SAN DIEGO OPERATIONAL AREA CRITICAL INFRASTRUCTURE PROTECTION PLAN

Prepared for

Office of Emergency Services
County of San Diego
5555 Overland Drive
San Diego, CA 92123

URS Project No. 27697104

July 2008

URS

1615 Murray Canyon Road, Suite 1000
San Diego, CA 92108-4314
619.294.9400 Fax: 619.293.7920

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Executive Summary 1

Section 1 Introduction 1-1

1.1 Purpose 1-1
1.2 Assumptions 1-2
1.3 Applicability 1-2
1.4 Background and Current Status 1-2
1.4.1 National CIP Efforts and Drivers 1-2
1.4.2 State Efforts 1-3
1.4.3 Relationship of this Plan to Other CIP Efforts 1-3
1.5 Authorities 1-3
1.6 Information Security/Sharing 1-4

Section 2 Roles and Responsibilities 2-1

2.1 Operational Area CIP Decision-Making Entities 2-1
2.1.1 Stakeholders Committee 2-1
2.1.2 Steering Committee 2-2
2.2 Local, State, and Federal Governments 2-2
2.3 Owners/Operators 2-2
2.4 Past Efforts 2-3
2.4.1 San Diego Urban Area Security Strategy 2-3
2.4.2 Buffer Zone Protection Program 2-3
2.4.3 Hazard Mitigation Plan 2-3
2.4.4 InfraGard 2-3

Section 3 Identifying Critical Assets 3-1

3.1 Develop the Initial List of Assets 3-1
3.2 Detailed Sector-Specific Information 3-6
3.2.1 Agriculture and Food Sector 3-6
3.2.2 Banking and Finance Sector 3-7
3.2.3 Chemical Sector 3-8
3.2.4 Commercial Facilities Sector 3-8
3.2.5 Communications Sector 3-9
3.2.6 Dams Sector 3-10
3.2.7 Defense Industrial Base Sector 3-10
3.2.8 Emergency Services Sector 3-11
3.2.9 Energy Sector 3-12
3.2.10 Government Facilities Sector 3-12
3.2.11 Information Technology Sector 3-13
3.2.12 National Monuments and Icons Sector 3-14
3.2.13 Nuclear Reactors, Materials and Waste Sector 3-14
3.2.14 Postal and Shipping Sector 3-14
3.2.15 Public Health, and Healthcare Sector 3-15
3.2.16 Transportation Systems Sector 3-15
3.2.17 Water Sector 3-16
3.3 Interdependency 3-16

TABLE OF CONTENTS

Section 4 Assessment Methodology 4-1

4.1 Consequence Assessment 4-1
4.1.1 Determine Consequence Factors and Weightings 4-2
4.1.2 Determine Criteria for Rating Asset Consequence and Rate Assets 4-3
4.1.3 Incorporate Interdependencies and Prioritize List 4-3
4.2 Threat Assessment 4-4
4.2.1 Consideration of All-Hazards 4-4
4.2.2 Man-Made Hazards 4-4
4.2.3 Natural Hazards 4-5
4.3 Vulnerability Assessment 4-6
4.4 Risk Assessment 4-7

Section 5 Decision Making Process 5-1

5.1 Resource Prioritization 5-1
5.1.1 Protective Measures 5-1
5.1.2 Resource Allocation 5-2
5.2 Resource and Funding Options 5-2
5.2.1 U.S. Department of Homeland Security Grant Programs 5-3

Section 6 Future Initiatives 6-1

6.1 Risk Management 6-1
6.2 Implement Protective Programs 6-1
6.2.1 Immediate Action Items 6-2
6.2.2 Potential Long Range Objectives 6-2
6.3 Assess Effectiveness 6-2
6.4 Coordination with Private Owner/Operators 6-3

Tables

Table 3-1 DHS Sector Function and Asset Selection Rationale
Table 4-1 San Diego Region Consequence Factors
Table 4-2 Upper-Bound Criteria
Table 4-3 Symbolic Importance Rating Criteria
Table 4-4 Critical Infrastructure Vulnerability Ratings

Figures

Figure 3-1 DHS Sector to Asset Mapping
Figure 4-1 Relative Risk Diagram
Figure 6-1 DHS Risk Management Diagram

ACAMS	Automated Critical Asset Management System
BZPP	Buffer Zone Protection Program
CCP	Citizen Corps Program
CI	Critical Infrastructure
CI/KR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIPP	Critical Infrastructure Protection Program
COOP	Continuity of Operations
County	San Diego County
DHS	Department of Homeland Security
DOC	Department of Commerce
DoD	Department of Defense
EM	Emergency Management
EMS	Emergency Medical Service
EOP	Emergency Operations Plan
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigations
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Administration
G&T	Office of Grants and Training
GCC	Government Coordinating Council
GIS	Geographic Information Systems
HAZMAT	Hazardous Material
HSGP	Homeland Security Grant Program
HSPD-7	Homeland Security Presidential Directive 7
IBSGP	Intercity Bus Security Grants
IPP	Infrastructure Protection Program
ISAC	Information Sharing and Analysis Centers
ISPs	Internet service providers
IT	Information Technology
JTTF	Joint Terrorism Task Force
MAST	Maritime Assessment and Strategy Tool
MMRS	Metropolitan Medical Response System
MSRAM	Maritime Security Risk Analysis Model
NIPP	National Infrastructure Protection Plan
OA	San Diego Operational Area
OES	County of San Diego Office of Emergency Services
OHS	California Office of Homeland Security
OIP	Office of Infrastructure Protection
PCII	Protected Critical Infrastructure Information
PSGP	Port Security Grant Program
PSTN	Public Switched Telecommunications Network
PTEs	potential threat elements
RG	Risk Group
RTTAC	Sheriff's Regional Terrorism Threat Assessment Center
SAR	Search and Rescue
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SHSP	State Homeland Security Program
SSA	Sector Specific Agency

SSP	Sector Specific Plan
SWAT	Special Weapons and Tactics
TLO	Terrorism Liaison Officer
TRAM	Transit Risk Assessment Module
TSA	Transportation Security Administration
TSGP	Transit Security Grant Program
TSP	Trucking Security Program
U.S.	United States
UASI	Urban Area Security Initiative
US&R	Urban Search and Rescue
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) published the National Infrastructure Protection Plan (NIPP) to define roles, responsibilities and procedures for protecting the nation's critical infrastructure and key resources (CI/KR). The NIPP provides guidance and direction to federal, state and local agencies to prepare Critical Infrastructure Protection Programs (CIPP), in conjunction with private owners and operators of critical assets, to mitigate and protect against man-made and natural hazards.

This San Diego Operational Area (OA) Critical Infrastructure Protection (CIP) Plan was initiated to establish a CIPP framework within the San Diego OA. The CIP Plan provides a methodology for evaluating CI/KR assets and acts as a decision making tool to support making informed financial investment decisions as they pertain to protecting the OA's critical assets.

Successful development and implementation of the San Diego CIPP requires coordination and input between many agencies and organizations across the OA. The process of preparing the CIP Plan began with an evaluation of how the 17 CI/KR Sectors are represented in the OA. (This plan was completed before DHS added the 18th Sector "Critical Manufacturing".) The process continued with the identification and consideration of the essential functions performed by each sector, the assets required to support those functions and the interdependencies between the essential functions to prepare a filtered list of prioritized critical assets.

The next step in CIP Plan development was the completion of an asset-level, all-hazards risk assessment on the prioritized list of critical assets. The methodology for this assessment was derived from a number of federal risk assessment methodologies to ensure compliance with DHS and NIPP requirements. The standard DHS formula calculates risk as the product of the consequence and the likelihood of an incident. In this instance likelihood is the combination of threat and vulnerability. The high-level all-hazard assessment generated consequence and likelihood scores for each asset. By plotting the scores for each asset, it was possible to divide the assets into multiple risk categories according to their overall risk profile.

This methodology provides the OA with a tool to monitor and track the success and effectiveness of the CIPP and their investment decisions. Effective investments will reduce the factors that comprise the risk profile, the result of which should be a migration of assets from higher to lower risk groups.

The long-term goal of the CIPP is to continue to increase the relevancy and accuracy of the decision making support provided by this CIP Plan by conducting more detailed risk assessments for particular man-made threat and natural hazards scenarios. The combination of detailed data from on-site inspections and conducting scenario based assessments will continue to enhance the effectiveness of the San Diego OA CIPP.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 1 INTRODUCTION

Over the last decade there have been multiple events that have drawn attention to the vulnerabilities and fragility of United States (U.S.) critical infrastructure and key resources (CI/KR). These events include the 2000 Y2K computer scare, the 2001 terrorist attacks on the World Trade Center, and the 2003 power outages of the northeast U.S.

The Homeland Security Act of 2002 defines critical infrastructure (CI) as; "*Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matter*s." The Act also defines key resources as; *"publicly or privately controlled resources essential to the minimal operations of the economy and government."* In the U.S., these critical systems, assets and resources support the everyday essential functions that without which would compromise national security, public health and safety, and economic vitality. To better classify the essential functions that CI/KR support, the Department of Homeland Security (DHS) has organized them into 17 sectors, including; Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Information Technology (IT), National Monuments and Icons, Nuclear Reactors, Materials, and Waste, Postal and Shipping, Public Health and Healthcare, Transportation Systems, and Water. This Plan was completed prior to DHS adding the 18th sector "Critical Manufacturing" future updates will include this sector.

Due to the daily reliance on CI/KR to maintain our current way of life, it is vital they are safeguarded and protected. In 2003 the President released the Homeland Security Presidential Directive 7 (HSPD-7), which outlines the need to identify, prioritize, and protect U.S. CI/KR. In response to HSPD-7, DHS developed the National Infrastructure Protection Plan (NIPP), which provides guidance to Federal, State, local and Tribal governments for developing CIP Programs (CIPP).

To protect national and economic security, public health and the current way of life, it is the shared responsibility of Federal, State, local and Tribal governments as well as the private sector, to mitigate threats, vulnerabilities, and consequences resulting from all hazards, including acts of terrorism as well as natural and man-made hazards, on the nation's CI/KR.

1.1 PURPOSE

The purpose of developing the San Diego Operational Area (OA) Critical Infrastructure Protection (CIP) Plan is to protect those regional assets that are essential to the OA's well-being and current way of life, from all hazards. The CIP Plan was developed in support of the OA CIPP. The CIP Plan was initiated to collect the necessary information to develop a justifiable investment strategy for the OA. This program included identifying sector specific essential functions, associated assets and the sector interdependencies of these assets as well as performing high level risk and vulnerabilities assessments on the identified CI/KR. The ultimate goal of the CIPP, and this Plan, is to reduce or eliminate the risks to the OA's CI/KR through a series of sequential steps designed to evaluate risks, vulnerabilities and consequences and implement protective measures.

The CIP Plan is not a response plan. The overall goal is to ensure that CI/KR is protected, prior to any event that may affect them, in an effort to lessen any effect from natural or man-made hazards. Therefore, it does not address response or recovery efforts when such assets are affected.

The lead agencies responsible for the development of the San Diego OA CIP Plan, is the County of San Diego (County) Office of Emergency Services (OES), the Sheriff's Regional Terrorism Threat Assessment Center (RTTAC) and the City of San Diego Office of Homeland Security (OHS). This Plan was designed to be a comprehensive and actionable CIP Plan that the OA can use to prioritize and protect assets. It identifies and synthesizes relevant guidance documents, best practices from other regional initiatives and input from local government and private owners/operators of the OA's CI/KR.

1.2 ASSUMPTIONS

The following assumptions were established in development of this Plan:

- The methodology used to develop this Plan and the investment strategy is based upon accepted DHS principles as well as previously completed plans and studies.
- This Plan was developed using an all-hazards approach, which includes assessment of natural and made-made disasters.
- This Plan's investment strategy was initially focused on public assets and not privately owned CI/KR.

1.3 APPLICABILITY

The goal of this Plan is to serve as a decision-making tool to support San Diego OA CIP policy and investment strategy development. It defines the processes for ensuring that the decision-makers have the necessary information to make judgments about protection. It also lays out the roles, responsibilities, and activities that need to be carried out to identify and prioritize CI/KR.

