The City of Los Angeles, California’s Critical Infrastructure/Key Resource Protection Program

SUMMARY
The City of Los Angeles identifies, assesses, and protects critical infrastructure through Operation Archangel, a comprehensive critical infrastructure and key resource (CI/KR) protection program. Operation Archangel utilizes the US Department of Homeland Security’s (DHS) Automated Critical Asset Management System (ACAMS), an automated data collection and reporting tool, to track and report CI/KR protection data. The City establishes relationships with private sector asset managers and conducts extensive site assessments, data collections, and target hardening efforts through the Archangel program. The CI/KR protection program is a partnership of DHS, the State of California, the City of Los Angeles, and the Los Angeles Police Department.

BACKGROUND
The City of Los Angeles reviewed its critical infrastructure inventory following the September 11, 2001, terrorist attacks. The inventory listed 600 sites as “critical,” but the list did not provide a meaningful indication of a site’s importance or criticality. The top 45 sites on the list were symbolic but contained no actual infrastructure. Furthermore, the list was geared toward providing information for SWAT operations and focused on the potential for criminal activity, not a terrorist attack. The list also contained inaccurate, irrelevant, or inconsistent information on many sites.

The City of Los Angeles launched a new CI/KR protection program, Operation Archangel, to identify and protect truly critical assets in 2004. Archangel supports the National Infrastructure Protection Plan (NIPP) by building security partnerships, managing risk, and maximizing efficient use of resources.

GOALS
The goal of the Los Angeles CI/KR protection program is to identify, assess, and protect key assets and critical resources in the Los Angeles metropolitan area. ACAMS facilitates the collection, storage, prioritization, and reporting of critical infrastructure information. Archangel enhances the security of critical assets through cooperative assessments, data collection and sorting, and real-time reporting capabilities.
DESCRIPTION

Operation Archangel is managed by Los Angeles Police Department law enforcement personnel working in partnership with the California Office of Homeland Security and DHS. A “core group” advises the Archangel program to ensure input from all relevant agencies and asset owners. The core group consists of public and private sector representatives who own and protect critical assets throughout the city. This group provides recommendations on the CI/KR protection program’s procedures and operational focus.

Defining “Critical Asset”

The City of Los Angeles began program development with an extensive research effort to define the terms “critical,” “asset,” and “infrastructure.” The CI/KR protection program then conducted an inventory of 481 critical assets, 26 buffer zone plans, and 847 Los Angeles Unified School District facilities from January through March 2005. This inventory provided the basis for Operation Archangel’s unique assessment and prioritization methodology.

The City and DHS conducted a long-term research effort in 2004 to define “critical asset” for the Los Angeles Urban Area. Critical assets were classified into three categories:

- **Critical Infrastructure**: An asset whose compromise would interrupt continuity of operations in 1 of 17 potential sectors:
  - Agriculture and Food
  - Banking and Finance
  - Chemical
  - Commercial Assets
  - Dams
  - Defense Industrial Bases
  - Emergency Services
  - Energy
  - Government Facilities
  - Healthcare and Public Health
  - Information Technology
  - National Monuments and Icons
  - Nuclear Power
  - Postal and Shipping
  - Telecommunications
  - Transportation
  - Water Supply and Delivery

- **Mass Population**: Assets such as locations, events, gatherings, and groups of people that, if compromised, may generate injuries, illness, or loss of life and that are significant in scale, method, or impact.

- **Symbolic/Psychological**: Cultural, religious, or national icons and patriotic locations and events.

Performing a Critical Asset Inventory

An inventory is the first step in critical asset information gathering. Archangel analysts constructed the initial list of assets using open-source research and general knowledge of a city or region. For critical infrastructure, Archangel analysts considered all fire, law enforcement, hospital, power, water, sanitation, and communications facilities. For mass population assets, they considered stadiums, chemical plants, storage facilities, and large

Los Angeles Urban Area Definition of Critical Asset

“Any entity or location, whether physical or virtual, the compromise of which would have a profound and negative effect on critical infrastructure, cause mass casualty, or have a profound and negative symbolic or psychological impact.”
gathering places such as malls. For symbolic/psychological impact sites, they considered local religious facilities, chambers of commerce, community groups, and special events.

All asset information collected in this inventory is inputted into ACAMS and assigned values based upon the critical asset categories. All assets in the critical infrastructure category are placed in level 1, all assets in the mass population category are placed in level 2, and all assets in the symbolic/psychological category impact are placed in level 3. Operation Archangel pursues more information from and establishes relationships with managers of level 1 assets.

