standards 200 - Minimum Security Requirements for Federal Information and Information Systems. The region and its jurisdictions can detect malicious cyber activity, conduct technical counter-measures against existing and emerging cyber-based threats, and quickly recover from cyber-attacks in order to ensure the security, reliability, integrity, and availability of its electronic systems and services.

Objective 2.4 Implementation Steps and Resource Elements

PLANNING	
2.4-P1	Ensure every county and major city has conducted an up-to-date cyber risk and vulnerability assessment and developed a written cyber security policy that addresses the purpose of its cyber security program, the scope of the cyber security program, and the roles and responsibilities of agencies and personnel.
2.4-P2	Ensure every county and major city has a cyber contingency/incident response plan aligned with its EOP.

2.4-P3	Ensure every county and major city has an Information Technology Service Continuity Plan that sets both post incident Recovery Time Objectives and the Recovery Point Objectives for any potentially affected essential government data.
2.4-P4	Develop a blue-print, budget and plan for a regional cyber incident response team to be housed in the NCRIC or other regional body.
ORGANIZATION	
2.4-O1	Develop a regional cyber preparedness focus group to develop regional priorities, share best practices, and develop regional cyber based projects.
2.4-O2	Develop cyber security analytic capabilities in the NCRIC to include, cyber information collection, cyber defense, cyber information sharing and cyber intelligence analysis so as to better process and respond to cyber incidents, cyber threat indicators, indicators of compromise, and cyber reporting.
2.4-O3	Develop a technical assistance program in the NCRIC to support operational areas in the conduct of risk and vulnerability assessments.
EQUIPMENT	
2.4-E1	
TRAINING	
2.4-T1	Ensure that each county and major city requires employees (new and existing) to successfully complete cyber security awareness level training (e.g., Information Security for Everyone (AWR175 or equivalent) or briefings on an annual basis. Training could be computer based.
2.4-T2	Bring the emergency management community into the cyber realm by having county and major city EOC managers successfully complete training on the EOC's Role in Community Cyber Security MGT384 (or equivalent), and the Role of the EOC in Cyber Incident Response.
2.4-T3	Provide county and major city law enforcement training on Cyber Investigators Training Level One, Cyber Security Essentials for Law Enforcement, and Prosecuting Cyber Crime.
2.4-T4	Each county and major city's IT staff has successfully completed Cyber Incident Analysis & Response (AWR169 or equivalent course) and the Importance of SCADA System Defense.
2.4-T5	Develop and implement a comprehensive Process Control/Supervisory Control and Data Acquisition (SCADA) cyber security awareness, education, and training program for the owners/operators of public sector SCADA-controlled CIKR within the Bay Area.
EXERCISES	
2.4-Ex1	

SECTION 6 GOALS AND OBJECTIVES

GOAL 3	Mission Area(s)	National Priorities	Core Capabilities	State Strategy
ENHANCE COMMUNICATIONS CAPABILITIES	Response	Strengthen Interoperable and Operable Communications Implement the NIMS/NRF Enhance Regional Collaboration	Operational Communications	Goal 3: Strengthen Communications Capabilities

The National Emergency Communications Plan (NECP)

Produced in 2007, DHS's *National Emergency Communications Plan (NECP)* establishes a comprehensive national vision for the future state of emergency communications. The desired future state is that emergency responders can communicate: as needed, on demand, and as authorized; at all levels of government; across all disciplines.

The *NECP* established three strategic goals:

- **Goal 1:** By 2010, 90 percent of all high-risk urban areas designated within the Urban Areas Security Initiative (UASI) are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.

- **Goal 2:** By 2011, 75 percent of non-UASI jurisdictions are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.

- **Goal 3:** By 2013, 75 percent of all jurisdictions are able to demonstrate response-level emergency communications within three hours.

In 2010, according to the DHS Office of Emergency Communications, which oversees the NECP and conducted assessments of 60 Urban Areas, Goal 1 has been met. The Bay Area successfully participated in the 2010 national assessment.

Bay Area Regional Interoperable Communications System

The Bay Area is currently deploying a region-wide, standards-based, communication "system of systems" that supports first responder communication needs for local and regional agencies and interoperates with state and federal public safety agencies and designated public service organizations operating within the Bay Area region. The Bay Area will accomplish this by implementing its 2008 strategic plan for achieving interoperable communications and by

coordinating its efforts with the goals and objectives of the California Statewide Communications Interoperability Plan (CalSCIP).

BayComm is the region's 700MHz Project 25 (P25) "system of systems" voice initiative. In the past, the Bay Area agencies have traditionally used disparate frequency and antiquated legacy analog systems. Interoperability required cache radios and gateways for agencies to team together effectively during multi-jurisdictional events and disasters. The BayComm seeks to alleviate these issues by providing Bay Area first responders with a common frequency band and a common open digital standard in P25.

In August 2011, the region established the Bay Area Regional Interoperable Communications System (BayRICS) Authority, a joint powers authority charged with governance and oversight of the Bay Area Enhanced Wireless Broadband (BayWEB), a regional broadband network designed to serve as a platform for fully interoperable voice, data and video communications throughout the region.

Objective 3.1: Enhance Operational Communications Capabilities

The emergency response community in the Bay Area has the ability to provide a continuous flow of mission critical voice, data and imagery/video information among multi-jurisdictional and multidisciplinary emergency responders, command posts, agencies, and Bay Area governmental officials for the duration of an emergency response operation. The Bay Area can also re-establish sufficient communications infrastructure within the affected areas of an incident, whatever the cause, to support ongoing life-sustaining activities, provide basic human needs, and transition to recovery.

Objective 3.1 Implementation Steps and Resource Elements

PLANNING	
3.1-P1	Complete an interagency communication process baseline report for each agency, operational area and sub-region that defines processes required to achieve interoperable communications within and between agencies.
3.1-P2	Reassess each Operational Area's current level of ability in the interoperable voice communications area to determine how the Bay Area region should move forward in planning and investing.
3.1-P3	Ensure all Tactical Interoperable Communications Plans (TICPs) in the region are fully up to date. Evaluate the possibility of developing a repository of all Bay Area TICPs for easy access for public safety policy makers.
3.1-P4	Ensure after action plans are developed and reviewed at the county/operational area and/or sub-regional and regional level to evaluate the effectiveness of communications mobilization and demobilization activities.
3.1-P5	Coordinate with and support BayRICS Authority efforts to integrate broadband data and video communications into regional interoperable communications plan.
3.1-P6	Develop COOPs that ensure continued operation of local and regional public safety communications nets during an incident response.
3.1-P7	Ensure incident commanders and first responders have awareness of primary and

	secondary systems and peripheral equipment for interoperable emergency communications.
ORGANIZATION	
3.1-O1	Provide limited initial funding for a Bay Area Regional Communications Coordinator position within the region to provide administrative support and to facilitate the regional approach to Interoperable Communications with an emphasis on mission critical voice communication while laying the ground work for future data communications. This person will liaison with the surrounding regions (CAP-BAY) and the State of California on technical issues as necessary.
3.1-O2	Ensure local incident commanders and first responders have awareness of primary and secondary systems and peripheral equipment for interoperable emergency communications.
EQUIPMENT	
3.1-E1	Manage, enhance and sustain the digital microwave network and other high speed data transport networks to support interoperability efforts in the Bay Area to link the various interoperability projects across the Bay Area to include redundant systems such as BayLoop.
3.1-E2	Develop a regional fiber optic backhaul network and transition regional interoperable communications infrastructure from microwave to fiber technology.
3.1-E3	Enhance BayWEB coverage through additional communications equipment or backhaul to improve coverage and performance in areas that demonstrate significant need.
3.1-E4	Acquire back-up equipment to support continuity of communications operations in the event primary communications systems are destroyed.
TRAINING	
3.1-T1	Ensure each county/operational area has at least four people trained as Communications Unit Leaders (COML).
3.1-T2	Provide hybrid training on the interoperability communications protocols, tools and efforts to include data, video and multimedia applications and TICPs so as to ensure that responders are prepared to work in the shared environments.
EXERCISES	
3.1-Ex1	Conduct TICP exercises at Operational Area levels.
3.1-Ex2	Use exercise scenarios that test multi-agency communication for the purpose of validating joint standard operating procedures (SOPs) for emergencies and regional communications SOPs.
3.1-Ex3	Continue to test and evaluate the region's first responders in the use of plain language during appropriate incidents.
3.1-Ex4	Conduct exercises to test and evaluate the ability to use back-up communications equipment.

SECTION 6 GOALS AND OBJECTIVES

GOAL 4	Mission Area(s)	National Priorities	Core Capabilities	State Strategy
STRENGTHEN CBRNE/WMD DETECTION, RESPONSE AND DECONTAMINATION CAPABILITIES	Response	Strengthen CBRNE Detection, Response, and Decontamination Capabilities	Infrastructure Systems On-Scene Security and Protection Public and Private Services Mass Search and Rescue Environmental Response	Goal 5: Strengthen Catastrophic CBRNE and All Hazards Incident Planning, Detection and Response Capabilities

WMD/CBRNE Overview

The National Fire Protection Association (*NFPA) 472: Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents* identifies the minimum levels of competence required by all responders to emergencies involving HazMat and WMD. *NFPA 472* is based on the premise that responders should be trained to perform their expected tasks, and that a responder cannot safely and effectively respond to a terrorism or criminal incident involving HazMat or WMD if they do not first understand basic hazardous materials response.[14] In addition, the standard redefines the awareness level away from "first responders" and to "persons who, in the course of their normal duties, could be the first on the scene of an emergency involving a hazmat/WMD and who are expected to recognize the presence of hazmat/WMD, protect themselves, call for trained personnel, and secure the area."[15]

---

[14] NFPA®Catalog, "Product Detail: NFPA 472: Standard for Competence of Responders to Hazardous Materials/ Weapons of Mass Destruction Incidents, 2008 Edition" (2012), at http://www.nfpa.org/catalog/product.asp?pid=47208.

[15] Gregory G. Noll, FireEngineering®, "NFPA 472: Developing a Competency-Based Hazmat/WMD Emergency Responder Training Program" (April 1, 2008), at http://www.fireengineering.com/articles/print/volume-161/issue-4/features/nfpa-472-developing-a-competency-based-hazmat-wmd-emergency-responder-training-program.html

For Official Use Only   **SECTION 6 GOALS AND OBJECTIVES**

NFPA 473: Standard for Competencies for EMS Personnel Responding to Hazardous Materials/Weapons of Mass Destruction Incidents identifies the levels of competence required of emergency medical services (EMS) personnel who respond to hazardous materials incidents. It specifically covers the requirements for basic and advanced life support personnel in the pre-hospital environment. The Bay Area will strive to adhere to both NFPA standard 472 and 473.