1.4 BACKGROUND AND CURRENT STATUS

This section provides background on how CIP is being addressed at both the Federal level and more locally within California and its regions, counties, and cities.

1.4.1 National CIP Efforts and Drivers

The Federal CIP effort is led by DHS, and consists of a sector-based approach for protecting CI/KR through a risk management process. The responsibility of protecting the nation's CI/KR was assigned to DHS by the Homeland Security Act of 2002. In 2003, the President issued HSPD-7 which designated DHS with the task of developing a comprehensive national plan for securing CI/KR. HSPD-7 also lists the specific Federal departments and agencies that are responsible for protection activities in the 17 CI/KR sectors.

In 2006, DHS released the NIPP which provides direction for implementing a coordinated national CIP effort. The NIPP details a sector-based approach for identifying and prioritizing critical assets, assessing vulnerabilities, and implementing protection measures within and across infrastructure sectors. The NIPP also delineates roles and responsibilities for carrying out these activities among Federal, State, local, Tribal, and private sector stakeholders.

1.4.2 State Efforts

The California Office of Homeland Security (OHS) has become the lead agency tasked with the identification, prioritization, and protection of the state's wide range of CI/KR. The State has worked extensively to build relationships with key partners and stakeholders including; site owners and operators, first responders, public and private organizations and associations, and other levels of government, in an effort to enhance protection of its CI/KR.

1.4.3 Relationship of this Plan to Other CIP Efforts

While there are multiple guidance documents from DHS, Federal Emergency Management Administration (FEMA) and the Department of Defense (DoD) for performing detailed vulnerability and risk assessments for specific assets, there is no comprehensive guidance for creating a regional CI/KR prioritization and investment strategy. This Plan is designed to aid the San Diego OA in protecting regional CI/KR by providing a comprehensive and actionable CIP Plan that the OA can use to prioritize and protect assets. This Plan supports both National and State CIP efforts. The San Diego OA CIP Plan is not intended to supersede other CIP strategies. The processes and methodologies described in this Plan were developed to bring together partners within the OA who have a common goal of maintaining the Region's way of life. No one plan can address the entire range of threats and vulnerabilities facing the nation's CI, however, this Plan's investment strategy provides a sound foundation for prioritizing and protecting the region's CI by reducing overall vulnerabilities and improving protection capabilities.

1.5 AUTHORITIES

The following plans and statutes are applicable to the CIP Plan:

- Federal
  - *Homeland Security Act of 2002*
  - *Homeland Security Presidential Directive 7*, 2003
  - *Guidance for Developing Sector-Specific Plans*, April 2004
  - *National Critical Infrastructure Protection Plan*, 2006
  - *Agriculture and Food Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Chemical Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Commercial Facilities Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Communications Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Dams Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Emergency Services Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Energy Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Government Facilities Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
  - *Information Technology Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007

- *National Monuments and Icons Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
- *Nuclear Reactors, materials and Waste Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
- *Postal and Shipping Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
- *Public Health and Healthcare Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
- *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007
- *Water Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007

- Local
  - *Operational Area Emergency Plan*, Unified San Diego County Emergency Services Organization, September 2006
  - *San Diego County Multi-Jurisdictional Hazard Mitigation Plan*, March 2004
  - *San Diego Operational Area Critical Infrastructure Protection Plan Risk Assessment*, 2008
  - *San Diego Urban Area Security Strategy*, City of San Diego Office of Homeland Security, June 2003
- Other
  - *Critical Infrastructure Protection Plan*, Washington State Homeland Security Region 6, September 2005

1.6 INFORMATION SECURITY/SHARING

It is vital for the success of the CIPP that there is active participation of all CI owners, including government and private owners. This participation and partnership cannot be advanced without a multi-directional information sharing network. County OES is committed to protecting the sensitive information that asset owner/operators provide for CIP investment strategy development.

To properly protect the information contained in the confidential *San Diego Operational Area Critical Infrastructure Protection Plan Risk Assessment*, 2008, it was certified as Protected Critical Infrastructure Information (PCII). The PCII Program, developed by DHS, is an information-protection program that enhances information sharing between the private sector and the government.

The PCII Program's safeguards ensure that specific information pertaining to CI/KR assets is:

- only accessed by authorized and properly trained individuals,
- properly marked as PCII,
- used appropriately for threat analysis, vulnerabilities and other homeland security purposes,
- protected from disclosure under the Freedom of Information Act and similar state and local disclosure laws, and,
- not used directly in civil litigation. [1]

The confidential *San Diego Operational Area Critical Infrastructure Protection Plan Risk Assessment*, 2008, was only distributed to those in the Steering Committee who were PCII certified.

[1] http://www.dhs.gov/xinfoshare/programs/gc_1193088517704.shtm

SECTION 2 ROLES AND RESPONSIBILITIES

2.1 OPERATIONAL AREA CIP DECISION-MAKING ENTITIES

The development of a justifiable investment strategy is a multi-step process that requires the participation and input of many experts.

The key to successful CIP planning is the utilization of region-wide coordination. The development of the CIP Plan was initiated through the implementation of the CIPP with the goal of fostering interagency coordination. The CIPP solicited information from the region's subject matter experts and stakeholders. To obtain the necessary information from these individuals there were multiple committees dedicated to identifying CI/KR within the OA and their associated risks and vulnerabilities. The two committees collaborating to develop the CIP Plan were the Stakeholders Committee and the Steering Committee. These committees were asked to provide oversight and recommendations on the development of this Plan.

2.1.1 Stakeholders Committee

The CIP Stakeholders Committee meeting was conducted to acquire corroboration on the program's vision, short- and long-term goals, and assumptions that were created based on best practices and previous CIP efforts. The CIP Stakeholders Committee consisted of representatives from the following agencies:

- City of Carlsbad Emergency Preparedness
- City of Carlsbad Police Department
- City of Escondido Fire Department
- City of Escondido Police Department
- City of National City Fire Department
- City of San Diego Fire Department
- City of San Diego Office of Homeland Security
- City of San Marcos Emergency Management
- City of Santee Fire Department
- County Hazardous Emergency Response Team
- County OES
- San Diego Federal Bureau of Investigation (FBI) – Joint Terrorism Task Force (JTTF)
- Sheriff's RTTAC
- U.S. DHS
- State of California OHS

2.1.2 Steering Committee

Members of the Stakeholders Committee with a solid understanding of the functions performed in one or more of the 17 infrastructure sectors were asked to volunteer to participate in the Steering Committee. The Steering Committee was a smaller group created to be involved in the decision-making of some of the more intricate details of the Plan. The Steering Committee included representatives from the following agencies:

- City of San Diego Fire Department
- City of San Diego Office of Homeland Security
- City of San Diego Police Department
- County Geographic Information Systems (GIS)
- County OES
- Sheriff's RTTAC
- State of California Office of Homeland Security

2.2 LOCAL, STATE, AND FEDERAL GOVERNMENTS

Protection of the nation's CI/KR and implementation of an effective CIPP requires participation at all levels of government. It is necessary that Federal, State and local governments are simultaneously working to ensure the security and stability of those assets identified as critical.

A responsibility that is inclusive to all levels of government is the identification of CI/KR at their level of government. The Federal government must identify those Federal assets that are critical and State, local governments must also do the same.

The responsibilities specific to each level of government include:

- Federal: It is the responsibility of the Federal Government to provide guidance for the development of an effective CIPP. Specifically, DHS is responsible for managing the Nation's overall CIP framework and overseeing NIPP development and implementation.

- State: It is the responsibility of the State to provide funding to local governments to assist in the CIPP development process.

- Local: It is the responsibility of local governments to develop and implement a CIPP as a part of their comprehensive homeland security program.

2.3 OWNERS/OPERATORS

An estimated 85 percent of the Nation's CI is owned by the private sector[2]. With no single, all-inclusive program managing both publicly and privately owned assets, the task of protecting the large majority of CI owned by the private sector is daunting. As a result, it is vital that the public and private sectors work

[2] United States Government Accountability Agency, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, October 2006.

together to protect these assets. As principal providers of essential goods and services, it is the responsibility of private owners/operators to ensure their own security. It is also the responsibility of private sector owners/operators to provide advice, recommendations, and subject matter expertise to the various levels of government involved in protecting the nation's CI/KR assets.

This Plan primarily addresses government and public assets, future efforts should include the involvement of private asset owners.

2.4 PAST EFFORTS

2.4.1 San Diego Urban Area Security Strategy

The San Diego Urban Area Security Strategy was released in 2003 and provided a framework and strategic direction for all jurisdictions within the County to enhance preparedness, improve response and recovery capabilities, and increase the area's capacity to prevent or reduce vulnerabilities and associated impacts resulting from a terrorist attack including the use of a weapon of mass destruction. The 2003 Urban Area Security Initiative (UASI) strategy development process included an OA risk assessment, including CI and other target ranking with a basic vulnerability assessment, and an in-depth needs examination using a weighted gap analysis model incorporating the principles of cost-benefit analysis.

The information gathered from the 2003 UASI effort was utilized to assist in the San Diego OA CIP Plan.

2.4.2 Buffer Zone Protection Program

The Buffer Zone Protection Program (BZPP), funded by DHS has increased the CIP capability of the OA in the past. BZPP assessment teams work closely with the private sector to identify security gaps and make recommendations for security enhancements. The BZPP program has been coordinated with the implementation and adoption of the State of California Automated Critical Asset Management System (ACAMS).

2.4.3 Hazard Mitigation Plan

The *County of San Diego Multi-Jurisdictional Hazard Mitigation Plan* released in 2004, identifies the hazards which assets in the OA are susceptible too. The information in the Hazard Mitigation Plan was used to determine the threat or susceptibility of the OA's CI/KR to natural hazards based upon the asset's location in the region.

2.4.4 InfraGard

InfraGard, operated by the FBI, is an information sharing association that includes businesses, academic institutions, state and local law enforcement agencies, and other participants. This association engages stakeholders that are committed to sharing information and intelligence to protect CI from both physical and cyber threats. This effort is designed to share and combine the knowledge base of a wide range of members.

The San Diego InfraGard Chapter engages OA Stakeholders in information sharing that assists in the protection of the region's CI/KR and consists of members from the 17 sectors, defined by DHS, from within the region.

SECTION 3 IDENTIFYING CRITICAL ASSETS

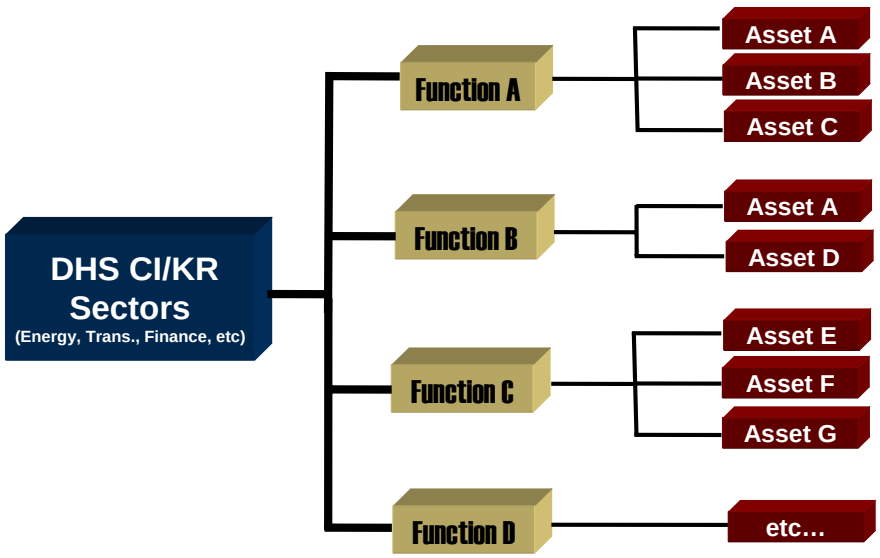
The first step in the development of a justifiable CIP investment strategy was the identification and prioritization of the CI/KR within the region. Not all assets are critical and not all CI/KR have the same consequence. To adequately address CIP and determine critical assets, there had to first be a thorough understanding of how the 17 CI/KR sectors were represented in San Diego OA, the interdependencies between them, the essential functions of each sector and a clear definition of what is considered to be a CI/KR. For this plan, CI/KR is an asset within the region that supports an essential function of one or more of the 17 CI/KR sectors. Once each of these was identified, an initial list of CI/KR in the OA could be developed.