All information collected by Operation Archangel is stored in DHS’s ACAMS system. ACAMS collects asset data, protection information, and response plans and in turn provides useful reports to assist in prevention, protection, and response efforts. ACAMS incorporates Protected Critical Infrastructure Information (PCII) protections into the system through a partnership with the DHS PCII Program Office. This unique attribute of DHS’s ACAMS system greatly reduces the amount of time needed to get information approved for PCII protection from DHS. PCII-protected information is shielded from public disclosure under statutory exemptions created by the Critical Infrastructure Act of 2002.

Establishing Relationships
The City of Los Angeles contacts the organizations that own critical infrastructure listed in the initial asset inventory. The City has found that assessments are more efficient and effective when a strong relationship exists between the asset manager and the law enforcement department that conducts assessments.

The City follows a three-step process to establish a relationship with an asset manager. First, CI/KR protection program personnel conduct open-source research on an asset’s vulnerabilities, dependencies, and redundancies. They use this information to communicate the specific reasons for and value of conducting an assessment. Second, CI/KR protection program personnel send a letter to the asset manager outlining the specific reasons for an assessment and the protections available for sensitive asset information. Finally, they call the asset manager to follow up on the letter and to discuss the next steps in the assessment process.

The CI/KR protection program recognizes that many asset managers may be hesitant to participate and share information. Asset managers may believe that site assessments are required by law or fear the assessment process will result in the release of sensitive information. The CI/KR protection program recommends a number of techniques to overcome this hesitation:

- Ask for information, don’t demand it;
- Understand a manager’s position and be prepared for skepticism;
- Be honest and answer questions directly;
- Stress public safety as the primary mission and ultimate goal of the assessment; and
- Emphasize the asset’s criticality and relationship with local emergency responders.
CI/KR protection program personnel initiate an Asset Management Questionnaire (AMQ) once they have established a relationship with an asset manager. The AMQ provides the CI/KR protection program and the asset manager with an online tool for collaboration and data collection.

**Standardized Assessment Methodology**

The centerpiece of the CI/KR protection program is a standard methodology for identifying, prioritizing, and assessing critical infrastructure. This methodology ensures accurate and up-to-date data is available for analysts and incident commanders in law enforcement and fire departments, emergency operations centers, and intelligence fusion centers. The methodology consists of four “stages” of assessment and sorting. The CI/KR protection program inventories assets within a defined geographic area in a preliminary stage. In “Stage I,” high-priority assets provide information that populates an ACAMS survey tool known as the Asset Management Questionnaire (AMQ). “Stage II” consists of an onsite assessment designed to verify the information collected in the AMQ. In “Stage III,” assets undergo a more thorough assessment by CI/KR protection program personnel in order to generate specific prevention and protection plans.

**Stage I: Asset Manager Questionnaire**

Completing an AMQ is the first step in the data collection and assessment process. **Level 1** asset managers access the AMQ online by registering for and logging in to the ACAMS system. The AMQ prompts asset managers to enter information on each critical asset network, site, or facility through a series of online forms in the ACAMS system. The AMQ requests the following information:

- Basic asset information
- Operating hours
- Hazardous materials
- Threat history
- Security procedures
- Emergency plans
- Other plans, maps, photos, and diagrams
- Mission
- Points of contact
- Facility population
- Facility description

Operation Archangel encourages asset managers to update the AMQ every 90 days, although asset managers may add to, amend, or update the AMQ anytime. Archangel assessment teams complete the AMQ through open-source research and interviews if an asset does not agree to a site visit or refuses to complete the AMQ.

**Stage II: Initial Asset Visit**

A City of Los Angeles critical assessment team conducts an initial asset visit (IAV) to each asset that has completed an AMQ and agrees to an onsite assessment. The primary purpose of an IAV is to verify the information contained in the AMQ. The IAV also enables the critical asset assessment team to confirm the criticality of a site, to identify vulnerabilities and critical nodes, to harden the target, and to begin to compose and coordinate prevention, protection, and response plans.