Established in 1998, the National Bomb Squad Commanders Advisory Board (NBSCAB) is an association of bomb squad commanders from around the country. The group provides advice and guidance to federal standard-setting agencies that support bomb squads and serves as the final decision-making authority on guidelines and standards for the public safety bomb squad profession. In coordination with NBSCAB, the FBI provides the standards for bomb squad certification based on formation, training and equipment. Every bomb squad technician attends the FBI's Hazardous Devices School for six weeks of initial training and returns to the school every three years for recertification. Each year there are over 200 hours of refresher training.

Objective 4.1 Improve Public and Private Services and Resources Management through Fire Incident Response Support

Fire service agencies across the Bay Area can dispatch initial fire suppression resources within jurisdictional response time objectives, and firefighting activities are conducted safely with fire hazards contained, controlled, extinguished, and investigated, with the incident managed in accordance with local and state response plans and procedures.

Objective 4.1 Implementation Steps and Resource Elements

PLANNING	
4.1-P1	Develop regional plans, programs, and agreements on fire-related public safety protection activities, including region-wide mutual aid response protocols.
4.1-P2	Develop regional firefighting plans and procedures to address ICS with a particular focus on unified command for multi-agency events and ensure they are integrated with onsite incident management plans.
4.1-P3	Develop regional specialized firefighting plans for CBRNE incidents involving mass transit.
EQUIPMENT	
4.1-E1	Acquire and maintain authorized firefighting equipment as agreed to by the region.
TRAINING	
4.1-T1	Develop and implement training to enable fire rescue and emergency medical services to recognize the presence of CBRNE materials.
4.1-T2	Conduct training in unified command structure and process under NIMS/SEMS/ICS for multi-agency events.
EXERCISES	
4.1-Ex1	Conduct exercises to test and evaluate fire incident response involving multiple agencies to test unified command.

Objective 4.2 Strengthen Mass Search and Rescue Capabilities

Public safety personnel in the Bay Area are able to conduct search and rescue operations to locate and rescue persons in distress and initiate community-based search and rescue support-operations across a geographically dispersed area. The region is able to synchronize the deployment of local, regional, national, and international teams to support search and rescue efforts and transition to recovery.

Objective 4.2 Implementation Steps and Resource Elements

PLANNING	
4.2-P1	Develop plans, protocols and SOPs for local and regional level search and rescue operations involving the most common incidents requiring search and rescue. This should include initial search plans using a column grid layout.
ORGANIZATION	
4.2-O1	Each operational area should continue to integrate EMS into search and rescue teams across the region.
EQUIPMENT	
4.2-E1	Acquire and sustain personal protective equipment for search and rescue teams.
4.2-E2	Acquire and sustain medical equipment for search and rescue teams.
4.2-E3	Acquire and sustain search and rescue watercraft and aviation equipment.
TRAINING	
4.2-T1	Update the Bay Area's search and rescue training mandates.
4.2-T2	Conduct training for search and rescue reconnaissance teams to provide preliminary recommendations on search priorities and strategy within 1 hour of an incident.
4.2-T3	Provide rescue systems 1 and 2 level training with an emphasis on identifying and mitigating the creation of hazards during search and rescue operations.
EXERCISES	
4.2-Ex1	Update the Bay Area's search and rescue exercise mandates.
4.2-Ex2	Test and evaluate search and rescue capabilities in operational area and regional exercises. Regional exercises should focus on the coordination, command and control of multiple search and rescue teams operating in a multi-jurisdictional incident.

Objective 4.3 Enhance Screening Search and Detection Capabilities

The Bay Area has systems and procedures to rapidly detect, locate and identify chemical, biological, radiological, nuclear, and/or explosive (CBRNE) materials at ports of entry, critical infrastructure locations, public events, and incidents, and can communicate CBRNE detection, identification and warning information to appropriate entities and authorities across the state and at the federal level.

Objective 4.3 Implementation Steps and Resource Elements

PLANNING	
4.3-P1	Prepare and apply for Domestic Nuclear Detection Office Securing the Cities grants in order to design and implement architectures in the Bay Area for the coordinated and integrated screening, search, detection and interdiction of radiological/nuclear materials that are out of regulatory control and may be used as a weapon.
4.3-P2	Ensure the region's radiological/nuclear detection plans and protocols are fully integrated with the State's preventive radiological/nuclear detection program.
4.3-P3	Develop intelligence and risk-based CBRNE screening, search and detection deployment protocols for major events, mass transit and other high profile events and CIKR.
4.3-P4	Develop plans and protocols for the NCRIC to notify appropriate personnel of CBRNE screening, search and detection data and results.
4.3-P5	Develop a records management protocol at the NCRIC for all CBRNE issues or alarms and their resolution.
4.3-P6	Develop plans and protocols to acquire and distribute CBRNE screening, search and detection equipment to large numbers of first responders across the region.
4.3-P7	Sustain and update plans and protocols among laboratories across the region for public information regarding CBRNE detection.
ORGANIZATION	
4.3-O1	Ensure laboratories across the region are adequately staffed for agent identification.
EQUIPMENT	
4.3-E1	CBRNE inspection, detection and screening systems equipment for deployment at pre-determined sites across the region such as seaports, airports, major public events, water supply, mass transit, etc.
TRAINING	
4.3-T1	Appropriate personnel have been identified for CBRNE screening, search and detection training (e.g., law enforcement, transit police and security, fire department, hazardous materials (HazMat), public health, private sector security, and critical infrastructure personnel).
4.3-T2	Awareness level training for first responders and CIKR personnel for each of the CBRNE agents.
EXERCISES	

4.3-Ex1	A program to test and evaluate new CBRNE screening, search and detection technology in the appropriate operational environment is made part of the overall exercise and evaluation program.

Objective 4.4 Strengthen On-Scene Security and Protection through Explosive Device Response Operations

Public safety bomb squads in the Bay Area are able to conduct threat assessments; render safe explosives and/or hazardous devices; and clear an area of explosive hazards in a safe, timely, and effective manner. This involves the following steps in priority order: ensure public safety; safeguard the officers on the scene (including the bomb technician); collect and preserve evidence; protect and preserve public and private property; and restore public services.

Objective 4.4 Implementation Steps and Resource Elements

PLANNING	
4.4-P1	Engage the DHS Office of Bombing Prevention for the purpose of conducting a Multi-Jurisdictional Improvised Explosive Device Security Planning assessment.
4.4-P2	Develop and sustain plans, tactics, techniques, and procedures to respond to vehicle borne improvised explosive devices among regional bomb squads.
4.4-P3	Develop and sustain plans, tactics, techniques, and procedures to respond to radio-controlled, improvised explosive devices among regional bomb squads.
4.4-P4	Develop and sustain plans, tactics, techniques, and procedures to respond to suicide bombers among regional bomb squads.
4.4-P5	Using a risk-based approach, evaluate those high-risk or particularly vulnerable locations in the Bay Area that might be beyond a 1-hour response time frame, and assess the potential for acquiring and pre-deploying additional explosive device response equipment to help meet the 1-hour time response frame.
ORGANIZATION	
4.4-O1	Ensure all bomb squads in the Bay Area are accredited by the FBI to standards set by the National Bomb Squad Commanders Advisory Board
4.4-O2	Ensure full use of the DHS Office of Bombing Prevention information-sharing portal, the Technical Resource for Incident Prevention (TRIPwire), and the ATF's clearing house (Bomb Arson Tracking System (BATS).
EQUIPMENT	
4.4-E1	Ensure all bomb squad personnel have appropriate personal protective equipment, e.g., ballistic vests and helmets with shields, for use during hand entry operations.
4.4-E2	Acquire and sustain necessary electronic counter measures and other EDRO equipment.
4.4-E3	Based on assessment results (4.4-P5), acquire, pre-deploy and sustain necessary explosive device response equipment for high-risk sites outside a 1-hour response time frame.

SECTION 6 GOALS AND OBJECTIVES

TRAINING	
4.4-T1	Provide training to bomb squad personnel on locating and neutralizing secondary devices and booby traps.
4.4-T2	Ensure all bomb squad training (including techniques, tactics, and procedures) is consistent with and enhances training delivered by the FBI Hazardous Devices School.
4.4-T3	Deliver training for responding to radio controlled improvised explosive devices.
4.4-T4	Deliver training for responding to suicide bombers.
4.4-T5	Deliver training for responding to vehicle borne improvised explosive devices.
4.4-T6	Provide general public and private sector personnel with bomb threat awareness training as needed.
4.4-T7	Ensure that all necessary law enforcement personnel are provided sufficient support and opportunities for continuing/refresher education and explosive device response training.
EXERCISES	
4.4-Ex1	Ensure explosive device response operations, to include responding to a VBIED, IED, waterborne IED and other scenarios are incorporated into exercise programs.

Objective 4.5 Enhance Environmental Response/Health and Safety through WMD/HazMat Response and Decontamination Capabilities

Responders in the Bay Area are able to conduct health and safety hazard assessments and disseminate guidance and resources, including deploying HazMat response and decontamination teams, to support immediate environmental health and safety operations in the affected area(s) following a WMD or HazMat incident. Responders are also able to assess, monitor, clean up, and provide resources necessary to transition from immediate response to sustained response and short-term recovery.

Objective 4.5 Implementation Steps and Resource Elements

PLANNING	
4.5-P1	Develop maintenance and safety plans for regional equipment caches used by multiple EMD/HazMat teams in the region.
4.5-P2	Develop SOPs for integration of fire personnel and law enforcement tactical teams.
4.5-P3	Ensure fire service has plans and procedures in place to decontaminate equipment and resources during a WMD/HazMat response.
4.5-P4	Ensure plans and procedures are in place to decontaminate deceased bodies during a WMD/HazMat response.
4.5-P5	Integrate the private sector into hazardous materials clean-up/recovery plans.
ORGANIZATION	
4.5-O1	Pre-identify resources (personnel and equipment) to provide rapid initial size-

	up of hazardous materials incident.
EQUIPMENT	
4.5-E1	Acquire equipment for WMD/HazMat teams using CalEMA, FIRESCOPE HazMat Team Standardized Equipment List and the Bay Area CBRNE Plan as guidelines.
4.5-E2	Acquire tools that may be used predominantly in the field by WMD/HazMat teams to generate effective plume modeling.
TRAINING	
4.5-T1	Ensure that all appropriate personnel are trained to NFPA 472 standard and provide refresher training as needed.
4.5-T2	Ensure that all appropriate personnel are trained to NFPA 473 standard and provide refresher training as needed.
4.5-T3	Ensure hazmat team(s) trains regularly with EMS to ensure proper coordination of victim care post-decontamination (identification of substance, administration of antidotes, etc.).
4.5-T4	Develop and implement training related to detection, identification and reporting of hazardous material.
4.5-T5	Provide training to WMD/HazMat teams on the use of plume modeling tools to improve response time and effectiveness in plume modeling.
4.5-T6	Conduct training for integration of fire personnel and law enforcement tactical team response operations.
4.5-T7	Conduct training for fire service on procedures to decontaminate equipment and resources during a WMD/HazMat response.
4.5-T8	Provide WMD/HazMat response and mitigation training to law enforcement personnel as needed.
4.5-T9	Conduct joint public and private sector training on the transition from response to recovery and clean up following a WMD/HazMat incident.
4.5-T10	Training for WMD/HazMat teams on proper use and understanding of the radioactive detection methods and equipment currently in use.
4.5-T11	Train Radiation Safety Officers for Type 1 teams to oversee the radiation equipment and standardize the radiation training each team as well as other mutual aid hazmat technicians.
EXERCISES	
4.5-Ex1	Test and evaluate the use of plume modeling tools to measure improvements in response time and effectiveness in plume modeling.
4.5-Ex2	Exercise CBRNE/WMD/HazMat capabilities and equipment into regional and statewide exercise opportunities.