3.1 DEVELOP THE INITIAL LIST OF ASSETS

Developing the list of assets began by reviewing how the 17 Sectors are represented in the OA. The Sector Specific Plans (SSPs) were reviewed to identify the general functions and operational requirements for each sector, the most important of these were considered the "essential functions". The essential functions and assets required to support those functions were identified by the project team through a review of previous Federal, State, and local assessments and asset lists, presented to the Steering Committee and discussed in more detail during interviews with local representatives from each of the applicable sectors. During these interviews, the draft list of assets required to support the essential functions of each sector was reviewed and updated. This process prepared the initial list of assets based upon their actual support of the OA's essential functions. The initial list of assets will be used to establish a baseline for the risk methodology with additional assets to be added in the future.

Figure 3-1 illustrates the overall process of mapping the sectors, essential functions and CI/KR assets. For example, the transportation sector has functions such as highway, air, rail, maritime, etc. Within each function are specific assets that help it to operate. For example, the function highway transportation may have assets such as tunnels, bridges, interchanges and overpasses. The goal of this process and the interviews with sector representatives was to determine which sectors, functions, and assets are essential to the San Diego OA.

Figure 3-1. DHS Sector to Asset Mapping



The first step in the process was to map the sectors to their respective functions. The next step of the process was to map assets, identified through a review of previous assessments, to their respective functions. This step produced upwards of 1,000 assets. The assessment team then scheduled meetings with representatives from each of the sectors to assist with filtering the list of assets down to a more manageable level. The initial asset selection process is subjective, based on the experience and knowledge of identified sector representatives. These representatives helped to identify specific assets or determine criteria that may assist with identifying the most critical assets. There was no predetermined number of assets within each sector that was desired; however, the assessment team attempted to limit the initial list of assets to approximately 100 assets and will continue to add assets in the future.

There were 107 assets upon completion of the filtering process. These assets served as the baseline to perform detailed consequence, threat and vulnerability assessments, all of which feed into the overall risk profile for the region.

Table 3-1 below provides a summary of the functions identified for the 17 CI/KR sectors as well as the asset selection rationale that was determined based on Steering Committee and sector representatives' input, and used to develop the initial list of CI/KR assets in the OA. The table below also identifies how many of the 107 assets per sector were identified on the initial list of assets. Section 3.2 Detailed Sector Specific Information provides a detailed description of each of the 17 CI/KR sectors as described in the SSPs as well as a description of the sector's role in the OA.

This assessment was completed prior to DHS adding the 18th sector "Critical Manufacturing" future updates will include assets from this sector.

Table 3-1 DHS Sector Function and Asset Selection Rationale

#	DHS Sectors	Functions	Asset Selection Rationale
1	**Agriculture and Food**	• Supply Chains • Process, Packaging, Production • Storage • Transportation, Distribution • Supporting Facilities	N/A –It was noted that the system itself could be used to stage and attack that may affect may people; however, sector representatives did not feel that any single asset within this sector was highly critical. No assets were identified in this sector on the initial OA CI/KR list.
2	**Banking And Finance**	• Banking and Credit • Securities and Commodities	N/A – It was determined that most of the highly critical assets within this sector are located in other cities. In addition, banking and finance's physical assets are highly redundant and the infrastructure that allows it to operate resides predominately within the communications and information technology sectors. No assets were identified in this sector on the initial OA CI/KR list.

Table 3-1 DHS Sector Function and Asset Selection Rationale

#	DHS Sectors	Functions	Asset Selection Rationale
3	**Chemical**	• Basic Chemicals • Specialty Chemicals • Life Sciences • Consumer Products.	These assets were primarily chosen based upon recommendations from the sector representatives using onsite quantities of hazardous materials and "worst case" scenario release studies from the *San Diego County Multi-Jurisdictional Hazard Mitigation Plan* (2004) as the primary criteria. No assets were identified in this sector on the initial OA CI/KR list. Due to dual functions of these assets, assets identified in this sector were included in other sector lists.
4	**Commercial Facilities**	• Public Assembly • Sports Leagues • Resorts • Lodging • Outdoor Events • Entertainment and Media • Real Estate • Retail	These assets were chosen based upon recommendations from the Steering Committee and the selections were based primarily on those assets that have high site population, visibility, or are otherwise well-known in the San Diego region. 17 assets were identified in this sector on the initial OA CI/KR list.
5	**Communications**	• Wireless • Satellite • Cablewire • Broadcast - Radio Towers • Broadcast - TV Towers	The assessment team met with a number of representatives from this sector, but was unable to determine the most critical assets. A list of communications assets were added that were referenced in a number of the other sector specific meetings as critical. Ten assets were identified in this sector on the initial OA CI/KR list.
6	**Dams**	• Dams • Mine Tailing • Hurricane Barriers • River Control Structures • Levees	Dams with the highest inundation zone casualties were chosen as well as those dams that consistently appeared on federal, state, or local critical asset lists. Nine assets were identified in this sector on the initial OA CI/KR list.
7	**Defense Industrial Base**	• Shipbuilding • Aircraft • Combat Vehicle • Ammunition • Weapons	The assessment team did not meet with representatives from this sector. A review of previous assessments concluded that these assets consistently appeared on federal, state, and local critical asset lists. Four assets were identified in this sector on the initial OA CI/KR list.

Table 3-1 DHS Sector Function and Asset Selection Rationale

#	DHS Sectors	Functions	Asset Selection Rationale
8	**Emergency Services**	• Law Enforcement • Emergency Medical Services • Fire and Rescue • Emergency Management	San Diego region law enforcement and fire department representatives agreed that major dispatch centers and other law enforcement and fire facilities are highly critical emergency services assets and should be included. 15 assets were identified in this sector on the initial OA CI/KR list.
9	**Energy**	• Electricity Petroleum • Natural Gas	The assessment team did not meet with representatives from this sector. A review of previous assessments concluded that these assets consistently appeared on federal, state, and local critical asset lists. Six assets were identified in this sector on the initial OA CI/KR list.
10	**Government Facilities**	• Personnel-Oriented Facilities • Government Research • Sensor and Monitoring • Other	These assets were added based upon the recommendation from the Steering Committee, which is made up law enforcement, fire, and city representatives. No criteria for the selections were mentioned. Four assets were identified in this sector on the initial OA CI/KR list.
11	**Information Technology**	• Domain Name Operators • Internet Service Providers • Internet Backbone Providers • Internet Portal and Email Providers • Computer Hardware Companies • Computer Software Companies • Security Service Vendors	N/A – It was determined that most of the highly critical assets within this sector are located in other cities. In addition, the assessment team was not able to determine any critical information. No assets were identified in this sector on the initial OA CI/KR list.

Table 3-1 DHS Sector Function and Asset Selection Rationale

#	DHS Sectors	Functions	Asset Selection Rationale
12	**National Monuments and Icons**	• Structures • Geographic Areas	N/A – San Diego has a number of regionally recognized icons and monuments, but it was determined that most of the nationally recognizable assets within this sector are located in other cities. No assets were identified in this sector on the initial OA CI/KR list.
13	**Nuclear Reactors, Materials and Waste**	• Nuclear Power Plants • Non-Power Nuclear Reactors (research, testing, training) • Nuclear Material (medical, industrial, academic) • Waste Management • Nuclear Fuel Fabrication Facilities	There was only one asset within the San Diego region that represents this sector and was added to the list. One asset was identified in this sector on the initial OA CI/KR list.
14	**Postal and Shipping**	• High-volume Automated Processing Facilities • Local Delivery Units • Collection, Acceptance, and Retail Operations	The assessment team did not meet with representatives from this sector. The assets within this sector were chosen based on the recommendation from the Steering Committee. Two assets were identified in this sector on the initial OA CI/KR list.
15	**Public Health and Healthcare**	• Routine and Emergency Healthcare Facilities • Short and Long Term Healthcare Facilities for Special Needs Populations • Public Health Assistance Facilities • Disease Testing and Surveillance Facilities • Vaccination and Immunization Facilities • Stockpile Facilities	The assets in this sector were chosen because they were main facilities that serve as communication nodes for other healthcare facilities or provided unique healthcare services in the OA. This criterion was based on the recommendation of sector representatives. Nine assets were identified in this sector on the initial OA CI/KR list.

Table 3-1 DHS Sector Function and Asset Selection Rationale

#	DHS Sectors	Functions	Asset Selection Rationale
16	**Transportation Systems**	• Aviation • Highway • Maritime • Mass Transit • Freight Rail • Commuter Rail - Heavy • Commuter Rail - Light • Maritime • Pipeline Systems (Non-Energy, Non-Water)	A review of previous assessments concluded that these assets consistently appeared on federal, state, and local critical asset lists. The interchanges listed in this sector were chosen based upon Average Annual Daily Traffic (AADT). This criterion was based on the recommendation of sector representatives. 21 assets were identified in this sector on the initial OA CI/KR list.
17	**Water**	• Water Distribution Facilities • Wastewater Facilities	A review of previous assessments concluded that these assets consistently appeared on federal, state, and local critical asset lists. In addition, some of the assets in this sector were added based upon the recommendation of sector representatives. Nine assets were identified in this sector on the initial OA CI/KR list.
18	**Critical Manufacturing**	• This sector was added after this assessment was completed. Future updates will include assets from this sector.	This sector was added after this assessment was completed. Future updates will include assets from this sector. No assets were identified in this sector on the initial OA CI/KR list.

3.2 DETAILED SECTOR-SPECIFIC INFORMATION

3.2.1 Agriculture and Food Sector

The Agriculture and Food CI SSP, released in 2007, is divided into two separate plans, one developed by the U.S. Department of Agriculture (USDA) and the other developed by the U.S. Food and Drug Administration (FDA).

The SSP developed by the USDA, focuses on food (Meat, Poultry, and Egg Products) and agriculture. The essential functions described in the *Agriculture and Food Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, include; complete post-harvesting components of the food supply chain including: processing, production, packaging, storage, distribution to retail sales, institutional food services, and for restaurant or home consumption; and complete supply chains for: feed, animals, animal products, crop production, seed, and fertilizer.

The SSP developed by the FDA focuses on the essential functions required to regulate the following five program areas; human drugs, devices, biologics, food and cosmetics, and animal drugs and feeds.

The Agriculture and Food Sector is an important part of the County's economy. As the 20th largest agriculture producer in the nation, the County's main crops include avocados, exotic flowers and nursery and decorative plants. The County also has the second largest number of farms in the nation.[3] According to the County of San Diego Department of Agriculture, Weights and Measures:

> San Diego County's unique topography creates a wide variety of microclimates resulting in nearly 30 different types of vegetation communities. This diversity allows San Diego farmers to grow over 200 different agricultural commodities - from strawberries along the coast, apples in the mountain areas, and to palm trees in the desert. The success of San Diego County's diverse agricultural industry is reflected in the 47 commercial crops with a value of over $1 million.[4]

Within the County there is not only an agricultural presence of this sector, but there is also a large section of biomedical research and production. According to the San Diego Regional Chamber of Commerce: "San Diego County has many notable medical research institutions within its borders, and a variety of significant biomedical and biotechnological developments have emerged from these facilities. With more than 32,000 biotech jobs in 499 companies, San Diego has the third largest concentration of biotech companies of all U.S. metropolitan areas."[5]

3.2.2 Banking and Finance Sector

The Banking and Finance SSP, released in 2007, was developed by the Department of Treasury. The Banking and Finance Sector is complex with a large amount of diversity which allows the sector to meet the needs of its large and assorted client base. The diversity also allows for high levels of redundancy among assets in the sector.

The *Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan,* 2007, defines the essential functions of the sector to be:

- Deposit;
- Consumer credit, and payment systems;
- Credit and liquidity products;
- Investment products; and.
- Risk-transfer products (including insurance).