**Critical Assessment Team**

A critical asset assessment team comprised of law enforcement and fire personnel visits a site following completion of the AMQ. The goal of an IAV is to develop a “game plan” to prevent or deter an attack at a critical asset. The critical asset team is composed of four or five members, including a team leader and two distinct groups: an internal assessment
team and an external assessment team. Critical asset assessment team members have subject-matter expertise in the following areas:

- Assault planning or tactical operations
- Bomb technician
- Cyber
- Engineering, building inspections, or construction
- Fire or hazardous materials

The internal team interviews the asset manager, engineer, and security manager to gather data on the operations of the critical asset. The internal team focuses on information such as the facility hours of operation, security procedures, emergency plans, and internal photos, maps, and diagrams. The external team also interviews the asset engineer and security manager but focuses on the outside of the facility. The external team collects information on the facility perimeter, physical security measures, approaches to the facility, and hazardous materials.

**IAV Conduct**

The CI/KR protection program places strong emphasis on appropriate assessment team conduct. The assessment teams conduct the visits in a friendly and professional manner. Assessment teams wear plainclothes instead of uniforms and are always local sworn law enforcement officers or firefighters. These teams avoid the use of language such as “threat” and “vulnerability” and refer to sites as “clients” instead of “targets.”

**IAV Data Collection and Analysis**

Data collected during an IAV is stored on the ACAMS system in the “IAV” section. The data from the AMQ automatically populates this new section, which provides a broader and more comprehensive look at the asset. Fields in the asset IAV section of ACAMS include:

- Additional POCs
- Approaches to the facility
- Buffer zones
- Critical nodes
- Intelligence (to be filled out by fusion center analysts)
- Options for consideration
- Perimeter data
- Photographs from the IAV
- Physical security data
- Security checklists
- Security enhancements

**Options for Consideration**

Critical asset assessment teams provide onsite target-hardening suggestions to asset managers and security personnel at the end of a site visit. Operation Archangel terms these suggestions “options for consideration.” Options for consideration provide asset managers with potential security solutions that are not regulatory or legal requirements. Options for consideration use DHS-approved language and avoid words such as “recommendation” and “checklist.” They are suggestions that an asset may or may not implement on its own, not “codes” or other measures that require enforcement. This practice reduces the asset manager's exposure to legal proceedings following an incident because the asset can not be faulted for failing to meet a regulatory mandate. The CI/KR protection program tracks implementation of the target-hardening measures but does not require that they be implemented.

There are two categories of options for consideration: random anti-terrorist measures taken without specific threat information and specific anti-terrorist measures taken after
intelligence indicates a threat to a region, sector, or site. Examples of random anti-terrorist measures include:

- A change in loading dock procedures
- Identity checks of all vehicle occupants
- Closed Circuit Television Cameras
- K-9 patrols
- Limits on deliveries
- Random vehicle checks
- Roving security patrols
- Offsite delivery screenings
- Tests and challenges of (red-team) procedures

Examples of specific anti-terrorist measures include:

- 100% identity checks
- 100% vehicle searchers
- Armed security officers
- Bomb detection K-9 units
- Closed Circuit Television Cameras
- Complete access control
- Hydraulic bollards, K-rail, and water-filled barriers
- Improvements on the fence line to deter surveillance
- Magnetometers
- Motion detectors
- Restrictions on deliveries
- Restrictions on parking in and around the facility
- Security officers at all critical nodes

Options for consideration focus security staff on unusual activity and also reduce crime around facilities.

**Stage III: Critical Asset Assessment**
The Critical Asset Assessment is the complete, full-scale assessment reserved for those assets deemed most critical by a jurisdiction. The City of Los Angeles is currently working with the Department of Homeland Security to develop the Stage III Critical Asset Assessment process.

**Reports**
ACAMS produces several useful reports for the prevention, protection, and response communities: Inventory Lists, Buffer Zone Plans, Pre-Incident Security Enhancement Plans, and Constellation Intelligence Reports.

**Inventory Lists**
These reports contain basic information on critical assets within a jurisdiction or geographic area. The report is categorized by critical asset category and infrastructure sector. This report is used most frequently by state and local governments with federal or state reporting requirements. ACAMS uses CI/KR taxonomy and criteria consistent with the National Asset Database.