Objective 4.6 Improve Environmental Response/Health and Safety through Responder Safety and Health

The Bay Area can reduce the risk of illnesses or injury to first responders, first receivers, medical facility staff members, or other skilled support personnel as a result of preventable exposure to secondary trauma, chemical/radiological release, infectious disease, or physical/emotional stress after the initial incident or during decontamination and incident follow-up.

Objective 4.6 Implementation Steps and Resource Elements

PLANNING	
4.6-P1	Develop and adopt agency/jurisdiction safety and health plans and program(s).
4.6-P2	Conduct a detailed analysis of relevant planning scenarios to ensure that all workers are protected while performing tasks from all hazards.
ORGANIZATION	
4.6-O1	Establish plans and procedures for identifying sources of additional equipment and expertise if the safety and health program is overwhelmed.
EQUIPMENT	
4.6-E1	Acquire and sustain authorized personal protective equipment as agreed to by the region to include SCBA, auto injectors, etc.
TRAINING	
4.6-T1	Provide training on acquired PPE.
EXERCISES	
4.6-Ex1	Integrate responder health and safety into exercises to develop and maintain appropriate health and safety knowledge and expertise for responders.

Objective 4.7 Enhance On-Scene Security and Protection through Emergency Public Safety and Security Response

Public safety agencies within the Bay Area are able to keep the public and critical infrastructure safe by securing a particular incident scene and maintaining law and order following an incident or emergency to include managing the criminal justice prisoner population.

Objective 4.7 Implementation Steps and Resource Elements

PLANNING	
4.7-P1	Develop plans and procedures for a Type 1 regional mobile field force (MFF) under NIMS to support emergency public safety and security.
4.7-P2	Develop plans and systems to maintain accountability of public safety personnel, track incident locations, and track resources.
4.7-P3	Develop activation and deployment plans for public safety and security with plans targeting 50 percent of total uniformed (patrol) staff of a jurisdiction having primary responsibility for the incident.
4.7-P4	Develop plans and protocols for alternate facilities for court services, prisoner holding and housing, prisoner transport, criminal intake and other criminal

	justice services.
4.7-P5	Ensure plans for sheltering, housing, and feeding law enforcement and other public safety personnel are in place
ORGANIZATION	
4.7-O1	Ensure MFF meets NIMS type 1 standards to include a tactical team (platoon) to include four 12-person squads and an officer in charge (OIC) and a Deputy OIC. Each squad should include a supervisor.
EQUIPMENT	
4.7-E1	Acquire and sustain MFF equipment to include protective clothing, soft body armor (helmet and face shield, gloves, shin guards), communications equipment, personal hydration, riot control gear, video equipment, mass arrest kits, and other necessary equipment.
4.7-E2	Acquire and sustain power and traffic control equipment.
TRAINING	
4.7-T1	Provide training to MFF to include, crowd control, traffic management, on-site security, etc.
4.7-T2	Develop and conduct public safety and security training programs to include joint local, state and federal teams pursuant to ESF 13 under the NRF.
EXERCISES	
4.7-Ex1	Test and evaluate MFF and such other public safety and security teams' activation and deployment capabilities.
4.7-Ex2	Test and evaluate criminal justice re-location plans.

GOAL 5	Mission Area(s)	National Priorities	Public Health and Target Capabilities	State Strategy
ENHANCE MEDICAL AND PUBLIC HEALTH PREPAREDNESS	Protection Response Recovery	Strengthen Medical Surge and Mass Prophylaxis Capabilities	Emergency Triage and Pre-Hospital Treatment Medical Surge Medical Countermeasure Dispensing Medical Materiel Management and Distribution Non-Pharmaceutical Interventions Laboratory Testing Public Health surveillance and Epidemiological Investigation Fatality Management	Goal 6: Improve Medical and Health Preparedness

Public Health and Medical Background

Health and medical preparedness is a fundamental component of homeland security. This fact is evidenced by the 2001 anthrax attacks, the outbreak of Severe Acute Respiratory Syndrome (SARS), and the 2009 H1N1 influenza outbreak. Given such risks, the Bay Area must ensure its medical and public health infrastructure is capable of protecting against, responding to, and recovering from such events.

At the National level, the Department of Health and Human Services has led the way with the creation of the National Health Security Strategy (NHSS), released in December 2009. The NHSS is designed to achieve two overarching goals:

- Build community resilience, and
- Strengthen and sustain health and emergency response systems.

As with the *Bay Area Homeland Security Strategy*, the NHSS is designed around building health and medical capabilities in order to achieve strategic goals and objectives based on the elements

For Official Use Only   **SECTION 6 GOALS AND OBJECTIVES**

of plans, organization, equipment, training, and exercises. As the Federal Government continues to develop implementation plans for the NHSS, the Bay Area will track federal guidance and integrate, where appropriate, such guidance into local and regional health and medical preparedness efforts.

In enhancing medical and public health preparedness, the Bay Area seeks to develop a comprehensive and integrated system of first responders, hospitals, clinics, and public health departments across the region. This includes fully integrating the Metropolitan Medical Response System (MMRS) in the Bay Area.

Finally, the region's CBRNE plan also plays a critical role relative to this strategic goal as several objectives within the plan cover medical and health preparedness concerning a CBRNE event. Jurisdictions and sub-regions should therefore, look to the CBRNE plan for additional guidance in this area.

Objective 5.1 Enhance Emergency Triage and Pre-Hospital Treatment

Emergency medical services (EMS) resources across the Bay Area can effectively and appropriately be dispatched (including with law enforcement tactical teams) to provide pre-hospital triage, treatment, transport, tracking of patients, and documentation of care appropriate for the incident, while maintaining the capabilities of the EMS system for continued operations up to and including for mass casualty incidents.

Objective 5.1 Implementation Steps and Resource Elements

PLANNING	
5.1-P1	Update local mass casualty plans and integrate local plans with the California Disaster Medical Operations Manual.
5.1-P2	Produce written plans and procedures for coordination of the local EMS system with the State and National Disaster Medical System (NDMS).
5.1-P3	Develop protocols and procedures for tracking triage and pre-hospital treatment response staff and equipment during day-to-day operations, as well as catastrophic incidents.
EQUIPMENT	
5.1-E1	Acquire and sustain emergency medical equipment to include patient tracking systems and PPE.
TRAINING	
5.1-T1	Provide training on the California Public Health and Medical Emergency Operations Manual.
5.1-T2	Develop and implement multi-disciplinary training programs for EMS personnel, based on local risk vulnerability assessments and lessons learned.
5.1-T3	Conduct training for EMS and tactical team personnel in joint response events.
5.1-T4	Conduct training for dispatch personnel in protocols and procedures for dispatch during catastrophic events.
5.1-T5	Provide the Tactical Emergency Casualty Care Course to EMS personnel.

EXERCISES	
5.1-Ex1	Develop and implement multi-disciplinary exercises to test and evaluate the ability of EMS agencies to move and track large numbers of patients during a multi-jurisdictional incident consistent with the California Disaster Medical Operations Manual.
5.1-Ex2	Conduct joint EMS and law enforcement tactical team exercises to test and evaluate the ability to operate jointly in a warm zone.

Objective 5.2 Increase Medical Surge

The Bay Area is able to provide adequate medical evaluation and care during incidents that exceed the limits of the normal medical infrastructure of an affected community or the region. The healthcare system in the region is able to survive a hazard impact and maintain or rapidly recover operations that were compromised. Those injured or ill from a medical disaster and/or mass casualty event in the Bay Area are rapidly and appropriately cared for. Continuity of care is maintained for non-incident related illness or injury.

Objective 5.2 Implementation Steps and Resource Elements

PLANNING	
5.2-P1	Develop and maintain medical surge plans that integrate with State and hospital plans including patient distribution plans.
5.2-P2	Develop and maintain medical mutual aid agreements for medical facilities and equipment.
5.2-P3	Develop and maintain surge capacity plans for acute care hospitals.
5.2-P4	Update local mass casualty plans and integrate local plans with the California Disaster Health Operations Manual.
EQUIPMENT	
5.2-E1	Acquire and sustain medical equipment, supplies and pharmaceuticals to support medical surge operations.
TRAINING	
5.2-T1	Provide training on the California Public Health and Medical Emergency Operations Manual.
5.2-T2	Provide training on the California Healthcare Surge Standards and Guidelines for healthcare facilities.
EXERCISES	
5.2-Ex1	Test and evaluate medical surge plans.

SECTION 6 GOALS AND OBJECTIVES

Objective 5.3 Strengthen Medical Countermeasure Dispensing

With the onset of an incident, the Bay Area is able to provide appropriate medical countermeasures (including vaccines, antiviral drugs, antibiotics, antitoxin, etc.) in support of treatment or prophylaxis (oral or vaccination) to the identified population in accordance with local, state and federal public health guidelines and/or recommendations.

Objective 5.3 Implementation Steps and Resource Elements

PLANNING	
5.3-P1	Develop and maintain plans, procedures, and protocols for medical countermeasure dispensing.
5.3-P2	Develop procedures for obtaining medical countermeasure dispensing supplies from the receipt, staging, and storage (RSS) sites in coordination with the Medical Supplies and Distribution Capability.
5.3-P3	Develop programs to ensure security of medical countermeasure dispensing during dispensing operations.
5.3-P4	Develop processes to ensure that first responders, public health responses, critical infrastructure personnel, and their families receive prophylaxis prior to POD opening.
ORGANIZATION	
5.3-O1	Develop a medical countermeasure dispensing inventory management system.
EQUIPMENT	
5.3-E1	Caches of medical supplies and strategic national stockpile (SNS) dispensing and distribution equipment.
TRAINING	
5.3-T1	Develop and implement training for medical countermeasure dispensing operations.
5.3-T2	Develop and implement training for medical countermeasure dispensing repacking, distribution, and dispensing, security of mass prophylaxis, and for mass prophylaxis inventory management.
EXERCISES	
5.3-Ex1	Conduct medical countermeasure dispensing exercises to test and evaluate all aspects of medical countermeasure dispensing, including distribution and dispensing, tactical communications, public information and communication, security, inventory management, and distribution.

Objective 5.4 Improve Medical Materiel Management and Distribution

The Bay Area is able to acquire, maintain (e.g., cold chain storage or other storage protocol), transport, distribute, and track medical materiel (e.g., pharmaceuticals, gloves, masks, and ventilators) during an incident and recover and account for unused medical materiel, as necessary, after an incident.