Each of these essential functions is vital to the U.S. economy. Deposit, consumer credit and payment systems allow consumers to utilize such functions as wire transfers, checking accounts, and credit and debit cards. This function also allows consumers to have access to mortgages and home equity loans; collateralized and uncollateralized loans; and lines of credit. Credit and liquidity products allow customers to have access to liquidity and credit for a wide variety of needs. Some of those needs include a mortgage, a business line of credit, and governments may issue sovereign debt obligations. Investment

[3] http://www.sdchamber.org/
[4] http://www.sdcounty.ca.gov/reusable_components/images/awm/Docs/stats_cr2006.pdf
[5] http://www.sdchamber.org/

products provide for a strong investment setting which is essential to the growth of the U.S. economy. Risk transfer products, including insurance, includes the transfer of financial risks, such as the financial loss due to theft or the destruction of physical or electronic property.

In the County the Banking and Finance Sector mainly consists of local branches of national and local banks as well as local credit unions. Within the San Diego OA there are no Federal or State financial institutions and there is significant redundancy among the local assets.

3.2.3 Chemical Sector

The Chemical SSP, released in 2007, was developed primarily by DHS, the Environmental Protection Agency (EPA), and the FBI. These entities, as well as many other members, are represented on the Chemical Government Coordinating Council (GCC), which is chaired by DHS. The *Chemical Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, describes the Chemical Sector as;

> A fundamental element of the U.S. economy by converting various raw materials into more than 70,000 diverse products, many of which are critical to the health and well-being of the Nation's citizenry, security, and economy. Many of the other sectors are extremely reliant of the Chemical Sector.
>
> The Chemical Sector essential functions described in the SSP, include the following activities; design, manufacturing, marketing, distribution, transportation, customer support, use, recycling, and disposal of chemical products.
>
> There are a vast amount of facilities in the U.S. that in some way use, manufacture, store, transport, or deliver chemicals. These facilities can include everything from petroleum refineries to pharmaceutical manufacturers to hardware stores. The facilities that make up the Chemical Sector typically belong to one of three key functional areas in the Chemical Sector value chain: (1) manufacturing plants, (2) transport systems, and (3) distribution systems (including storage/stockpile/supply areas).

There are a wide variety of facilities in the County that contribute to the Chemical Sector, which include both public agencies and private companies. One of the main contributors to the Chemical Sector, in the County, is the many pharmaceutical manufacturing facilities that have been developed as part of the large biomedical presence in the region. Due to many sectors' reliance on chemicals for everyday functioning, numerous assets in the Chemical Sector have dual functions and can also be included in other sectors, i.e., water treatment facilities.

3.2.4 Commercial Facilities Sector

The Commercial Facilities SSP, released in 2007 was developed by the Department of Treasury. The *Commercial Facilities Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, describes the Commercial Facilities Sector as;

> In the Commercial Facilities Sector, the Federal security partners include the DHS and its many organizations, the EPA, the FBI, and the Department of Commerce (DOC). The Commercial Facilities Sector is a key resources sector which includes assets where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes. The assets that make up this sector are divided into eight sub-sectors: Entertainment and Media (e.g., motion picture studios,

> broadcast and print media); Lodging (e.g., hotels, motels, conference centers); Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades); Public Assembly (e.g., arenas, stadiums, convention centers, performing arts centers, aquariums, zoos); Real Estate (e.g., office and apartment buildings, condominiums, self-storage); Resorts (e.g., casinos); Retail (e.g., retail centers and districts, shopping malls); and Sports Leagues (e.g., professional sports leagues and federations).

In the County the Commercial Facilities Sector plays a vital role to the local economy. Tourism is one of the most important industries in the region, and therefore must be supported with sufficient lodging and entertainment to support the demand. The San Diego regional Chamber of Commerce states that:

> San Diego is considered one of the most desirable year-round vacation spots in the nation, and it is regularly ranked in the top ten most popular destinations in the continental U.S. for international visitors. Despite a worldwide downturn in the tourism industry and especially in air travelers, San Diego successfully targeted several West Coast drive-in markets, bringing more regional vacationers to the area. In 2001 total revenue from visitors topped $5.1 billion. As a result, service industries have seen continued growth in past years, specifically in areas such as dining, lodging, shopping and recreation services.[6]

3.2.5 Communications Sector

The Communications SSP, released in 2007 was developed by the National Communications System, within DHS. The essential functions for the Communications Sector identified in the *Communications Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, include;

> Provide communications infrastructure, wireline, wireless, satellite, cable, and broadcasting capabilities, and the transport networks that support the Internet and other key information systems; provide voice and data service to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks.
>
> Relationships in the Communications Sector span a magnitude of private sector, government, and international organizations. The communications infrastructure is a complex system of systems that incorporates multiple technologies and services with diverse ownership. The infrastructure includes wireline, wireless, satellite, cable, and broadcasting, and provides the transport networks that support the Internet and other key information systems. The resiliency built into the communications infrastructure increases the availability of service to its customers and reduces the impact of outages. The sector mitigates cascading effects of incidents by designing and building resilient and redundant communications systems and networks to ensure disruptions remain largely localized and do not affect the national communications backbone.

In the County the Communications Sector is vital to the region's way-of-life and consists of both public and private providers. The majority of industries and agencies within the region are reliant on both the public and private providers to maintain a consistent level of communication.

[6] http://www.sdchamber.org/

Some of the customers within the County which are dependent on the Communications Sector include: Public Safety which relies on radio systems to communicate within the region as well as with State and Federal agencies; local media networks which rely on cable, broadcasting capabilities, and satellite infrastructure to function; and the public which are dependent on landline and wireless telephone services for everyday communication.

3.2.6 Dams Sector

The Dams SSP, released in 2007 was developed by the Office of Infrastructure Protection (OIP), a component of the DHS National Protection and Programs Directorate. The *Dams Critical Infrastructure and Key Resources Sector-Specific Plan,* 2007, describes the sector as;

> A key resources sector which includes assets that provide a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.
>
> The Dams Sector comprises the assets, systems, networks, and functions related to dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, or other similar water retention and/or control facilities. Dam projects are complex facilities that typically include water impoundment or control structures, reservoirs, spillways, outlet works, powerhouses, and canals or aqueducts. In some cases, navigation locks are also part of the dam project. Some larger or more symbolic dams are major components of other critical infrastructure systems that provide water and electricity to large populations, cities, and agricultural complexes

In the County the Dams Sector plays an important role in the collection and storage of local water resources for the region. Due to the variable and often limited rain-fall within the region, San Diego relies heavily on water imported from outside sources. Within the County there are many dams owned and operated by both the private and public sectors, these dams provide for the collection, storage and distribution of local water to residents throughout the region. These dams can also be used as back-up water storage which can be distributed in the event that outside water sources are unavailable.

The many dams in the County also provide the region with recreational uses such as fishing, boating and camping.

3.2.7 Defense Industrial Base Sector

The Defense Industrial Base SSP, released in 2007 was developed by the Department of Defense. The *Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan,* 2007, describes the sector as;

> Unlike other infrastructure sectors, the Defense Industrial Base is defined not based primarily on the type of goods and services it produces, but rather on who the customer is for these goods and services. It includes companies performing under direct contract with DoD, their subcontractors, and companies providing incidental materials and services to either. It ranges across all sectors and sub-sectors of the industrial landscape, includes services as well as products, and varies from one-person or family-owned businesses to the largest corporations in the world.

> The Defense Industrial Base is an extraordinarily large, diverse, complex, interdependent, independent, hierarchical, and free-flowing collection of asset owner/operators governed by varying regulations, laws, treaties, and precedents. DoD and DOC estimate that the Defense Industrial Base is composed of hundreds of thousands of worldwide government and private sector sites, with capabilities to perform research and development, design, produce, and maintain military weapons systems, subsystems, components, or parts to meet military requirements .

The County has a large Military presence with multiple Navy and Marine Corps installations as well as many Federal defense contractors located in the region. There are approximately 120,000 active duty personnel living in San Diego, an additional 129,000 family members, 57,900 retired military personnel and 22,500 Department of Defense civilian personnel.[7] The assessment team did not meet with representatives from this sector. A review of previous assessments concluded that these assets consistently appeared on federal, state, and local critical asset lists, and thus are not further evaluated in this Plan.

3.2.8 Emergency Services Sector

The Emergency Services SSP, released in 2007 was developed by OIP. The assets for the Emergency Services Sector include: fire, rescue, emergency medical services, and law enforcement resources and personnel that are called upon to save lives and property in the event of an accident, natural disaster, or terrorist incident

The essential functions identified in the *Emergency Services Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, include:

> Law Enforcement, maintaining law and order and protecting the general public from harm; Bomb Explosive Ordinance Disposal, conducting searches to locate hidden bombs, investigating suspicious packages, and if necessary, rendering safe any bombs and ensuring safe disposal; Special Weapons and Tactics (SWAT) and Tactical Operations, responding to highly dangerous and critical incidents, and engaging in high-risk services; Firefighting, minimizing loss of life and property during incidents from fire, medical emergencies, and other all-hazards events; Emergency Medical Service (EMS), providing medical care and assistance at the scene of an incident and during transport and delivery of injured personnel to a hospital; Search and Rescue (SAR), locating persons beloved to be in distress (e.g., lost, sick, injured) in remote or difficult-to-access areas (e.g., mountains, deserts, forests, sea); Urban Search and Rescue (US&R), locating, rescuing (extricating), and medically stabilizing victims trapped in confined spaces and collapsed buildings; Emergency Management (EM), leading efforts to prepare for, respond to, and recover from all types of incidents; Hazardous Materials (HAZMAT) Response, recognizing and responding to weapons of mass destruction incidents, establishing mass decontamination sites, and protecting the public, the environment, and property during incidents involving real or potential release if hazardous materials.

Within the County there are 18 incorporated jurisdictions, each of these jurisdictions as well as the County, coordinate emergency services separately. Due to this, there are many emergency services agencies throughout the County, including multiple law enforcement and fire departments. In addition to local emergency services, there are also State agencies within the County, including California Highway Patrol.

[7] http://www.navynews.com/military.htm

3.2.9 Energy Sector

The Energy SSP, released in 2007 was developed by the Department of Energy. The Energy Sector is divided into two separate sub-sectors; electricity and oil and natural gas. The essential functions identified in the Energy SSP includes; production, refining, storage, and distribution of oil and gas, and electrical power (except for commercial nuclear power facilities). The *Energy Critical Infrastructure and Key Resources Sector-Specific Plan, 2007*, describes the sector as:

> Energy assets and critical infrastructure components are owned by private, Federal, State, and local entities, as well as by some types of energy consumers, such as large industries and financial institutions (often for backup power purposes).
>
> The electricity portion of the Energy Sector includes the generation, transmission, and distribution of electricity. The use of electricity is ubiquitous, spanning all sectors of the U.S. economy. Electric generation accounted for 40 percent of all energy consumed in the U.S. in 2005. Although there are some significant regional differences, more than 98 percent of electricity is generated domestically, though some of the fuels used to generate electricity are imported.
>
> Electricity system facilities are dispersed throughout the North American continent. Although most assets are privately owned, no single organization represents the interests of the entire sector.

The County Energy Sector provides a basic utility that is a necessity to the entire region. There are many types of energy producing facilities in the County, the majority of which are privately owned, including; wind, oil/gas, hydroelectric, and water-to-energy facilities.

3.2.10 Government Facilities Sector

The Government Facilities SSP, released in 2007 was developed by the by DHS, Immigration and Customs Enforcement, and Federal Protective Service in coordination with the Government Facilities GCC.

The *Government Facilities Critical Infrastructure and Key Resources Sector-Specific Plan, 2007*, describes the sector as:

> The Government Facilities Sector includes a wide variety of facilities owned or leased by Federal, State, Territorial, local, or tribal governments, located domestically and overseas. Although some types of government facilities are exclusive to the Government Facilities Sector, government facilities also exist in most other sectors. Many are open to the public for business activities, commercial transactions, provision of services, or recreational activities. These types of facilities include: Offices and office building complexes; Housing for government employees; Correctional facilities; Embassies, consulates, and border facilities; Education facilities; Courthouses; Maintenance and repair shops; and Libraries and archives. Other facilities not open to the public contain highly sensitive information, materials, processes, and equipment. These types of facilities include: Research and development facilities; Military installations; Record centers; Space exploration facilities; Sensor and monitoring systems; Storage facilities for weapons and ammunition, precious metals, currency, and special nuclear materials and waste; and Warehouses used to store property and equipment.