**Buffer Zone Plans**
The ACAMS system can generate a properly formatted Buffer Zone Plan suitable for submission to DHS. This report supports the identification of preventive and protective measures to devalue, deter, and defend an asset. A subsequent Vulnerability Reduction Purchase Plan may be generated that assists with the implementation of preventive and protective measures.
Pre-Incident Security Enhancement Plans
Pre-Incident Security Enhancement Plans are easy-to-read, structured plans that map out specific actions an incident commander can take to harden an asset based upon intelligence or a change in the Homeland Security Advisory System (HSAS). This plan contains specific instructions for enhancing the security of an asset and provides suggested locations for command posts, staging areas, personnel, and other site-specific information. The plan pre-identifies equipment and personnel needs to effectively protect an asset and to deter threats. ACAMS makes the plans available to law enforcement and fire stations as well as to asset managers who can read and implement the plan following a change in HSAS or a receipt of actionable intelligence.

Constellation
Constellation is an open source data-mining and intelligence gathering tool that DHS has incorporated with the ACAMS system. Constellation searches the ACAMS database along with other open source databases to produce “hits” based on search terms and strings known as “concepts.”

Fusion Centers
ACAMS makes information available to and produces several useful reports for the prevention community. The ACAMS system is currently used in Los Angeles’ Joint Regional Intelligence Center (JRIC). The Constellation program and the ACAMS database provide intelligence analysts with the ability to cross-reference critical asset data and any available threat or intelligence information.

Protective Security Task Force
The CI/KR protection program employs Protective Security Task Forces (PSTF) to augment site security based on threat or intelligence information. A PSTF is a rapidly deployable group of police officers that temporarily provide low-profile security at critical assets. The PSTF is visible to an individual or group conducting pre-operational surveillance on an asset but not to the general public. The PSTF primarily seeks to deter individuals or groups observing a critical asset. A PSTF can be deployed without disrupting an asset’s normal business operations. Officers arrive at the site in plain-clothes and in unmarked cars.

Program Expansion
The California Office of Homeland Security and the U.S. Department of Homeland Security has supported the roll-out of ACAMS to California’s four CI/KR protection regions in 2006 through the Archangel Critical Asset Assessment Training (ACAAT) pilot program.

REQUIREMENTS

Keys to Success
- **Relationship-Building.** Trust is a critical component of successful public-private information sharing. The Archangel “business model” incorporates asset managers into protection and assessment efforts in order to gain their buy-in and build trust between the private sector and emergency responders. For example, sworn law enforcement officers and fire personnel conduct all assessments and emphasize emergency response concerns throughout the visit.
- **Protecting CI/KR data from disclosure:** CI/KR data received by ACAMS is validated as Protected Critical Infrastructure Information. PCII designation protects sensitive information from disclosure through the Freedom of Information Act (FOIA) and similar state and local disclosure laws and from use in civil litigation and regulatory actions. This protection is crucial for private sector entities that want assurances that shared information is safeguarded and not used inappropriately.
Any person authorized to access information held in ACAMS must first complete PCII training. In addition, non-federal employees must sign a non-disclosure agreement.

- **Technology.** The ACAMS platform provides the means for secure information flow and real-time data management. The system incorporates assessment methodologies, information sharing tools, and PCII compliance to provide an environment for data collection, storage, and reporting. ACAMS and/or other similar database systems can be leveraged as a data management solution to support implementation of the NIPP at the state and local level.

**Resources**
The CI/KR protection program is run by a core staff of four to eight Los Angeles Police Department Officers. The program was supported through the DHS Office of Grants and Training (G&T), the DHS Office of Infrastructure Protection (IP) Risk Management Division (RMD), the City of Los Angeles, and the California Office of Homeland Security.

**Training**

**ACAAT Training**
DHS and the State of California sponsored the Archangel Critical Asset Assessment Training (ACAAT) pilot program in 2006. The five-day course was provided to CI/KR assessors, intelligence analysts, counter-terrorism officials, and other public safety and first responder personnel throughout California. ACAAT was supported through the California Office of Homeland Security, DHS’ G&T, and DHS’ IP/RMD.

**CITATIONS**


McDonald, Lt. Tom. Officer in Charge, Operation Archangel, Los Angeles Police Department. Interview with *Lessons Learned Information Sharing*, 06 Sep 2006.

**DISCLAIMER**

*Lessons Learned Information Sharing (LLIS.gov)* is the US Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the emergency response and homeland security communities. The Web site and its contents are provided for informational purposes only, without warranty or guarantee of any kind, and do not represent the official positions of the US Department of Homeland Security. For more information on *LLIS.gov*, please email Feedback@llis.dhs.gov or visit [www.llis.gov](http://www.llis.gov).