Objective 5.4 Implementation Steps and Resource Elements

PLANNING	
5.4-P1	Develop plans for establishing staging areas for internal and external medical response personnel, equipment, and supplies.
5.4-P2	Establish strategies for transporting materials through restricted areas, quarantine lines, law enforcement checkpoints and so forth that are agreed upon by all affected parties.
5.4-P3	Obtain demographic/health-related data to plan for the types of medications, durable medical equipment, or consumable medical supplies that may need to be provided during an event (including supplies needed for populations requiring functional or medical care).
TRAINING	
5.4-T1	Provide training on the demobilization of medical supplies.
5.4-T2	Provide training in medical supplies management and distribution in the pre hospital triage environment.
5.4-T3	Provide training on CDC supply tracking software.
EXERCISES	
5.4-Ex1	Exercise plans procedures and systems for transporting and tracking medical material assets with specific focus on the demobilization of medical supplies.

Objective 5.5 Strengthen Non-Pharmaceutical Interventions

Public health agencies in the Bay Area are able to recommend to the applicable lead agency (if not public health) and implement, if applicable, strategies for disease, injury, and exposure control. Strategies include the following: isolation and quarantine, restrictions on movement and travel advisory/warnings, social distancing, external decontamination, hygiene, and precautionary protective behaviors. Legal authority for those applicable measures is clearly defined and communicated to all responding agencies and the public. Logistical support is provided to maintain measures until danger of contagion has elapsed.

Objective 5.5 Implementation Steps and Resource Elements

PLANNING	
5.5-P1	Ensure legal authority is in place for authorizing isolation and quarantine.
5.5-P2	Develop and maintain plans for coordinating quarantine activation and enforcement with public safety and law enforcement.

79

ORGANIZATION	
5.5-O1	Establish systems, programs, and resources for implementing isolation and quarantine.
TRAINING	
5.5-T1	Develop and implement exercises for isolation and quarantine.
EXERCISES	
5.5-Ex1	Exercises to test plans for implementing isolation and quarantine.

Objective 5.6 Improve Laboratory Testing

Laboratories in the Bay Area are able to conduct rapid and conventional detection, characterization, confirmatory testing, data reporting, investigative support, and laboratory networking to address actual or potential exposure to all-hazards. Confirmed cases and laboratory results are reported immediately to all relevant public health, food regulatory, environmental regulatory, and law enforcement agencies in support of operations and investigations.

Objective 5.6 Implementation Steps and Resource Elements

ORGANIZATION	
5.6-P1	Identify, establish and maintain working collaboration with all Laboratory Response Network (LRN) Sentinel and LRN Clinical Chemistry laboratories.
5.6-P2	Develop and maintain an accurate and current database of contact information and capability for all the Laboratory Response Network (LRN) Sentinel and LRN Clinical Chemistry laboratories.
EQUIPMENT	
5.6-E1	Laboratory equipment to test and evaluate CBRNE agents.
TRAINING	
5.6-T1	Train all LRN Sentinel laboratories in the use of LRN biological agent ruled-out protocols, specimens or isolate referral responsibilities and notification algorithms.
EXERCISES	
5.6-Ex1	Exercises to test select LRN sentinel and LRN clinical chemistry laboratories

Objective 5.7 Strengthen Public Health Surveillance and Epidemiological Investigation

Bay Area public health agencies have the ability to create, maintain, support, and strengthen routine surveillance and detection systems and epidemiological investigation processes, as well as to expand these systems and processes in response to incidents of public health significance. This includes the ability to identify potential exposure to disease, mode of transmission, and agent.

Objective 5.7 Implementation Steps and Resource Elements

PLANNING	
5.7-P1	Develop plans, procedures, and protocols for investigating a potential disease outbreak.
5.7-P2	Develop and maintain procedures for identification of disease, vector and epidemic.
TRAINING	
5.7-T1	Training for staff on activities required to conduct epidemiological surveillance and detection including exposure and disease detection, surveillance, analysis, reporting, and use of equipment.
EXERCISES	
5.7-Ex1	Exercises to evaluate epidemiological surveillance and detection.

Objective 5.8 Enhance Fatality Management

Bay Area agencies, e.g., law enforcement, public health, healthcare, emergency management, and medical examiner/coroner) are able to coordinate (to ensure the proper recovery, handling, identification, transportation, tracking, storage, and disposal of human remains and personal effects; certify cause of death; and facilitate access to mental/ behavioral health services to the family members, responders, and survivors of an incident.

Objective 5.8 Implementation Steps and Resource Elements

PLANNING	
5.8-P1	Ensure plans are in place to allow for the contracting or use of private sector resources in support of mass fatality to include the use of just in time contracts for body storage, etc.
EQUIPMENT	
5.8-E1	Acquire and sustain mass fatality equipment as called for in the Bay Area Regional Catastrophic Incident Mass Fatality Plan.
5.8-E2	Acquire authorized and needed body storage equipment as agreed to by the region.
TRAINING	
5.8-T1	Provide training on the implementation of the Bay Area Regional Catastrophic Incident Mass Fatality Plan.
5.8-T2	Conduct training on mass fatality equipment.
EXERCISES	
5.8-Ex1	Conduct exercises to test and evaluate the Bay Area Regional Catastrophic Incident Mass Fatality Plan across all phases – trauma, contamination and pandemic.

GOAL 6	Mission Area(s)	National Priorities	Core Capabilities	State Strategy
STRENGTHEN EMERGENCY PLANNING AND CITIZEN PREPAREDNESS CAPABILITIES	Response Recovery	Strengthen Planning and Citizen Preparedness Capabilities	Community Resilience Public Information and Warning Operational Coordination Situational Assessment Critical Transportation Public and Private Resources Mass Care Services	Goal 4: Enhance Planning and Community Preparedness Capabilities

Community Resiliency

The Bay Area has long viewed emergency and community planning and preparedness as a core element of homeland security. In 2007-2008 the region developed a community preparedness program guide to help identify local best practices concerning social marketing programs as they relate to community preparedness, determine national best practices for citizen preparedness programs, and assess the effectiveness of the various characteristics of community preparedness programs available in the Bay Area. The program guide is a valuable tool to assist the region, sub-regions and jurisdictions in their development of community preparedness programs for all hazards. The program guide also serves as a key element and implementation tool for each of the objectives under this Strategic goal.

Effectively communicating threat or disaster risk, warnings, protective actions, and other information to the community continues to gain prominence as a critical element of keeping communities safe before, during, and after disasters. While researchers and practitioners have made significant strides towards identifying risks and establishing new technology protocols and solutions, the challenge of communicating alerts, warnings, and protective actions across multiple independent jurisdictions with a widely diverse population such as those in the Bay Area still needs to be addressed within the region.

In 2012, the Bay Area developed a comprehensive emergency public information and warning assessment and strategic plan. That plan provides the overall blueprint for how the region can strengthen its emergency public information and warning capability. The *Bay Area Homeland*

Security Strategy tracks and reinforces what the emergency public information and warning strategic plan consists of in more detail.

Coordination of Emergency Operations

An emergency operations center (EOC) is a location from which centralized strategic management of an incident is performed. The EOC is a coordination point, not an incident scene command, control and management center; it does not provide tactical direction to field activities. The EOC may manage multiple incidents that have established incident command posts. The EOC coordinates the delivery of resources to address conditions facing field resources, communicates with the next highest level of level of government to provide information regarding the emergency and the acquisition of resources not readily available within the requesting level of government.

There are numerous EOCs in the Bay Area. Each operational area in the region has an EOC as do several major cities, including the cities of Oakland and San Jose. When activated, an operational area EOC will coordinate mutual aid requests between the county, the operational area member jurisdictions, and the State Regional Emergency Operations Center (REOC). EOCs in the region operate under the SEMS, the NIMS based system for emergency management and its five essential functions: Command or Management, Operations, Planning, Logistics and Finance.

Objective 6.1 Strengthen Emergency Public Information and Warning Capabilities

The Bay Area has an interoperable and standards-based system of multiple emergency public information and warning systems that allows Bay Area leaders and public health and safety personnel to disseminate prompt, clear, specific, accurate, and actionable emergency public information and warnings to all affected members of the community in order to save lives and property concerning known threats or hazards.

Objective 6.1 Implementation Steps and Resource Elements

PLANNING	
6.1-P1	Develop a process for joint regional procurement of future emergency public information and warning tools and for sustaining current emergency public information and warning capabilities. Ensure all equipment purchases are compliant with the Common Alerting Protocol (CAP).
6.1-P2	Review and update Operational Area databases of partner community based organizations and advocacy groups for populations with access and functional needs and/or limited English proficiency.
6.1-P3	Enhance local and regional plans/programs for Joint Information Center (JIC) operations, and develop network-based "virtual" JIC support.
6.1-P4	Update the Regional Emergency Coordination Plan (RECP) and develop an annex to the RECP focused on a regional concept of operations (ConOps) for addressing emergency public information and warning and establishing and operating a regional JIC based on the SEMS, NIMS and the ICS.
6.1-P5	Update local Emergency Operation Plans (EOPs) to include an emergency

83

	public information and warning annex or amendment(s) to each base plan.
6.1-P6	Develop policy and guidance for social media use in emergency public information and warning and formally integrate social media activities into Operational Area and regional response plans.
6.1-P7	Develop protective actions for all potential Bay Area hazards and develop science-based warning message templates to communicate effective protective actions to the public.
6.1-P8	Develop plans and procedures for providing timely and effective warning information to isolated populations in the Bay Area.
6.1-P9	Develop or determine a regional shared "clearinghouse" server that uses the CAP standard to activate multiple Operational Area warning output systems (sirens, telephone, email, etc.) concurrently with a common message.
6.1-P10	Implement the federal Integrated Public Information Warning System (IPAWS) and Commercial Mobile Alerting System (CMAS) across the Bay Area.
6.1-P11	Obtain a State of California agreement regarding areas and types of warnings each agency will issue using IPAWS.
ORGANIZATION	
6.1-O1	Develop regional policy and program structures and assign a regional program manager for emergency public information and warning initiatives, and programs.
6.1-O2	Develop an MOU/MOA template for Operational Areas to customize and establish agreements with partner organizations and advocacy groups.
6.1-O3	Establish a regional operational support cell for effective public warning to include necessary MOUs and ConOps.
EQUIPMENT	
6.1-E1	Implement a virtual platform (e.g., UASI web platform) so emergency public information providers and policy makers (e.g., Bay Area Emergency Public Information Network and Emergency Public Information and Warning Work Group) have a mechanism to collaborate.
6.1-E2	Acquire and sustain equipment required to warn isolated populations (e.g., variable message signs to warn transient/commuter populations; sirens and public announcement systems to warn homeless; tone alert radios.
6.1-E3	Acquire and sustain equipment, laptops, tablets and other computing devices, to enable regional Warning Support Cell personnel connectivity to existing warning systems across the region.
6.1-E4	Procure equipment for Operational Areas necessary for integrating with the regional clearinghouse CAP server.
6.1-E5	Obtain IPAWS-certified warning control software packages for Operational Areas.
TRAINING	
6.1-T1	Provide joint training to community based organization (CBO) public information officers and Operational Area emergency management officials on the protocols and procedures for the handling and dissemination of emergency public information and warning to CBO members/constituents.