In the County the Government Facilities Sector plays an important role in everyday operations. Each of the 18 incorporated jurisdictions as well as the County maintains the typical government facilities including; civic centers, law enforcement offices, fire department, correctional facilities, and all other facilities necessary for local government operation. In addition to the local government facilities there are multiple Navy and Marine installations within the region that are addressed as part of the Defense Industrial Base Sector.

3.2.11 Information Technology Sector

The Information Technology (IT) SSP, released in 2007, collaboratively developed by DHS' National Cyber Security Division as the Sector Specific Agency (SSA) for the IT Sector and sector security partners, including the IT Sector Coordinating Council and IT GCC.

The *Information Technology Critical Infrastructure and Key Resources Sector-Specific Plan, 2007*, defines the essential functions of the sector to be:

> The six essential functions identified for the IT Sector in SSP include: provide IT products and services; provide incident management capabilities; provide domain name resolution services; provide identity management and associated trust support services; provide Internet-based content, information, and communications services; and provide Internet routing, access and connection services.
>
> These functions are distributed across a broad network of infrastructure, managed on a proactive basis and therefore able to withstand and rapidly recover from most threats. These critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—who provide hardware, software, IT systems, and services. IT services include development, integration, operations, communications, and security. IT Sector entities include the following: Domain Name System root and Generic Top-Level Domain operators; Internet service providers (ISPs); Internet backbone providers; Internet portal and e-mail providers; Networking hardware companies (e.g., fiber-optics makers and line acceleration hardware manufacturers) and other hard-ware manufacturers (e.g., personal computer (PC) and server manufacturers and information storage); Software companies; Security services vendors; Communications companies that characterize themselves as having an IT role; Edge and core service providers; IT system integrators; and IT security associations. In addition, Federal, State, and local governments are a component of the IT Sector as providers of government IT services that are designed to meet the needs of citizens, businesses, and employees. The IT Sector includes public and private sector entities.

In the County the IT Sector is critical to the region's everyday activities and consists of both public and private providers. Due to the complexity of IT operations, some of the local governments in the OA, including the County, outsource to private companies. Within the region there are not only IT services providers but there are also large IT manufacturers which produce critical components to IT operations.

3.2.12 National Monuments and Icons Sector

The National Monuments and Icons SSP was released in 2007, and developed the U.S. Department of the Interior. The *National Monuments and Icons Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, describes the sector as: "comprises the diverse array of national monuments, symbols, and icons that represent our nation's heritage, traditions, values, and political power. This sector is considered to include any structure, system, or resource that has cultural, historic, psychological, or political significance at the local, regional, or national-level if compromised or destroyed."

San Diego has a number of regionally recognized icons and monuments, but it was determined that most of the nationally recognizable assets within this sector are located in other cities. Thus the Steering Committee chose not to further evaluate this sector in the OA.

3.2.13 Nuclear Reactors, Materials and Waste Sector

The Nuclear Reactors, Materials, and Waste Sector SSP was released in 2007, and was developed by OIP, Chemical and Nuclear Preparedness and Protection Division within DHS. The *Nuclear Reactors, Materials and Waste Critical Infrastructure and Key Resources Sector-Specific Plan, 2007*, describes the sector as: "The Nuclear Reactors, Materials and Waste Sector includes the nation's 104 commercial nuclear reactors in 31 states as well as: non-power nuclear reactors, used for research, testing, and training; nuclear materials in medical, industrial, and academic settings; facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste."

Within the County there is one commercial nuclear reactor which produces approximately 20% of the County's energy[8]. There are no other facilities in the region with a nuclear materials permit.

3.2.14 Postal and Shipping Sector

The Postal and Shipping SSP was released in 2007, and was developed by the Transportation Security Administration (TSA), in its role as the SSA. The *Postal and Shipping Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, describes the sector essential functions as:

> The Postal and Shipping Sector receives, processes, transports, and distributes billions of letters and parcels annually. Businesses, government, and individuals rely on the continuity and timely functioning of the sector to conduct vital, daily economic and personal transactions. A major disruption of the sector's ability to provide its services could have a sizable negative impact on the economy, business and government operations, and personal lives.

The Postal and Shipping Sector provides an important service to County operations. Within the County there are both public and private postal and shipping companies which provide services to local government, private business and the public.

[8] http://voiceofsandiego.org/articles/2007/12/03/news/01nuclear120307.txt

3.2.15 Public Health, and Healthcare Sector

The Public Health and Healthcare SSP was released in 2007, and was developed by the Department of Health and Human Services. *The Public Health and Healthcare Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007, describes the sector as:

> The sector provides a full array of goods and services for acute hospital and ambulatory healthcare, public health, public health information, mental health, substance abuse treatment, environmental and occupational health, long-term care, tele-health, pharmaceuticals, mortuary services, medical supplies, and others. Private sector as well as Federal, State, and local agencies provide healthcare and public health services, and participate in ongoing surveillance and detection of potentially devastating threats to the Nation's CI/KR from bioterrorism and other manmade and natural threats. In public health and medical emergencies, additional capabilities such as mass vaccination, mass casualty and mortality services, and medical surge involving additional numbers of ill, injured, or worried citizens must be efficiently coordinated within the sector to permit essential healthcare for the Nation.

In the County the Public Health and Healthcare Sector provides a vital service necessary for the continued operation of the County. Within the County there is a combination of public community and private public health and healthcare facilities and providers.

3.2.16 Transportation Systems Sector

The Transportation Systems SSP was released in 2007, and was developed by the DHS, including TSA, the U.S. Coast Guard (USCG), and Office of Grants and Training (G&T); Department of Transportation; Department of Justice, including the FBI; and the DoD.

The *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan, 2007*, describes the sector as:

> The Transportation Systems Sector—a sector that comprises all modes of transportation (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline)—is a vast, open, interdependent networked system that moves millions of passengers and millions of tons of goods. The transportation network is critical to the Nation's way of life and economic vitality. Ensuring its security is the mission charged to all sector partners, including government (Federal, State, regional, local, and tribal) and private industry stakeholders. Every day, the transportation network connects cities, manufacturers, and retailers, moving large volumes of goods and individuals through a complex network of approximately 4 million miles of roads and highways, more than 100,000 miles of rail, 600,000 bridges, more than 300 tunnels and numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports.

In the County, the Transportation Sector is a vital component of everyday life. The County's transportation systems are maintained by both public and private agencies. The highway sub-sector is particularly critical to the County due to the large geographic area of the region, and limited access to mass transit from all locations. The majority of the region's population travels by private vehicle, thus the highway systems are a significant asset to the OA.

3.2.17 Water Sector

The Water SSP was released in 2007, and was developed by the EPA. The W*ater Critical Infrastructure and Key Resources Sector-Specific Plan, 2007*, describes the sector as:

> The Water Sector consists of two basic, yet vital, components: drinking water supply and wastewater collection and treatment. Although it can be broken down into two basic components, the sector is successful through a complete integration of people, facilities, and cyber-based controls. On the supply side, the primary focus of critical infrastructure protection efforts is the Nation's 170,000 public water systems. These utilities depend on reservoirs, dams, wells, and aquifers; as well as holding, filtration, cleaning, and treatment facilities, pumping stations, aqueducts, cooling systems, transmission pipelines, and other delivery mechanisms that provide for domestic and industrial applications, including firefighting. The wastewater industry's emphasis is on the 19,500 municipal sanitary sewer systems, including an estimated 800,000 miles of sewer lines. Wastewater utilities collect and treat sewage and process water from domestic, commercial, and industrial sources. The Wastewater Sector also includes storm water systems that collect and sometimes treat storm water runoff.

In the County the Water Sector provides a critical service to the entire region. Within the County there are many different water authorities which are owned and operated by both the private and public sectors. Due to the variable and often limited rain-fall within the region, San Diego relies heavily on water imported from outside sources. The Metropolitan Water District of Southern California supplies most of the water to the region. The San Diego County Water Authority is the region's wholesale supplier of water to its 24 member agencies throughout the County. The 24 member agencies consist of local and federal government as well as private agencies.

3.3 INTERDEPENDENCY

It is not only important to determine the importance of the sectors individually, but it is also necessary to determine how the sectors interrelate and rely on the functions that the other sectors provide. Each of the sectors provide a vital service to the operation of everyday life in the OA, and are all interdependent on the other sectors to accomplish their essential functions. Certain assets may rely greatly on assets in other sectors and it is necessary to determine the level and extent of these interdependencies to truly determine which assets are critical in the OA.

To factor in the interdependencies of the OA assets, a system was developed to provide a weighted score for those assets within sectors in which many other sectors are highly dependent on. This scoring system is described in more detail in Section 4.1.3 Incorporate Interdependencies and Prioritize List. This system was developed to assist in identifying which assets are truly critical and which need to be protected most.

This identification of interdependencies allowed for the further prioritization of the initial list of 107 CI/KR in the OA by identifying the assets that provide a vital service or function to the other assets in the OA and that support essential functions across multiple sectors. The addition of interdependencies was necessary to differentiate the assets that may not be as critical in isolation but that support other assets to perform their essential functions.

SECTION 4 ASSESSMENT METHODOLOGY

The process used to evaluate risk for the San Diego OA CIP Plan was an asset-level all-hazards risk assessment and was derived from a number of Federal level risk assessment methodologies to ensure compliance with DHS guidance. These methodologies include:

- Maritime Assessment and Strategy Tool (MAST)
- Transit Risk Assessment Module (TRAM)
- Strategic Homeland Infrastructure Risk Assessment (SHIRA)
- Maritime Security Risk Analysis Model (MSRAM)
- A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection (AASTO Guide)
- A Guide to Physical Security Risk Management for Transportation Management Centers

The overall goal of the risk assessment was to provide a framework to gather information on identified CI/KR to help evaluate their relative risk and to identify physical security, response, or recovery needs within the region. The primary contributors to the San Diego OA CIP Plan risk assessment methodology were the MAST and TRAM. These two methodologies apply an overall risk management strategy and were developed by the U.S. DHS, G&T, which is now under the FEMA, Grants Program Directorate. These methodologies have been proven and accepted through implementation at more than 30 mass transit agencies and four major seaports throughout the nation.

These methodologies assess risk by comparing the overall likelihood and consequence of an attack or event. The likelihood can be defined as the combination of threat, which is the likelihood of an attack or event occurring, and the vulnerability, which is the likelihood of the attack or event being successful. The consequence can be evaluated through determining the consequence of an asset and the estimated impact of a particular attack or event. Therefore, the assessment evaluated risk as defined by DHS:

Risk = Threat * Vulnerability * Consequence

The long-term goal of the San Diego OA CIP Plan will be to determine the risk of particular terrorist attack or natural hazard scenarios with the data gathered by performing on-site security assessments of assets; essentially a scenario-based assessment. However, the short-term goal and the product of this report was to perform an asset-based assessment which determined consequence, threat, and general vulnerability without regard for particular scenarios. As the OA performs the on-site security assessments, scenarios will be developed and a more detailed consequence, threat, and vulnerability assessment will be produced. The process for developing the CIP Plan addressed each of these factors as described below.

4.1 CONSEQUENCE ASSESSMENT

The consequence assessment identified the initial list of assets and prioritized those assets based upon their relative importance to the OA. This process assumed total loss of the asset without consideration of any threat scenarios which would produce varying degrees of impact. The result of this process essentially determined the “Consequence” of an assets total destruction.

The consequence assessment methodology has four major steps:

1. Develop the Initial List of Assets (as described in Section 3 Identifying Critical Assets)
2. Determine Consequence Factors and Weightings
3. Determine Criteria for Rating Asset Consequence and Rate Assets
4. Incorporate Interdependencies and Prioritize List

Each step of the process was initially completed by the assessment team and then reviewed and agreed upon by the Steering Committee.