84

6.1-T2	Have all authorized warning originators complete a two-hour online course on IPAWS procedures and appropriate use.
6.1-T3	Provide training in social media use, and establish a regional platform to exchange best practices and develop regional awareness around existing social media capabilities.
6.1-T4	Deliver the California's Senior Officials Workshop to elected and senior officials across the region with an emphasis on emergency public information and warning.
EXERCISES	
6.1-Ex1	Conduct a regional exercise to evaluate JIC operations.
6.1-Ex2	Conduct exercise(s) that involve those with access and functional needs and isolated populations to evaluate emergency public information and warning capabilities to reach these groups.
6.1-Ex3	Conduct local and regional exercises to test and evaluate regional Warning Support Cell capabilities
6.1-Ex4	Involve local media in exercises to educate all participants on emergency public information and warning roles, responsibilities and capabilities.
6.1-Ex5	Conduct coordinated testing of warning systems from across the region.

Objective 6.2 Strengthen Operational Coordination Capabilities

The Bay Area has a fully integrated response system through a common framework of the Standardized Emergency Management System, Incident Command System and Unified Command including the use of emergency operations centers, incident command posts, emergency plans and standard operating procedures, incident action plans and the tracking of on-site resources in order to manage major incidents safely, effectively and efficiently. EOCs in the Bay Area can effectively plan, direct and coordinate information and activities internally within EOC functions, and externally with other multi-agency coordination entities, command posts and other agencies to effectively coordinate disaster response operations.

Objective 6.2 Implementation Steps and Resource Elements

PLANNING	
6.2-P1	Update or develop jurisdiction emergency operations plans (EOPs) that are compatible and integrate support for unified command during multi agency or multi-jurisdictional operations.
6.2-P2	Develop policies and procedures for utilizing the Law Enforcement Online Virtual Command Center capability at EOCs and other command posts.
6.2-P3	Develop regional plans and procedures to address ICS with a particular focus on unified command for multi-agency events and ensure they are integrated with onsite incident management.
6.2-P4	Ensure Department Operations Centers (DOCs) and EOCs have IT staffing requirements in their activation plans.
6.2-P5	Revise EOC activations plans as necessary to include 24 hour staffing for finance support during an emergency.

6.2-P6	Ensure that medical and health agencies and personnel are fully integrated in emergency operations plans and standard operating procedures at the regional, operational area, local and field levels.

ORGANIZATION	
6.2-O1	Develop or maintain Type I or II or III or IV incident management team.
6.2-O2	Establish SOPs for addressing staffing issues that area commands cannot address during an incident.

EQUIPMENT	
6.2-E1	Ensure DOCs and EOCs have sufficient information technology equipment and software (WebEOC) that is standardized/interoperable
6.2-E2	Ensure EOCs have operational and redundant communications equipment.
6.2-E3	Acquire and sustain back up power equipment for EOCs as needed.
6.2-E4	Acquire and sustain physical security enhancement equipment for the EOCs.
6.2-E5	Acquire and sustain inspection and screening systems at the EOC as necessary.

TRAINING	
6.2-T1	Ensure all appropriate personnel are trained in NIMS/SEMS incident command and unified command.
6.2-T2	Train personnel in accordance with NIMS/SEMS typing.
6.2-T3	Establish and maintain ICS training benchmarks and metrics and integrate them with relevant regional training plans.
6.2-T4	Provide training on the use of the Law Enforcement Online Virtual Command Center capability.
6.2-T5	Provide FEMA Independent Study Program: IS 700-NIMS, An Introduction; FEMA Independent Study Program: IS 800-National Response Plan, An Introduction; FEMA Independent Study Program: IS 275-EOC Management and Operations training.
6.2-T6	Provide FEMA Independent Study Program: IS 100-Introduction to Incident Command System; FEMA Independent Study Program: IS 200-ICS for Single Resources and Initial Action Incident training.
6.2-T7	Brief or train local chief executives and other key officials of the jurisdiction in the jurisdiction's command, control and coordination plans for large-scale emergencies.
6.2-T8	Establish and train appropriate personnel on standardized reporting format for area commands to utilize during briefings with EOCs and DOCs.
6.2-T9	Provide training to EOC personnel on the NIMS/ICS/SEMS and overall EOC functions and responsibilities in an emergency.

EXERCISES	
6.2-Ex1	Test to ensure all on-site incident management activities are coordinated through the Incident Command System with a focus on testing and evaluating unified command.
6.2-Ex2	Test whether formal operational briefings are conducted at the start of each operational period.
6.2-Ex3	Test whether IAP is re-assessed, revised, distributed, and briefed at least at the start of each new operational period.
6.2-Ex4	Develop exercise program to evaluate the effectiveness EOC incident

	management processes; communications and standards, and exercise programs for emergency operations plans, policies and procedures.
6.2-Ex5	Test and evaluate the integration of medical and health agencies and personnel in emergency operations plans and standard operating procedures at the regional, operational area, local and field levels.

Objective 6.3 Enhance Critical Transportation Capabilities

The Bay Area can provide transportation (including infrastructure access and accessible transportation services) for response priority objectives, including the evacuation of people, including those with access and functional needs, and animals, and the delivery of vital response personnel, equipment, and services into the affected incident areas to save lives and to meet the needs of disaster survivors.

Objective 6.3 Implementation Steps and Resource Elements

PLANNING	
6.3-P1	Update, as needed, the Bay Area Regional Catastrophic Earthquake Mass Transportation/Evacuation Plan.
6.4-P2	Evaluate the threats and hazards that may cause the need for large evacuations or sheltering in-place and determine evacuation/shelter zones (the areas where people must evacuate from or shelter within) based upon the potential consequences caused by the incident.
6.3-P3	Develop plans and procedures for evacuation/shelter-in place of access and functional needs populations.
6.3-P4	Develop plans and procedures for sheltering in place during a CBRNE event.
6.3-P5	Develop plans and procedures for evacuation/shelter-in place of companion animals.
ORGANIZATION	
6.3-O1	Develop and distribute public education materials on evacuation/shelter-in-place preparation, plans, and procedures for natural hazards and CBRNE events.
6.3-O2	Pre-arrange contracts and agreements to ensure provision of transportation vehicles (land, air and sea) and drivers during an incident requiring mass evacuations.
EQUIPMENT	
6.3-E1	Traffic control equipment (barriers, cones, directional signals).
TRAINING	
6.3-T1	Provide training on the implementation of the Bay Area Regional Catastrophic Earthquake Mass Transportation/Evacuation Plan.
6.3-T2	Develop and implement programs to train local citizens on evacuation, reentry and shelter-in place processes.
EXERCISES	
6.3-Ex1	Conduct exercises to test and evaluate the Bay Area Regional Catastrophic Earthquake Mass Transportation/Evacuation Plan.

Objective 6.4 Improve Mass Care

87

Mass care services, including sheltering, feeding, and bulk distribution, are rapidly, effectively and efficiently provided for the impacted population, including those with access and functional needs, in a manner consistent with all applicable laws, regulations and guidelines.

Objective 6.4 Implementation Steps and Resource Elements

PLANNING	
6.4-P1	Update, as needed, the Regional Catastrophic Mass Care and Sheltering Plan. Ensure the American Red Cross is fully accounted for in planning aspects.
6.4-P2	Develop plans and procedures for mass care involving a CBRNE incident.
6.4-P3	Develop mass care plans at the operational area level that integrate and account for those individuals and families with access and functional needs consistent with state and federal guidelines such as the Americans with disabilities Act.
ORGANIZATION	
6.4-O1	Develop pre-designated vendor agreements, blanket purchase agreements, or MOAs for critical mass care resources (pre-packaged meals ready to eat and ice).
6.4-O2	Develop public education materials concerning mass care services.
6.4-O3	Conduct an inventory of available shelter space for people and companion animals.
EQUIPMENT	
6.4-E1	Acquire, sustain and store directly or through partners mass care equipment such as cots (standard and accessible), blankets, feeding equipment (e.g., food storage containers), food and beverages, first-aid supplies, and animal supplies, etc.
TRAINING	
6.4-T1	Provide mass care training to include a focus on those with access and functional needs.
EXERCISES	
6.4-Ex1	Conduct exercises to test and evaluate the implementation of the Regional Catastrophic Mass Care and Sheltering Plan. Ensure the American Red Cross is an exercise participant.
6.4-Ex2	Test and evaluate the Bay Area's ability to provide relocation assistance or interim housing solutions for families unable to return to their pre-disaster homes.

Objective 6.5 Increase Community Resiliency

The Bay Area has a formal structure and process for ongoing collaboration between government and nongovernmental resources at all levels to prevent, protect/mitigate, prepare for, respond to and recover from all known threats and hazards.

Objective 6.5 Implementation Steps and Resource Elements

PLANNING	
6.5-P1	Ensure CERT Teams are integrated into ICS/NIMS/SEMS.
ORGANIZATION	
6.5-O1	Establish regional citizen educational programs on personal protective measures,

	disaster kits and communications plans that can be implemented locally.
6.5-O2	Develop regional public awareness and preparedness campaigns and education materials for access and functional needs populations that can implemented locally.
EQUIPMENT	
6.5-E1	Provide and sustain CERT teams with necessary equipment.
TRAINING	
6.5-T1	Train the public, with an emphasis on citizen corps volunteers, to be aware and to report suspicious items, smells and behavior to local law enforcement (with follow-on reporting by law enforcement to the regional NCRIC for analysis).
6.5-T2	Conduct CERT Team training on integration with first responders through ICS/NIMS/SEMS.
EXERCISES	
6.5-Ex1	Implement an exercise and evaluation process to assess citizen preparedness programs through specific exercises or as part of larger overall exercise
6.5-Ex2	Conduct exercises to test CERT capabilities.

Objective 6.6 Enhance Volunteer Management and Donations

Volunteers and donations within the Bay Area are organized and managed throughout an emergency based upon pre-designated plans, procedures and systems.

Objective 6.6 Implementation Steps and Resource Elements

PLANNING	
6.6-P1	Update, as needed, the Regional Catastrophic Donations Management Plan.
6.6-P2	Develop plans and procedures to improve local government and volunteer organizations' ability to recruit, screen, credential and manage both pre-affiliated and spontaneous volunteers.
ORGANIZATION	
6.6-O1	Provide standardized outreach to local jurisdictions in multiple languages, increasing the ability to effectively utilize all volunteers as necessary.
EQUIPMENT	
6.6-E1	Acquire and sustain interoperable volunteer management tracking systems. Ensure systems can manage spontaneous volunteers as well as on-call volunteers that can support a variety of capability and mission needs during and after a disaster.
TRAINING	
6.6-T1	Provide training on the implementation of the Regional Catastrophic Donations Management Plan.
6.6-T2	Develop just-in-time training program for volunteers to perform required tasks.
EXERCISES	
6.6-Ex1	Conduct exercises on the implementation of the Regional Catastrophic Donations Management Plan.

Objective 6.7 Improve Public and Private Services and Resources Management through Critical Resource Logistics

The Bay Area has a system to track and manage critical resources and make them appropriately available to incident managers and emergency responders from across the Bay Area to enhance emergency response operations and aid disaster victims in a cost-effective and timely manner.

Objective 6.7 Implementation Steps and Resource Elements

PLANNING	
6.7-P1	In coordination with the State, develop a comprehensive region-wide system of resource typing, inventoried resources and credentialing (Metrics Project) so as to provide emergency managers and incident commanders and first responders the ability to locate, track and request needed resources in a coordinated and effective manner.
6.7-P2	Develop a regional critical resource logistics plan for catastrophic incident response.
6.7-P3	Develop standardized procedures for utilizing Law Enforcement Online Virtual Command Center to assist with logistics operations.
ORGANIZATION	
6.7-O1	Ensure a logistics planning manager for regional coordination of logistics operations and planning.
6.7-O2	Pre-negotiate vendor contracts for critical resources and essential services.
EQUIPMENT	
6.7-E1	Acquire and sustain CBRNE logistical support equipment.
TRAINING	
6.7-T1	Develop and deliver training in emergency logistics that incorporates linkages among damage/needs assessment, logistics management, and volunteer/donations management.
EXERCISES	
6.7-Ex1	Test and evaluate resource and logistic tracking and recording.

GOAL 7	Mission Area(s)	National Priorities	Core Capabilities	State Strategy
ENHANCE RECOVERY CAPABILITIES	Recovery	N/A	Infrastructure Systems Economic and Community Recovery	Goal 7: Enhance Recovery Capabilities

The National Recovery Framework

Given the risk of a major disaster occurring in the Bay Area, it is essential for the region to establish both short-term and long-term recovery capabilities. Building recovery capabilities has for some time been a neglected element of homeland security and emergency preparedness. To help address this gap, in September 2011, DHS released the final National Disaster Recovery Framework. The NDRF defines how Federal agencies will organize and operate to utilize existing resources to promote effective recovery and support states, tribes and other jurisdictions affected by a disaster.

The NDRF seeks to define:

- Roles and responsibilities of the newly-proposed recovery coordinators and other stakeholders;
- A coordinating structure, which includes proposed Recovery Support Functions, that facilitates communication and collaboration among all stakeholders;
- Guidance for pre- and post-disaster recovery planning; and
- The overall process by which, together as a nation, we can capitalize on opportunities to rebuild stronger, smarter, and safer communities.

The NDRF compliments and aligns with the National Response Framework (NRF) and utilizes an operational structure to develop a common recovery framework in a manner similar to how the NRF establishes a common response framework. The NDRF replaces the NRF Emergency Support Function #14 (ESF #14) - Long-Term Community Recovery with six Recovery Support functions (RSFs):

- Community Planning and Capacity Building.
- Economic.
- Health and Social Services.
- Housing.
- Infrastructure Systems.
- Natural and Cultural Resources

The Bay Area will utilize the NDRF as a guide for developing its own recovery framework in coordination with the State of California and the Federal Government. In doing so, certain key principles will guide the development of the regional recovery framework:

- Critical to recovery preparedness is pre-disaster planning, an ongoing responsibility for all levels of governments; individuals and families; the business community; and voluntary, faith-based and community organizations.
- Local governments have primary responsibility for disaster recovery in their community and play the lead role in planning for and managing all aspects of community recovery.
- Partnerships and inclusiveness between local businesses; owners and operators of critical infrastructure and key resources; and voluntary, faith-based, and community organizations are vital.

The Bay Area has significant experience in this area and will build upon that experience to ensure that essential functions from initial damage assessment to housing to economic and community restoration takes place as quickly and as smoothly as possible.

Finally, the NIPP and the CIKR Annex to the NRF provide a bridge between steady-state CIKR protection and resilience programs and incident response. The NDRF links both documents and their related protection and response missions to the recovery mission area. As the Bay Area develops its own recovery framework, it will ensure integration with its CIKR protection and incident response programs where applicable.

Objective 7.1 Strengthen Infrastructure Systems

The Bay Area can provide accurate situation needs and damage assessments by utilizing the full range of engineering, building inspection, and code enforcement services in a way that maximizes the use of resources, aids emergency response, implements recovery operations, and restores the affected area to pre-incident conditions as quickly as possible. The Bay Area can coordinate activities between critical lifeline operations and government operations to include a process for getting the appropriate personnel and equipment to the disaster scene so that lifelines can be restored as quickly and as safely as possible to support ongoing emergency response operations, life sustainment, community functionality, and a transition to recovery.

Objective 7.1 Implementation Steps and Resource Elements

PLANNING	
7.1-P1	Each Operational Area, and the region as a whole, has a complete inventory of critical lifelines within each Operational Area and across the region.
7.1-P2	Provide assessments, inventories and planning recommendations to mitigate seismic risks in the Bay Area by completing an assessment and inventory of soft story construction in the Bay Area.
7.1-P3	Ensure damage assessment protocols and procedures in the Regional Emergency Coordination Plan are kept up to date.
7.1-P4	In coordination with the State, conduct infrastructure intersection/interdependency analysis and work plans for guiding mitigation projects, response priorities and post-disaster recovery actions within operational areas and across the region.
7.1-P5	Continue to utilize the San Francisco Lifelines Restoration Project as a foundation for regional lifelines restoration planning.
ORGANIZATION	

7.1-O1	Consistent with the Regional Volunteer Management Plan, develop plans and procedures to recruit volunteers to join assessment teams and conduct structural damage assessments post disasters.
7.1-O2	In coordination with the State sponsored Metrics Project, develop standards and procedures, to include a database to identify qualified contractors offering recovery/restoration services and equipment across the Bay Area.
7.1-O3	Develop qualification and certification standards for paid and volunteer staff.
7.1-O4	Develop and maintain disaster assessment teams per NIMS - Type I, or II, and/or III Disaster Assessment Teams, and Engineering Service Teams.
EQUIPMENT	
7.1-E1	Acquire and sustain technology and systems that can predict the effects of a specific incident or hazard, including estimated damage to the region's transportation system, type, amount and location of debris, and number of buildings severely or completely damaged.
7.1-E2	Acquire, sustain and inventory personal protective equipment for recovery damage assessment teams. Deploy caches of equipment outside danger zones if necessary.
7.1-E3	Acquire and sustain damage assessment data collection system (hardware and software).
7.3-E4	Acquire and sustain back-up generators for short term restoration of lifelines.
TRAINING	
7.1-T1	Provide training to volunteers and paid personnel on damage assessment procedures, plans and equipment.
7.3-T2	Provide training to government entities on the restoration of lifelines process.
EXERCISES	
7.1-Ex1	Ensure damage assessment procedures and mitigation plans and procedures are exercised independently or as part of a regional exercise.
7.1-Ex2	Coordinate with other lifelines companies/sectors to create cross-sector exercises to test restoration plans.

Objective 7.2 Enable Economic Recovery

During and following an incident, the Bay Area can estimate economic impact, prioritize recovery activities, minimize business disruption, and provide individuals and families with appropriate levels and types of relief with minimal delay.

Objective 7.2 Implementation Steps and Resource Elements

PLANNING	
7.2-P1	Develop Regional Recovery Support Function (RSF) or equivalent recovery framework that addresses housing, economic, environmental, infrastructure, and health and social service needs.
7.2-P2	Update, as needed, the Regional Catastrophic Interim Housing Plan.
ORGANIZATION	

7.2-O1	Identify responsibilities for the position of a Regional Disaster Recovery Coordinator (RDRC) or equivalent, and resources for regional recovery support functions.
TRAINING	
7.2-T1	Develop and implement recovery training and education as a tool for building recovery capacity and making it available to all other stakeholders.
7.2-T2	Provide training on the implementation of the Regional Catastrophic Interim Housing Plan.
EXERCISES	
7.2-Ex1	Exercise stabilization and recovery plans to include the Regional Catastrophic Earthquake Interim Housing Plan through specific exercises or as part of larger overall regional exercise.

Objective 7.3 Improve Environmental Response Health and Safety Capabilities

After the primary incident, the Bay Area is able to assess, monitor, perform cleanup actions, including debris and hazardous waste removal, and provide resources to prevent disease and injury through the quick identification of associated environmental hazards.

Objective 7.3 Implementation Steps and Resource Elements

PLANNING	
7.3-P1	Update, as needed, the Regional Catastrophic Debris Removal Plan.
7.3-P2	Develop plans to enhance capacity of sewage treatment facilities for major disasters.
7.3-P3	Pre-identify potential routes for debris removal and debris management.
7.3-P4	Develop debris removal and debris management annexes to EOPs where necessary.
TRAINING	
7.3-T1	Provide training on environmental health to pre-designated managers, responders, and volunteers of mass-care operations.
7.3-T2	Provide training to environmental health strike teams.
7.3-T3	Develop and conduct emergency response training relevant to all waste water systems including field staff and managers of waste water programs, waste water utilities, public health, and emergency management.
EXERCISES	
7.3-Ex1	Conduct, or include as part of broader exercises, tests and evaluations of environmental health teams in the region.
7.3-Ex2	Conduct, or include as part of broader exercises, tests of waste water sewage facilities' capacity.

SECTION 6 GOALS AND OBJECTIVES

GOAL 8	Mission Area(s)	National Priorities	Core Capabilities	State Strategy
ENHANCE HOMELAND SECURITY EXERCISE, EVALUATION AND TRAINING PROGRAMS	All	All	All	Goal 9: Enhance Homeland Security Exercise, Evaluation and Training Programs

Bay Area Training and Exercise Program

The Bay Area's multi-year Homeland Security Exercise, Evaluation and Training Program is designed to address regional goals, build towards and test against target capabilities within this Strategy, and improve the operational readiness of the homeland security system in the Bay Area across the full spectrum of prevention, protection, mitigation, response and recovery.

The training and exercise goal is primarily focused on developing a system and framework to implement the training and exercise needs identified in the implementation steps within the other objectives in the *Strategy*. The goals, vision and mission of the Bay Area's training and exercise program are set forth below.

Figure 8: Bay Area Planning and Investment Process

Goals: The Training and Exercise Planning Workgroup will engage in fair, open and transparent processes throughout the planning and implementation processes to ensure that products and services rendered, are equitably distributed, are at a reasonable cost, and ensure fair competition.

Vision: To promote, encourage and provide training and exercise opportunities for our emergency response workforce, and by ensuring our workforce is maintained in a state of readiness and competencies for all communities in region.