4.1.1 Determine Consequence Factors and Weightings

The next step in the consequence assessment was to determine consequence factors and then weight the factors' relative importance. The consequence factors assisted in defining the importance of each asset and remained consistent between sectors. The assessment team reviewed several federal risk methodologies such as the MAST, TRAM, SHIRA, and MSRAM to help determine which factors to choose and to ensure a level of continuity with national efforts. The final list of factors was determined by the assessment team and approved by the Steering Committee.

Each consequence factor was weighted on a scale from one (1) *least important* to five (5) *maximum importance*, to establish relative importance. Table 4-1 shows the final consequence factors, their relative weighting, and definitions.

Table 4-1. San Diego Region Consequence Factors

Consequence	Weight	Brief Description
Potential Casualties	**5**	The potential for loss of or serious injury to human life associated with an attack on the asset, both internal and external (e.g., due to an explosion, biological or chemical attack, or catastrophic failure/collapse of the asset).
Emergency Response Function	**4**	The role the asset plays in emergency response, either in direct services or in enabling access to emergency services, including gaining access to affected locations and evacuating people from affected locations.
Economic Impact	**4**	The local, state, regional, or national economic effect of losing the asset. This considers the number of people affected and possible destruction of infrastructure from flooding. This also includes the loss of recreational areas.
Government / Military Impact	**3**	The extent to which the asset supports national security/defense or government continuity.
Replacement Cost	**1**	The cost of replacing the asset if destroyed. This includes only the cost of replacing the asset and not the cost of cleanup. This cost will be the cost of construction of the asset in today's dollars.
Environmental Impact	**1**	The potential environmental impact due to flooding or from release of hazardous materials located at the asset.

4.1.2 Determine Criteria for Rating Asset Consequence and Rate Assets

The next step in the consequence assessment was to rate each asset based on the consequence factors. To assist with this step of the process the assessment team developed consequence factor criteria to use as a guide for rating. For each consequence factor, criteria were developed to define the rating scale ranging from a lower-bound rating of zero (0) to an upper-bound rating of ten (10). Table 4-2 lists the upper-bound criteria for each consequence factor. The upper-bound criteria may vary depending on the region of the country you are assessing, but overall definition is consistent with national efforts.

Table 4-2. Upper-Bound Criteria

Consequence Factors	Upper-Bound Criteria
Potential Casualties	Deaths or serious injuries likely to exceed 1,800 people.
Emergency Response Function	Assets that serve critical evacuation routes for highly populated areas with no reasonable alternate route, massively disrupt emergency response command and control functions (little/no redundancy), and/or provides emergency and in-patient medical services and can accommodate a large number of people and/or provides unique medical services.
Economic Impact	Moderate impact on the national economy.
Government / Military Impact	Massive impact on the U.S. Military to respond to a regional crisis or change/degradation to national government continuity.
Replacement Cost	Replacement cost likely to exceed $90 million.
Environmental Impact	Massive/long-term environmental impact that may require a significant response possibly from federal resources for the cleanup effort.

Using this criteria as a guide, the assessment team assigned each asset an applicability value from zero (0) to ten (10) for each consequence factor. The total consequence for each asset was then calculated by multiplying the consequence rating by the consequence factor weighting, for each consequence factor, and then summing across each.

4.1.3 Incorporate Interdependencies and Prioritize List

Not only is it necessary to assess the consequence of assets individually, it is also important to review an asset's interoperability and interdependency among other assets and sectors. To determine the significance of interdependency between the critical assets, a scoring system similar to the consequence rating system was developed. The system included ascertaining a weighted interdependency score and adding that score to the total consequence rating to obtain each asset's overall score.

The first step in determining the interdependency score was to establish the relative weight of the sectors. This was accomplished by taking the average asset consequence score for each sector and then ranking the sectors based on this average. The top four sectors were given a weight of three, the middle four sectors were given a weight of two and the remaining sectors received a weight of one.

The interdependency of the individual assets was then determined based on the SSPs. Each interdependency established in the plans was given a score of one. The sum total of all interdependencies and associated sector weight was then determined for all assets. Assets with high interdependencies

among the sectors had a higher score than those with low interdependencies among the other sectors. The total interdependency score was then added to the consequence ratings to obtain each asset's total score.

The final prioritization was completed by sorting the total consequence plus the interdependency scores within each of the sectors.

A review of the prioritized asset list after the addition of interdependency scores showed the increased priority of those assets that many other sectors are highly dependent on. The sectors that were most affected by the addition of interdependency scores were the Energy, Emergency Services and Water Sectors. This outcome was expected due to the critical nature of these sectors.

4.2 THREAT ASSESSMENT

4.2.1 Consideration of All-Hazards

It is vital that when assessing the threat to an asset that all-hazards be considered. Following the all-hazards approach for the overall risk assessment, the second step in the process evaluated the assets' "threat" with respect to both man-made and natural hazards.

The assessment for man-made threats evaluated the relative likelihood that a given asset may be targeted for attack. Specific scenarios have not been developed as this is an asset-level assessment that determined the target attractiveness of a particular asset without regard for the type of weapon that may be employed. This assessment was not a traditional threat assessment as it did not evaluate the intents or capabilities of potential threat elements (PTEs) in the San Diego region, the likelihood of PTEs acquiring a weapon, or the possibility of a weapon being delivered to a particular asset. Such information will be acquired and analyzed once an asset has had an onsite vulnerability assessment performed and specific attack scenarios have been developed. Vulnerability assessments within the region are currently being coordinated by Steering Committee and performed by a select set of individuals with the proper training and credentials.

The natural hazard threat assessment used data collected during the *Multi-Jurisdictional Hazard Mitigation Plan* to determine the threat or an asset's susceptibility for damage from an earthquake, liquefaction, flood, wildfire, tsunami, or landslide. Building upon previous natural hazard studies and GIS information, the threat assessment determines an asset's likelihood of natural hazards based upon the asset's location in the region.

4.2.2 Man-Made Hazards

Likelihood can be defined as the product of threat, which is the probability of an attack or event occurring, and Vulnerability, which is the probability of the attack or event being successful. Likelihood is evaluated with consequence to determine risk:

Likelihood = Threat * Vulnerability

The man-made threat assessment process uses an approach similar to the consequence assessment by rating an asset's likelihood to be targeted for attack using predetermined scales and criteria.

The first step in the process was to determine each asset's threat rating. The threat rating was comprised of four factors related to the asset's target attractiveness, as viewed from a terrorist's perspective. These target attractiveness factors represent the commonly accepted aspects of CI targets that correspond to the

potential goals of a terrorist attack. These factors: Potential Causalities, Economic Impact, Government/ Military Impact and Symbolic Importance.

The four target attractiveness factors were rated for each asset on a scale from zero (0) to ten (10) with zero representing no target attractiveness and ten representing maximum target attractiveness. The ratings for Potential Casualties, Economic Impact, and Government/Military Impact were taken directly from the consequence assessment using the same scales and criteria.

Symbolic Importance is commonly used as a factor in determining target attractiveness in other State and Federal assessments and was also rated on a scale from zero to ten. Much like the consequence factors, criteria was developed for Symbolic Importance to define the rating scale ranging from a lower-bound rating of zero (0) to an upper-bound rating of ten (10). Table 4-1 lists the criteria for Symbolic Importance.

Table 4-3. Symbolic Importance Rating Criteria

RATING	SYMBOLIC IMPORTANCE
Very High (9-10):	The asset is internationally recognized for its historical, cultural, economic, or political importance.
High (7-8):	The asset is nationally recognized for its historical, cultural, economic, or political importance.
Medium (5-6):	The asset is regionally recognized for its historical, cultural, economic, or political importance.
Low (3-4):	The asset is locally (city-wide) recognized for its historical, cultural, economic, or political importance.
Very Low (0-2):	The asset is not well known for its historical, cultural, economic, or political importance.

Unlike the consequence assessment, the threat assessment did not assign a weight to each target attractiveness factor individually. Instead the threat posed to an asset was determined by calculating the average of the four target attractiveness factors.

Threat = Average [Target Attractiveness]

There is not a consistent or standardized approach for the threat assessment process. Threat assessments at each level of government may or may not weight the threat factors depending upon the individual assessment. This assessment did not use weightings for the target attractiveness factors because the assessment team did find compelling evidence through historic targeting or through terrorist handbooks that have favored any one of the threat factors more than the others. While the four target attractiveness factors are identified in terrorist handbooks, including Al-Qaeda's training publications, they do not identify a specific priority for those factors.

4.2.3 Natural Hazards

The natural hazard threat assessment used GIS data collected during the *Multi-Jurisdictional Hazard Mitigation Plan*, 2004, to determine the threat or susceptibility for damage from an earthquake, liquefaction, flood, wildfire, tsunami, dam inundation or landslide. Using this data, the level of threat or susceptibility of each asset to each type of hazard was analyzed. For the natural hazards of Coastal

Storm/Erosion & Tsunami, Dam, Flood, Landslide, and Liquefaction the GIS data established whether or not an asset was at risk to each hazard. The GIS data for earthquake and wildfire established a level of threat for each hazard. Each asset was scored as having a "high" or "low" risk for earthquake damage and an "extreme", "very high", "high", "moderate" or "little or no threat" for wildfire risk.

4.3 VULNERABILITY ASSESSMENT

The final step in the risk assessment was a high-level assessment to determine the general probability of an attack or event being successful in order to determine each asset's vulnerability. Determining the vulnerability for each asset was the second part of the Likelihood equation described in 4.2.2 Man-Made Hazards. The product of the threat and vulnerability determined the overall likelihood of an attack occurring and being successful at a particular asset.

This vulnerability assessment was based upon open source information and did not include detailed site visits or interviews with asset owners/operators. It is assumed the prioritized list of assets generated by the CIP Plan will serve to prioritize follow-on efforts for conducting detailed site visits and security assessments for high priority assets.

The first step in the vulnerability assessment was to rate and prioritize each asset based on criteria that was developed by the assessment team to determine the likelihood of an attack being successful. Much like the consequence factors, criteria was developed to define the rating scale ranging from a lower-bound rating of zero (0) to an upper-bound rating of ten (10) for the vulnerability factor. Table 4-3 lists the criteria and associated rating scale for vulnerability.

Table 4-4. Critical Infrastructure Vulnerability Ratings

RATING	VULNERABILITY
Very Low (9-10):	The countermeasures in place are very unlikely to defeat an attack. Perceived soft target with little or no security countermeasures.
Low (7-8):	The countermeasures in place are unlikely to defeat an attack. Examples may include, but are not limited to, random offsite security patrols, little/no monitored physical security system (although basic security practices may be followed), little/no perimeter control and/or open public access, basic safety lighting, and a perceived inability to detect or aid in the apprehension of perpetrators of any offensive action.
Medium (5-6):	The countermeasures are somewhat likely to defeat an attack. Examples may include, but are not limited to, random offsite security force, offsite monitored basic physical security system, open public access during hours of operation, good safety lighting, and a perceived ability to detect and possibly apprehend perpetrators of aggressive offensive actions.
High (3-4):	The countermeasures in place are likely to defeat an attack. Examples may include, but are not limited to, stationed security force or onsite consistent patrols, onsite monitored physical security system, perimeter access control, limited public access, high security lighting, and a perceived ability to delay or prevent aggressive offensive actions.
Very High (0-2):	The countermeasures are very likely to defeat the attack. Examples may include, but are not limited to, stationed security force, effective layered physical security system, strong perimeter access control (to include vehicle control), high security lighting, and a perceived ability to repel or defeat aggressive offensive actions.

Using these criteria as a guide, the assessment team assigned each asset a score from zero (0) to ten (10) based on known information related to each asset's physical setting and countermeasures. Likelihood of an attack for each asset was the product of the asset's threat and vulnerability.