Mission: Utilizing the Training and Exercise Strategic Plan, the Alameda County Sheriff's Office, on behalf of the Bay Area UASI program, will promote equitable distribution of training and exercise funds amongst various agencies and disciplines within the region.
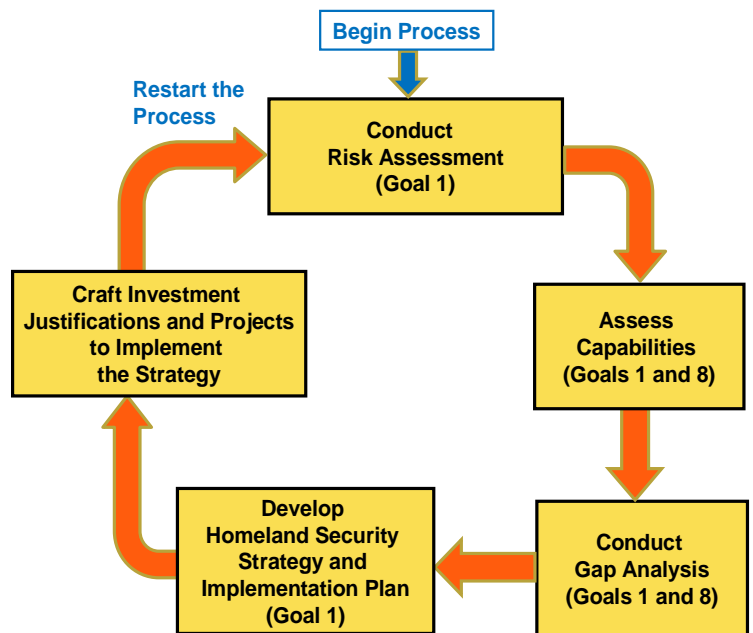
Figure 8 above reinforces the Bay Area planning process chart by demonstrating once again the cyclical nature of the risk management and planning process and how Goals 1 and 8 play an overarching role in this process by first identifying the priority risks faced by the Bay Area jurisdictions, and the priority capabilities needed to address those risks. This is followed by constructing the exercise and evaluation means to determine if those priority capabilities are

being enhanced through the implementation steps within each of the objectives throughout the Strategy.

Training and exercises provide the means to enhance, test, and evaluate the Bay Area's proficiency in homeland security generally and the priority capabilities in particular. Exercises, as discussed in the Strategy Evaluation Section, are a critical means of determining whether the Bay Area is actually enhancing those priority capabilities designed to reduce the region's risk. Any assessment program must include a robust exercise and evaluation element to ensure data from simulated incidents are integrated with self-assessment data, and of course, real-world incident data collected both during and after the incident when available. Such a process will put the Bay Area in the best possible position to understand whether it is truly enhancing capabilities and overall preparedness.

Training and Exercises Plans and Procedures

The Bay Area will develop and maintain a regional training program that covers all public safety, health and medical agencies and support entities. The program will be managed by an executive agent/program manager. The executive agent/program manager will oversee, either directly or through separate contracts, all training for the region and will manage all training reimbursements from other member jurisdictions and manage the overall program for the entire Bay Area. The purpose is to build a training program that unifies all jurisdictions within the Bay Area toward a common set of goals while recognizing that each jurisdiction and discipline will have differing levels of capabilities and training needs.

The Bay Area's jurisdictions possess differing levels of preparedness regarding terrorism prevention, protection, mitigation, response, and recovery capabilities. Because of these differences, the Bay Area exercise and evaluation program will use a building-block approach in the design of the overall exercise program. This building-block approach ensures successful progression in exercise design, complexity, and execution, and allows for the appropriate training and preparation to take place in the jurisdiction or area conducting the exercise. Exercises conducted at all jurisdictional levels within the Bay Area – local, operational area, full region - should follow the planning, training, exercise, and improvement plan cycle. As the cycle indicates, it is recommended that jurisdictions accomplish the following specific planning steps prior to conducting an exercise:

- Assess current operations plans for completeness and relevance
- Assess the current level of training and operational plan familiarity for all relevant agencies within the jurisdiction
- Conduct necessary training for all relevant agencies
- Train personnel on newly received equipment
- Conduct exercises using equipment, training, and operations plans
- Develop an After Action Report (AAR) that captures the lessons learned.

The exercise progression for each jurisdiction is to move from a seminar to a table top, to a functional exercise, and finally, to a full scale exercise. These particular exercise types allow for a logical progression of regional and jurisdictional preparedness by increasing in size, complexity, and stress factor, while allowing for significant learning opportunities that

96

effectively complement, build upon, and directly lead into one another. This model is flexible enough to allow for the addition of other desired exercise types.

The Bay Area's Urban Shield Exercise

Urban Shield is a national model, full-scale exercise, designed to assess and validate the speed, effectiveness and efficiency of capabilities, as well as test the adequacy of regional policies, plans, procedures and protocols. Urban Shield incorporates regional critical infrastructure, emergency operations centers, regional communication systems, equipment and assets, as well as personnel representing all aspects of emergency response including intelligence, law enforcement, explosive ordnance disposal units, fire, EMS, etc. The Urban Shield exercise is unique because of its focus on training during the exercise. This training provides first responders, homeland security officials, emergency management officials, private and non-governmental partners, and other personnel with the knowledge, skills, and abilities needed to perform key tasks required in large-scale disasters.

Objective 8.1: Strengthen the Regional Exercise and Evaluation Program

The Bay Area exercise program tests and evaluates the region's enhancement and/or sustainment of the right level of capability based on the risks faced by the region with an evaluation process that feeds identified capability gaps and strengths directly into the region's risk management and planning process for remediation or sustainment.

Objective 8.1 Implementation Steps and Resource Elements

PLANNING	
8.1-P1	Develop and maintain a comprehensive regional exercise plan and program for the development and conduct of exercises based on risk and capability needs that cover the spectrum of prevention, protection, mitigation, response and recovery mission areas.
8.1-P2	Coordinate with local jurisdictions to incorporate locally driven needs into the regional exercise plan.
8.1-P3	Collaborate with local jurisdictions to develop regional exercise goals to meet multiple exercise requirements and foster participation in regional exercises.
8.1-P4	Coordinate regional exercises with State driven exercises (Golden Guardian) to reduce duplication of effort.
8.1-P5	Design After Action Reports and improvement plans that are built from capability targets and capture capability proficiencies and gaps that can be readily assessed and quantified for planning purposes.
8.1-P6	Host agency of major exercise(s) should reconvene participants to review key findings to ensure lessons learned are identified and taken back to all involved agencies.
8.1-P7	The exercise program management office will evaluate the feasibility of developing a regional exercise calendar.
8.1-P8	The exercise program management office will review HSEEP portal for trends on best practices and lessons learned and report this information to the Training and Exercise Committee on an as needed basis.

EQUIPMENT	
8.1-E2	Procure authorized and necessary equipment to conduct exercises.
TRAINING	
8.1-T1	Train exercise planning and evaluation staff at the regional and jurisdictional levels on exercise design, management and evaluation procedures.
EXERCISES	
8.1-Ex1	Develop at least one, regional multi-disciplinary full-scale exercise consistent with the identified theme of the annual statewide exercise and run the exercise at multiple locations with multiple partners in the region.
8.1-Ex2	Conduct multiple exercises at the sub-regional and jurisdictional level annually.

Objective 8.2 Enhance the Regional Training Program

The Bay Area has a multi-discipline multi-jurisdictional risk and capabilities based training program that enhances and sustains priority capabilities in order to mitigate the region's most pressing risks.

Objective 8.2 Implementation Steps and Resource Elements

PLANNING	
8.2-P1	Develop and maintain a comprehensive regional training plan and program for the development and conduct of training based on risk and capability needs that cover the spectrum of prevention, protection, mitigation, response and recovery mission areas.
EQUIPMENT	
8.2-E1	Materials and supplies, reproduction of materials, and such other equipment needed to conduct the training and support the training program.
8.2-E2	Tools and systems to document and manage training programs.
TRAINING	
8.2-T1	Implement training to all disciplines based on the regional training program.

SECTION 6 GOALS AND OBJECTIVES

SECTION 7
STRATEGY IMPLEMENTATION

7.1 Implementation Overview

With the development and update of the *Strategy*, the Bay Area must have a comprehensive implementation process to ensure the data and priorities encapsulated in the *Strategy* actually drive the region's policies, structures, projects and investments. This requires assigned roles and responsibilities and a process and tools that link the Bay Area's investments back to the *Strategy's* goals and objectives.

The Bay Area UASI Management Team will have overall responsibility for managing and tracking implementation of the *Strategy*. This will include day-to-day management of the *Strategy* and ensuring that it is updated and followed. This will be done through the development of investment justifications and annual reporting (discussed in the following section).

The Bay Area's strategic approach to implementing the *Strategy* through investing will be premised on two overarching principles:

- First, sustain current priority programs and capabilities in the region.
- Second, close gaps in capabilities with an emphasis on those capabilities that have the highest risk relevance and the largest capability gaps

Given the current fiscal reality of strained state and local budgets, the Bay Area will strive to integrate the various homeland security and preparedness grants that flow into the region to include those from DHS and HHS. This will be done while respecting the responsibilities and authorities vested in individual grantees.

7.2 Investment Justifications

The purpose of submitting investment justifications to DHS is to obtain grant funding necessary to implement the goals and objectives of this *Strategy*. Investment justifications that fall outside the goals and objectives of this *Strategy* will not be submitted. In addition, funding received from other sources related to homeland security may be leveraged in accordance with the goals and objectives of this *Strategy*.

The investment justification process must be viewed as the culmination of a comprehensive homeland security planning and implementation process and not simply as a ninety-day application writing event in order to ask for money from the federal government. This process requires specific steps and management in order to ensure the region as a whole presents a unified investment picture to DHS and the State of California. As such, the *Strategy* outlines, at a high level, those steps that, at a minimum, must be taken in order to ensure the regions operates efficiently and effectively in the planning and investment process.

SECTION 7 STRATEGY IMPLEMENTATION

7.3 Strategy Implementation Process

While the specific details concerning the *Strategy's* implementation process may vary from year to year, certain fundamentals will be followed to ensure the region is achieving and tracking its homeland security goals and objectives. For the Bay Area, given its size and diversity, the process will involve a combination of jurisdictional, sub-regional and region-wide efforts and responsibilities.

7.3.1 Strategy Implementation Guidance

For each fiscal year, the UASI Management Team will develop specific strategy implementation guidance for working groups and applicants to follow during each investment justification cycle relative to the UASI grant program. This will include planning timelines, investment strategies and priorities for a given grant cycle, grant guidance to include funding allocation formulas and allowable spending areas, project templates, and such other materials and policies as necessary.

7.3.2 Project Template

For the UASI grant cycle, and as part of the implementation guidance, the UASI Management Team will develop a project template to be used by applicants to outline proposed projects. The template will be designed to link projects to the Bay Area Strategy by requiring applicants to link to the goals, objectives and implementation steps, including POETE elements, within the Strategy. It is through the project templates that the Bay Area will first link dollars to objectives and in turn link capabilities to dollars to help better answer where and how the region is better prepared.

7.3.3 Project Development

The project template designed by the Bay Area UASI Management Team will be a primary tool with which to vet proposed projects by the region's stakeholders. Only upon vetting by the Bay Area UASI Management to ensure compliance with grant guidelines and UASI policy or the work group shall a project be put forward for final approval by the Approval Authority to implement a specific goal and objective(s) in the Strategy.

With support from the Management Team, the entities, planning hubs, or work groups responsible for overseeing the implementation of the goals and objectives in the Strategy will work with project managers and others to track whether an implementation step within each objective is complete, partially complete or ongoing and report this information to the Advisory Group and Approval Authority as necessary. A complete step is one that is finished and requires no additional resources for implementation. A partially complete step is one where some, but not all, of the step is finished and requires additional resources for completion. An ongoing step is one that may be finished insofar as the plan has been written or the equipment has been purchased but where additional resources are need for sustainment.

SECTION 8
STRATEGY EVALUATION

8.1 Evaluation Overview

In order to truly understand what value the Bay Area is getting for its homeland security investments, the region must have a consistent mechanism by which to measure the effectiveness of the homeland security activities – plans developed, personnel hired, organization and operations conducted, equipment purchased, number of people trained, and exercises conducted – generated through those investments.

In 2011, the Bay Area conducted a preliminary analysis of UASI grant effectiveness. The report qualitatively and quantitatively documented progress made by the Bay Area in building capabilities, reducing risk, and enhancing regional preparedness through investments that support the goals and objectives in the *Bay Area Homeland Security Strategy*, which aligns with the National Preparedness Guidelines and supports the implementation of the State of California Homeland Security Strategy and the National Security Strategy. The report serves as a baseline for future assessments and evaluations of how the region is implementing its Strategy and the effectiveness of the grant programs and other funding sources utilized to do so.

8.2 The Evaluation Process

The long-term goal for the Bay Area is to build a process and tools in order to qualitatively and quantitatively document progress made by the Bay Area in building capabilities, reducing risk, and enhancing regional preparedness based on implementing the goals and objectives outlined in the *Bay Area Homeland Security Strategy*. The result will be the *Bay Area Effectiveness Report*.

Where the *Bay Area Homeland Security Strategy* presents what the region needs to achieve or sustain in homeland security, the *Bay Area Effectiveness Report* presents what the region has actually accomplished in the area of homeland security as a result of investments called for in the *Strategy* from different sources, including local budgets, state budgets, and grants.

Built into each goal and objective in this *Strategy* is a previously conducted risk and capabilities assessment and gap analysis which helped prioritize each goal and objective and identify gaps in each capability. To measure the implementation of the *Strategy*, the Bay Area will evaluate each goal and its related objectives based upon the following high level evaluation guidelines the implementation of which shall be developed and coordinated by the UASI Management Team:

- Update the outcome for each objective in the *Strategy*. This outcome will set the agreed upon broad and overall target level of capability upon which evaluation for each objective will be based.

- Develop Bay Area specific preparedness and performance measures and targets based on the TCL/Core Capabilities List and NIMS/SEMS resource types as well as other resources. Both the TCL and the NIMS/SEMS have laid out critical tasks, preparedness and performance measures, targets and standards for resources that can serve as useful

indicators regarding the current level of preparedness in a given capability area. However, they are not tailored to the specific needs of a given jurisdiction or region. Therefore, the Bay Area must define those targets, measures, and metrics specifically for the region and will consider doing so according to the Core Capabilities or some combination of the TCL and Core Capabilities in the near future.

- Conduct the exercise and evaluation program. The Bay Area's HSEEP must be **designed upfront** to test whether target capability performance outcomes and related critical tasks are being achieved. Exercises should be designed around testing and evaluating the region's ability to prevent, protect against, mitigate, respond to and recover from the highest risk terrorism scenarios against the highest risk CIKR across the region.

- Inventory investments and projects based on each capability. Each objective has a set of implementation steps broken out by POETE, which coincides with the funding solution areas allowed under most DHS grant programs. That data will be used directly against the performance measures to help determine increases in capability and better understand allocation of resources by capability.

8.3 Methods for Evaluation

Evaluating the implementation of this *Strategy* will be done in the form of measuring whether risk based capability needs are being implemented and tracked. Each objective in this *Strategy* has a set of outcomes in the form of performance objectives tied to it. Those outcomes will form the basis or capability target for measuring whether the region is on pace to achieving or maintaining that objective. It must be noted that each outcome in this *Strategy* is set at the UASI regional level and not at the jurisdictional level within the Bay Area UASI. Thus, each jurisdiction may have different outcomes based on jurisdictional level planning efforts that may be influenced by unique risk and need factors.

To date, there is no single agreed upon method to assess capabilities. Rather, there are a number of data sources and methodologies to help with this process each of which the Bay Area will utilize in the evaluation process:

- Self-Assessments
- Performance based assessments (real world and exercise events)
- Modeling and simulation

8.3.1 Self Assessments

Self-assessments are those where members of the Bay Area homeland security community convene to evaluate their capability levels based on a series of questions and defined metrics and measures. These assessments can cover a wide array of capabilities and public safety disciplines or be targeted to a specific capability or function (e.g., law enforcement). While useful, self-assessments are subjective and can be influenced by factors including the number and type of attendees at the assessment and the questions asked or not asked.

Self-assessments will most often involve workshops, interviews or webinars whereby subject matter expert participants will be asked a series of questions to get an understanding of how they view their level of ability to perform a specific task or set of tasks during a given scenario. For example, SWAT or bomb squad team-based capability assessments can begin with audits of team equipment, supplies, and training records, as well as on site visits to interview team members to capture data.

The Bay Area has undergone several self-assessments over the last several years, most recently in 2009, 2010 again in 2011. In 2009, the Bay Area conducted a region-wide assessment whereby subject matter experts from across the region evaluated the region's level of ability within each of the 37 Target Capabilities. A similar assessment was conducted in 2010 with the difference being the assessment was broken out into four assessments. In 2011, a region wide assessment was once again conducted along with assessments at each of the 12 operational areas.

8.3.2 Performance Based Assessments

Performance-based assessments are most common in the form of exercises, although an ability to track and measure performance during a real world incident would provide the most accurate picture of capability. For the Bay Area, performance-based exercises should be based on testing the region's ability to prevent, protect against, mitigate, respond to and recover from the highest risk terrorism scenarios against the highest risk CIKR as outlined in the risk overview section of the *Strategy*. The Bay Area's primary mechanism for performance based assessment is the Urban Shield Full Scale Exercise conducted annually.

Urban Shield tests the Bay Area's ability to manage numerous on-going critical incidents through the use of multiple incident commands. The critical incidents take place in a variety of venues over an extended period of time. The exercise requires full implementation of the components of the NIMS and SEMS. An Incident Command System (ICS) structure, with four Area Commands and a Department Operations Center are implemented to manage this extremely large exercise.

8.3.3. Modeling and Simulation Assessments

Quantitative capability models can be used to assist with planning and resource allocation, and to help determine capability gaps. Models can provide an independent baseline estimate of required levels of capability for a given jurisdiction or the region, based upon national averages, demographic information, and risk criteria. These models can use quantitative data to inform investment decisions by estimating the full lifecycle costs of achieving a given level of a capability, identifying capability gains from investments, and optimizing placement of new resources.

Appendix A
Crosswalk of Target and Core Capabilities

Target Capability	Core Capability
Planning	Planning
Critical Infrastructure Protection	Physical Protective Measures
Information Gathering and Indicators and Warnings	Intelligence and Information Sharing
Intelligence and Information Sharing and Dissemination	
Intelligence Analysis and Production	
Risk Management	Risk Management for Protection Programs and Activities
Responder Safety and Health	Environmental Response Safety and Health
WMD/HazMat Response	
Environmental Health	
Counter-Terrorism and Law Enforcement	Interdiction and Disruption
Emergency Public Safety and Security Response	On-Scene Security and Protection
Explosive Device Response Operations	
On-site Incident Management	Operational Coordination
EOC Management	
Emergency Public Information and Warning	Public Information and Warning
Triage and Pre-Hospital Treatment	Public Health and Medical Services
Medical Surge	
Mass Prophylaxis	
Isolation and Quarantine	
Laboratory Testing	
Epidemiological Surveillance and Investigation	
Medical Supplies Management and Distribution	
Communications	Operational Communications
Fire Incident Response Support	Public and Private Services and Resources
Volunteer Management and Donations	
Critical Resource Logistics and Distribution	
Search and Rescue (Land Based)	Mass Search and Rescue
CBRNE Detection	Screening, Search and Detection
Restoration of Lifelines	Infrastructure Systems
Structural Damage Assessment	
Economic and Community Recovery	Economic Recovery
Community Preparedness and Participation	Community Resilience
Citizen Evacuation and/or Shelter In-Place	Critical Transportation
Mass Care	Mass Care Services
Fatality Management	Fatality Management Services
Food and Agriculture Safety and Defense	Supply Chain Integrity and Security
Animal Disease Emergency Support	
Not Applicable	Risk and Disaster Resilience Assessment
	Situational Assessment
	Long Term Vulnerability Reduction
	Access Control and Identity Verification
	Forensics and Attribution
	Threat and Hazard Identification
	Cyber Security
	Health and Social Services
	Housing
	Natural and Cultural Resources

104

Appendix B
Record of Changes

The following table tracks the significant changes made to the *Strategy*. Revisions that should be documented include the following:

- Updates in risk and capability assessment information.
- Completion or removal of implementation steps
- Addition, reprioritization or other change in goals and objectives following a capabilities assessment or similar analysis.
- Changes in Urban Area organization.
- Changes in vision or mission.

Date of Change	Page(s)	Brief Description of Changes
October 2013	26	Added new section 4.5 on the Bay Area Compendium of Core Capabilities.
October 2013	32	Section 5.4 Critical Infrastructure and Key Resources. The number of CIKR is now nearly 13,000.
October 2013	34	Section 5.5 Risk Profile. Updated threats and hazards and likelihood versus risk comparison.
October 2013	36	Added new section 5.5.3 on the Threat Hazard Identification and Risk Assessment.
October 2013	37-38	Section 5.6 Asset Risk by Sector. Update all data.
October 2013	39-41	Section 5.7 Capabilities Assessment. Updated risk relevant capabilities list and table linking threats, CIKR sectors and capabilities all based on new data and taxonomy of Core Capabilities.
October 2013	50-54	Goal 2, added new introductory section on cyber security
October 2013	60-61	Goal 2, Objective 2.4. Added new cyber security objective and implementation steps.
October 2013	84-89	Section 6. Reorganized goals and objectives. Moved objective 4.5 to new 6.7 and moved objective 4.7 to new 6.2.