4.4 RISK ASSESSMENT

The three primary components of the risk assessment: consequence, threat, and vulnerability, were used to determine the relative risk of each asset. An asset's risk to a particular hazard was the product of the consequence, threat and vulnerability. The product of the threat and vulnerability was the asset's likelihood. Therefore risk can also be assessed by evaluating an asset's likelihood and consequence which is the definition of risk used by DHS:

Risk = Likelihood * Consequence

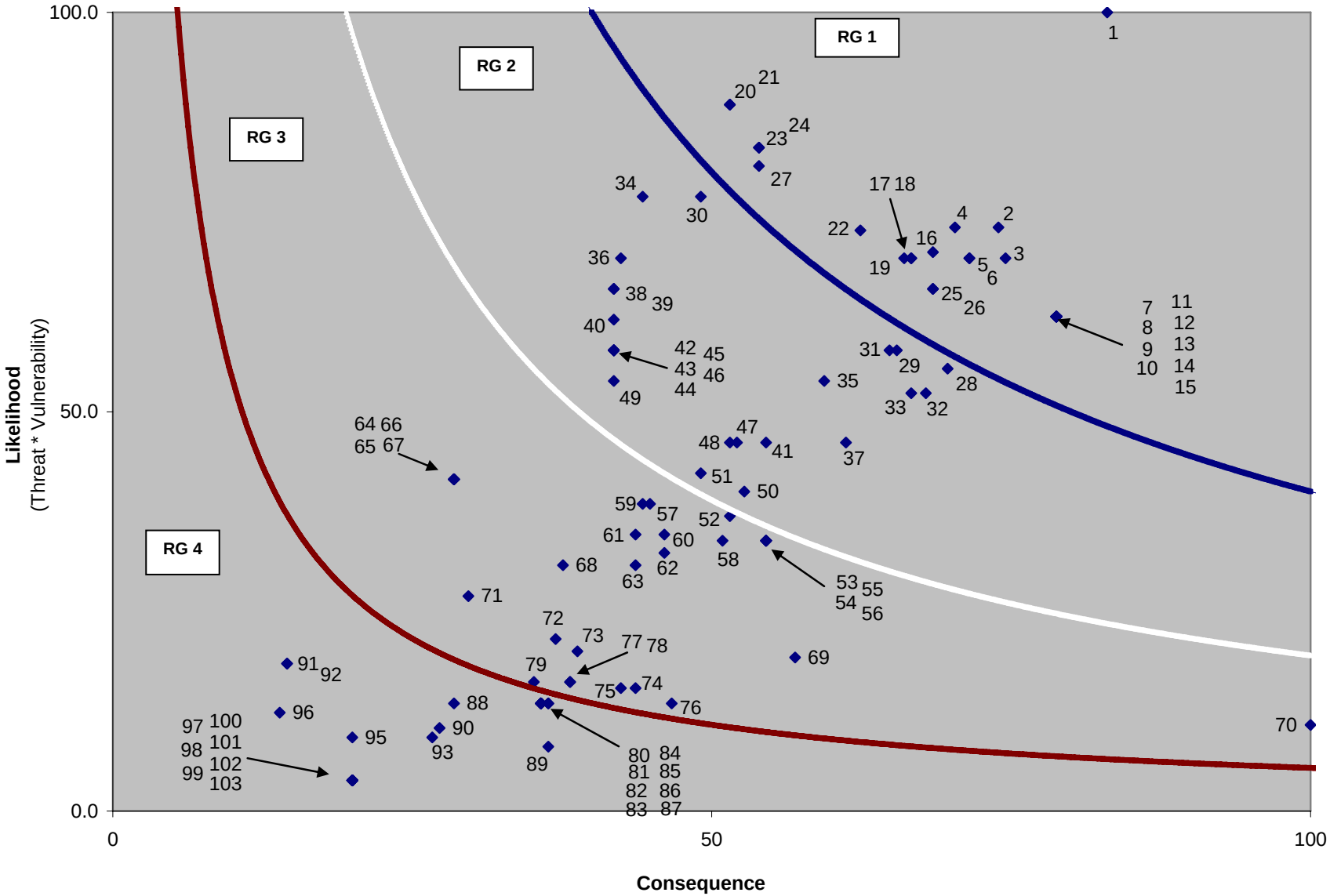
To facilitate evaluation of the risk results, the likelihood and consequence ratings were normalized on a scale of zero to 100. Each consequence score was divided by 165, the maximum actual consequence value, and then multiplied by 100. Each likelihood score was divided by 65, the maximum actual threat value, and then multiplied by 100. The relative risk for each asset was calculated by multiplying the normalized consequence by the normalized likelihood.

In order to comparatively evaluate the risks for each asset the relative risk results were plotted on a relative risk scatter diagram. The normalized consequence rating, which represents the impact to the region from losing the functionality of an asset, was plotted on the horizontal axis. The normalized likelihood rating, which represents the likelihood of a successful attack occurring, was plotted on the vertical axis.

This methodology is not discrete enough to compare the individual asset risk ratings because the judgments by which those ratings were determined were subjective in nature and made on coarse scales (e.g. 0-10). While there is some level of uncertainty associated with the final risk calculations, the overall methodology is rational, defensible and transparent.

With this in mind, the assessment team divided the assets into four Risk Groups (RG) based on their respective levels of relative risk. All assets within a particular RG are considered to have an approximately equal level of risk. The RGs are delineated by the lines of equal risk as depicted in Figure 4-1. Those assets above the upper-right most risk line, RG 1, are considered to have the highest risk and those below the bottom most risk line, RG 4, are considered to have the lowest risk.

Figure 4-1 Relative Risk Diagram



SECTION 5 DECISION MAKING PROCESS

5.1 RESOURCE PRIORITIZATION

One of the challenges of enhancing the security and protection of CI/KR is determining the most efficient way to prioritize the allocation of the limited resources and grant dollars for protective measures for the specific assets. The consequence, threat, vulnerability and risk assessments, described in Section 4 Assessment Methodology, developed a prioritized list of CI/KR within the San Diego OA. The prioritized list of assets in the OA is divided into four RGs, with RG 1 having the highest consequence and the highest level of threat (see Figure 4-1 Relative Risk Diagram). The goal of allocating resources and funding for protective measures to these assets is to lower their threat and therefore lowering their RG.

The next step in determining resource prioritization is to determine the most effective and beneficial protective measures for the assets in RG 1 through 4, beginning with RG 1. To select protective measures that will most effectively lower the threat of an asset, the current threat score must be assessed and reviewed for areas of improvement (described in Section 4.2 Threat Assessment). Once these security gaps have been identified prospective protective measures can be evaluated, funded and implemented.

5.1.1 Protective Measures

Once the County has identified the security gaps and areas of improvement for protection of the CI/KR in RG 1, described in Section 4 Assessment Methodology, protective measures can be identified and reviewed. Based on the type of asset, there are different categories of protective measures which can be considered for enhanced security and protection. General CI/KR protective measures that the County may consider, which may also be eligible for FEMA/DHS grant funding, include:

- Physical security, including extension of security perimeter beyond the limits of facility to create a buffer zone;
- Roving security inspections;
- Access control;
- Background checks for employees, temporary workers, contractors, subcontractors, security force, and potential first responders;
- Loss prevention, material control, and inventory management;
- Delivery service verification (e.g., request delivery worker identity card);
- Control-room security;
- Policies and procedures;
- Information/cyber security;
- Intelligence, particularly for specific assets (e.g., East Coast vs. West Coast);
- Training on security plans;
- Drills involving employees, contractors, public, and media;
- Crisis management and emergency response, including incident command system; and,
- Communication of hazards by asset owners to public sector protection forces.

The criterion used to evaluate the effectiveness of protective measures varies between the different categories. One of the most important factors to consider when selecting a protective measure is the cost-benefit. There are two types of costs associated with a protective measure, the initial up-front cost and the recurring cost. Both of these should be weighed when selecting a protective measure.

The effectiveness of a protective measure should also be reviewed when considering resource prioritization. Effectiveness can be estimated by determining the associated reduction of threat achieved by implementing a given protective measure. To do this the asset's threat should be re-scored considering the addition of the protective measure. If the new threat score places the asset into a lower RG, then the protective measure would be considered effective. The lower the asset's risk becomes with the addition of the protective measure, the more effective the protective measure should be considered.

Once the protective measures have been reviewed the County will then use this information to identify which protective measures to fund and how that funding will be obtained.

5.1.2 Resource Allocation

After determining the overall benefit and effectiveness of all potential protective measures for each of the assets in RG 1, all options should be reviewed and compared. Resource allocation priority should be given to those assets with the combination of the highest consequence and threat and most effective protective measure. Once a review has been completed the assets which have been determined to benefit most from the available resources will be selected to receive funding.

5.2 RESOURCE AND FUNDING OPTIONS

This section describes the primary sources of funding for CIP and the influence that the funding requirements have on the County's resource allocation decisions. The main source of CIP grants and funding is through the DHS G&T. There are additional sources of grant funding that may be used for CIP, including Federal preparedness programs offered by:

- Department of Health and Human Services through the Centers for Disease Control and Prevention (CDC);
- Health Resources and Services Administration;
- FDA;
- USDA;
- U.S. Department of Justice;
- U.S. Department of Transportation; and other relevant organizations;
- California State homeland security and preparedness programs and resources; and,
- Local and tribal homeland security and preparedness programs and resources.

Although other grant programs exist, FEMA/DHS is the most consistent and largest provider of funds for CIP. Therefore, this section will focus on grant prospects from FEMA/DHS. The County should however explore these alternative sources of funding when considering and seeking out financial resources for protective measures for CI/KR.

5.2.1 U.S. Department of Homeland Security Grant Programs

The two largest grant programs from FEMA/DHS are the Homeland Security Grant Program (HSGP) and the Infrastructure Protection Program (IPP).

HSGP consolidates four grant programs into one application process, these include:

- State Homeland Security Program (SHSP);
- Urban Areas Security Initiative (UASI);
- Citizen Corps Program (CCP); and,
- Metropolitan Medical Response System (MMRS).

IPP consolidates five grant programs into one application process these include:

- Buffer Zone Protection Program (BZPP);
- Transit Security Grant Program (TSGP);
- Port Security Grant Program (PSGP);
- Trucking Security Program (TSP); and,
- Intercity Bus Security Grants (IBSGP).

There are many FEMA/DHS grant programs but there are a limited number that are applicable for CI/KR protection funding, these programs include SHSP, UASI, BZPP, TSGP, PSGP and TSP. Each of these programs provide specific guidance on what funds can be used towards, therefore, the County must be sure to submit requests for the appropriate grant program and in the correct amount. The following sections provide a brief description of each of the major FEMA/DHS grant programs which are applicable for CI/KR funding. For more information on specific grant programs visit the FEMA website at http://www.fema.gov/government/grant/index.shtm.

5.2.1.1 State Homeland Security Program (SHSP)

SHSP supports building and sustaining capabilities at the State and local levels through planning, equipment, training, and exercise activities and helps states to implement the strategic goals and objectives included in state homeland security strategies. SHSP provides funding to all 56 states and territories based on a formula combination of risk and effectiveness.

FEMA/DHS is directing that at least 25 percent of funds allocated from both SHSP and UASI build state and local law enforcement terrorism prevention capabilities.

The County should work to identify CIP activities that may be eligible for Federal funding under SHSP. As of the FY 2008 FEMA/DHS guidance, the four areas eligible for funding under SHSP include planning, training, equipment and exercises.

Total Funding Available in FY 2008: $862.9 million.

5.2.1.2 Urban Areas Security Initiative (UASI)

UASI provides financial assistance to address the unique multi-disciplinary planning, operations, equipment, training, and exercise needs of high-threat, high-density urban areas, and to assist them in building an enhanced and sustainable capacity to prevent, respond to, and recover from threats or acts of terrorism. Allowable costs for the urban areas mirror those under SHSP, and funding is allocated based on

Urban Area Homeland Security Strategies. This program provides funding to high-risk urban areas based on risk and effectiveness.

FEMA/DHS is directing that at least 25 percent of funds allocated from both SHSP and UASI build state and local law enforcement terrorism prevention capabilities.

The eligible funding areas for UASI are the same as those described for SHSP, except for the addition of operational reimbursements, and the requirement to satisfy the strategies described in the Urban Area Homeland Security Strategy.

Total Funding Available in FY 2008: $781.6 million.

5.2.1.3 Buffer Zone Protection Program (BZPP)

BZPP is intended to significantly enhance the protection around CI/KR sites and deter threats or incidents of terrorism aimed at those facilities. BZPP supports the development and implementation of Buffer Zone Plans for preventing and protecting the perimeter of CI sites, including chemical facilities, nuclear and electric power plants, dams, stadiums, arenas and other high-risk areas from terrorist site surveillance or attacks with a focus on public-private partnership and fusion center coordination. This program provides funding to states and territories with eligible CI/KR sites.

BZPP funding is provided to pre-determined CI/KR sites as determined by DHS, the County may be able to align their CI/KR priorities with those of BZPP and utilize the funding for both purposes.

Total Funding Available in FY 2008: $48.5 million.

5.2.1.4 Port Security Grant Program (PSGP)

The PSGP provides grant funding to port areas for the protection of critical port infrastructure from terrorism. PSGP funds help ports enhance their risk management capabilities, domain awareness, training and exercises, and capabilities to prevent, detect, respond to, and recover from attacks involving improvised explosive devices and other non-conventional weapons.[9]

Total Funding Available in FY 2008: $388.6 million.

5.2.1.5 Transit Security Grant Program (TSGP)

The TSGP provides grants to the Nation's key high-threat Urban Areas to enhance security measures for their critical transit infrastructure including bus, rail, and ferry systems. This year, the TSGP will also provide funding to Amtrak for continued security enhancements for its intercity rail operations between key, high-risk Urban Areas throughout the United States.[9]

Total Funding Available in FY 2008: $388.6 million.

[9] http://www.ojp.usdoj.gov/odp/grants_ipp2007.htm

5.2.1.6 Trucking Security Program (TSP)

The TSP provides funding for an anti-terrorism and security awareness program for highway professionals in support of the National Preparedness Guidelines. Anyone is eligible to apply for program funding as long as they support all four funding priority areas: participant identification and recruitment; training; communications; and information analysis and distribution for an anti-terrorism and security awareness program.[10]

Total Funding Available in FY 2008: $15.54 million.

[10] http://www.ojp.usdoj.gov/odp/grants_ipp2007.htm

SECTION 6 FUTURE INITIATIVES

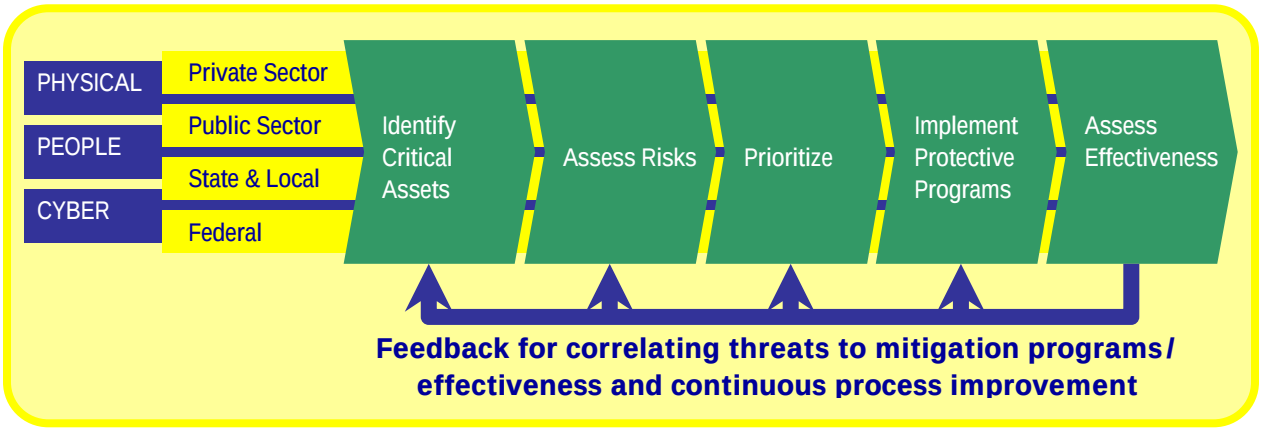
The next steps in the CIPP include identifying opportunities to move assets from higher to lower RGs through a variety of potential actions, thereby reducing their overall relative risk. This process can be measured over time and as more detailed site assessments are performed the factors associated with each asset can be updated to provide a more accurate perspective of the risk associated with the OA's CI/KR.

6.1 RISK MANAGEMENT

The overall goal of the CIPP is risk management. Risk management is the method of weighing the cost of protecting an asset against the associated reduction of risk. Risk management is a multiple step process which DHS has applied to protecting CI/KR in the NIPP as illustrated in Figure 6-1.

The desired outcome of the CIPP for the OA is to maximize the reduction of risk to CI/KR by investing in protective programs and measures with the greatest benefit.

Figure 6-1 DHS Risk Management Diagram



This Plan has completed an initial draft of the first three steps. The next step in the risk management process is the deployment and implementation of protective programs and the assessment of the effectiveness of these programs.

6.2 IMPLEMENT PROTECTIVE PROGRAMS

A CI/KR protective program provides the framework for sustaining existing protective measures while providing a strategy for addressing and minimizing existing vulnerabilities in the future. The protective program balances the provision of specific protective measures with cost-effective decision making that evaluates security threats across sector boundaries. Protective programs prevent, deter and mitigate threats and reduce the consequences from an attack or natural disaster. Potential protective programs that may benefit the OA include both immediate action items as well as long range planning objectives.

6.2.1 Immediate Action Items

The immediate action items to be considered for reducing the risk of the OA's CI/KR include conducting a tabletop review of the specific physical security vulnerabilities of specific assets and conducting detailed, on-site surveys of the assets with the highest risk factors. Both of these action items would be prioritized to evaluate assets in RG 1 first and address the assets in the other RGs as additional time and funding are available.

The tabletop review would involve staff with specific knowledge and familiarity of the assets who could provide recommendations for improving the physical security and protective posture of these assets. These recommendations can be packaged into CI projects for future funding requests. A standardized list of physical security countermeasures and associated cost estimates has been provided in the *San Diego Operational Area Critical Infrastructure Protection Plan Risk Assessment,* 2008 to help facilitate the development of cost estimates for specific projects.

In order to prepare detailed, asset-specific action plans, more thorough on-site surveys are required to collect and assess the particular attributes of each asset. These site visits should be conducted by a team of physical security and engineering experts. In keeping with the all-hazards approach, the team should also be accompanied by additional experts who are knowledgeable in assessing opportunities to mitigate risk associated with the natural hazards specific to the respective assets.

6.2.2 Potential Long Range Objectives

Potential protective programs that will aid in managing the risk associated with the OA's CI/KR may include:

- Develop surge capacity plans to increase OA's CI/KR's capacity during crisis.
- Develop standard measures to reconstitute capabilities if CI/KR facilities and systems are damaged.
- Develop security/protection plans for individual CI/KR owned by the County and jurisdictions.
- Identify potential infrastructure protection incentives for CI/KR owners in the private sector.
- Develop strategies and guidelines for protection of CI/KR personnel;
- Develop CI/KR protection package for the CI/KR owners in the OA (guidance on improving physical security, Continuity of Operations (COOP) Plan, Emergency Operations Plan (EOP), and Facility Evacuation Plan templates).
- Develop processes for collecting and maintaining CI/KR data. Identify mechanisms for protecting sensitive and confidential data.

6.3 ASSESS EFFECTIVENESS

As part of the OA's risk management program, it is possible to assess the effectiveness of reducing risk for individual assets as well as the CIPP as a whole.

One of the main benefits of the methodology used to create the CIP Plan is the development of a set of metrics that can be used to assess effectiveness of the County's CIP efforts. The metrics used to score the

OA assets for the consequence, threat, vulnerability and risk assessments can also be used to assess the effectiveness of protective measures and protective programs. Assets can be re-scored following the implementation of a protective measure or program and identify progress based on an improved score. Re-scoring OA assets can also identify new priorities based on changing threat and vulnerabilities which may occur over time. This method of assessing effectiveness can be used immediately by the OA.

The NIPP relies on a system of metrics to evaluate the success and continuous improvement of CI/KR Protective Programs. While quantitative metrics provide the simplest means of comparison, they can often be difficult to obtain as many indicators are not easily quantified. The NIPP relies on a combination of descriptive and quantitative measures to track sector specific metrics and core metrics, which cross sector boundaries. The County should develop a framework for preparing a meaningful series of core and sector-specific metrics that are relevant to the San Diego OA CIPP. These metrics should establish a baseline, describe the data necessary and the sources of that data to track the progress of each metric. Some of the specific topics to be addressed by these metrics should include, but should not be limited to:

- Establish the criteria to measure the progress and effectiveness of the CI/KR Program implementation in the OA.
- Monitor the implementation progress and effectiveness of protective measures of the CI/KR Program.
- Monitor the progress of developing EOPs, COOP plans, and CI Security plans by the owners of the CI/KR assets in the OA.
- Develop and conduct exercise programs to test CI/KR security/protection and surge capacity plans.

6.4 COORDINATION WITH PRIVATE OWNER/OPERATORS

An estimated 85 percent of the Nation's CI is owned by the private sector[11]. As a result, it is vital that the public and private sectors work together to protect these assets. Through future initiatives of the CIPP, the involvement of Stakeholders which represent private interests across the 18 infrastructure sectors identified in the *National Infrastructure Protection Plan* (NIPP) are necessary to ensure adequate regional CI/KR protection. The ultimate protection of the CI/KR owner by the private sector depends on the action of the owner/operators of those assets. The following organizations and programs are available to facilitate the necessary coordination and sharing of information with the private sector.

Regional Terrorism Threat Assessment Center (RTTAC)

The RTTAC has three major initiatives including intelligence gathering/dissemination, development of the Terrorism Liaison Officer (TLO) program, and execution of CI Site Assessments. The intelligence portion of the RTTAC will help to develop a regional threat assessment picture and will directly connect to other RTTAC's throughout the state and the State Terrorism Threat Assessment Center (STTAC) to share information and produce assessments, reports and other threat and warning products.

At the local level law enforcement and public safety agencies have designated TLOs trained in the review and assessment of local reporting and in conducting outreach to other public safety agencies, critical

[11] United States Government Accountability Agency, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, October 2006.

infrastructure operators and community groups. The TLO is the local agency point of contact for all terrorism-related alerts, requests for information, warnings and other notifications from regional, State or Federal homeland security agencies. The TLOs review local agency reports, manage local reporting and initiate or respond to requests for information. TLOs are coordinated by each RTTAC on a regional basis and supply and disseminate information through the RTTAC.

The primary focus of the Site Assessments is to collect information needed to develop justifiable investment strategies and resource allocations. These detailed Site Assessments evaluate individual assets to identify upgrades and improvements to the assets' physical security. The ultimate objective of these assessments is to identify specific opportunities for managing and reducing the risk associated with individual assets.

InfraGard

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories.

Within San Diego the InfraGard program is coordinated by the FBI with a private sector representative as the Director. Quarterly meetings typically consist of all-hazards presentations, information sessions, or training held at various venues throughout the region. The goal of InfraGard is to help educate the private sector of terrorism related issues, which may help the private sector to strengthen its security posture.

Homeland Security Information Network (HSIN)

DHS's Information Analysis and Infrastructure Protection's Homeland Security Information Network initiative is expanding its internet-based counterterrorism communications network to all 50 states, five territories, Washington, D.C., and 50 major urban areas to strengthen its real-time, collaborative flow of threat information to state and local communities. The HSIN significantly strengthens the real-time, exchange of secure threat information to state and local agencies at the Sensitive-but-Unclassified level. Future program expansion will include the county level agencies, communication at the classified SECRET level, and the involvement of the private sector.

Currently HSIN is primarily used by public safety and intelligence entities within the region as one of many mechanisms to communicate with each other regarding terrorism related information.

Information Sharing and Analysis Centers

The mission of the Information Sharing and Analysis Centers Council (ISAC) is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government.

There are various ISACs related to individual sectors and sub-sectors to be used as a mechanism for raising the level of security within their respective areas of responsibility. ISACs are typically a national effort and are utilized by the individual asset owners/operators within the region.