

AGENDA
City of Los Angeles
EMERGENCY OPERATIONS BOARD

REGULAR MEETING

Tuesday, July 19, 2016
2:00 P.M.
Media Center Conference Room
Emergency Operations Center
500 E. Temple Street, Los Angeles, CA 90012

Members of the public are invited to address the Emergency Operations Board on any item on the agenda prior to action by the Board on that specific item. Members of the public may also address the Board on any matter within the subject matter jurisdiction of the Board. The Board will entertain such comments during the Public Comment Period. Public comment will be limited to two (2) minutes per individual for each item addressed, unless there are more than ten (10) comment cards for each item, in which case the public comment will be limited to one (1) minute per individual. The aforementioned limitation may be waived by the Chair of the Board.

(NOTE: Pursuant to Government Code Section 54954.3(b) the legislative body of a local agency may adopt reasonable regulations, including, but not limited to, regulations limiting the total amount of time allocated for public testimony on particular issues and for each individual speaker.)

Members of the public who wish to address the Board are urged to complete a Speaker Card and submit it to the Executive Assistant prior to commencement of the public meeting. The cards are available at the sign in table at the meeting or the Emergency Management Department public counter, Room 1533, City Hall. However, should a member of the public feel the need to address a matter while the meeting is in progress, a card may be obtained from the Executive Assistant to the Board, who will submit the completed card to the Chair of the Board prior to final consideration of the matter.

It is requested that individuals who require the services of a translator contact the Board Secretary no later than the day preceding the meeting. Whenever possible, a translator will be provided.

Sign language interpreters, assistive listening devices, or other auxiliary aids and/or services may be provided upon request. To ensure availability, you are advised to make your request at least 72 hours prior to the meeting you wish to attend.

NOTE: The meeting is tape-recorded and the tape is kept for 30 days.

I. Declaration of Quorum; Introductions; Approval of November 17, 2015 and March 15, 2016 Minutes

II. Action Items

A. November 19, 2015 Annual Emergency Operations Center (EOC) Functional Exercise After Action Report/Improvement Plan (AAR/IP) – Rob Freeman

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee, approve and forward to the Mayor for transmittal to the City Council, the November 19, 2015 Annual EOC Functional Exercise AAR/IP.

B. 2016 Los Angeles Marathon EOC Activation After Action Report/Corrective Action Plan (AAR/CAP) – Carol Parks

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee, approve and forward to the Mayor for transmittal to the City Council, the 2016 Los Angeles Marathon EOC Activation AAR/CAP.

C. City of Los Angeles 2016 Cyber Security Table Top Exercise After Action Report/Improvement Plan (AAR/IP) – Rob Freeman

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee, approve and forward to the Mayor for transmittal to the City Council, the City of Los Angeles 2016 Cyber Security Table Top Exercise AAR/IP.

D. UCLA Boelter Hall Active Shooter Emergency Operations Center (EOC) Activation After Action Report/Corrective Action Plan – Carol Parks

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee, approve and forward to the Mayor for transmittal to the City Council, the UCLA Boelter Hall Active Shooter EOC Activation AAR/CAP.

III. Information Items

- A. DSCA 101/Annual Exercise – Rob Freeman
- B. Annual Emergency Management Workshop – Rob Freeman
- C. LA Fleet Week – Carol Parks
- D. Firmin Street Orphan Wells Project – Chris Ipsen
- E. Pre-Positioned Antibiotics – Emily Helder
- F. Other Announcement – Board Members

IV. Presentations (as requested)

V. Public Comment Period

VI. Adjournment

Upon request, sign language interpretation, real-time translation services, agenda materials in alternative formats, and other accommodations are available to the public for City-sponsored meetings and events. All requests for reasonable accommodations must be made at least three working days (72-hours) in advance of the scheduled meeting date. For additional information, contact the Emergency Management Department at (213) 485-2121.

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: July 12, 2016

To: Charlie Beck, Chair
Emergency Operations Board

Emergency Operations Board Members

From: Anna Burton, Executive Assistant
Emergency Operations Board

A handwritten signature in black ink that reads 'Anna Burton'. The signature is written in a cursive, flowing style.

Subject: **CITY OF LOS ANGELES 2015 FUNCTIONAL EXERCISE
AFTER ACTION REPORT/IMPROVEMENT PLAN**

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee (EMC), approve the attached City of Los Angeles 2015 Functional Exercise After Action Report/Improvement Plan (AAR/IP) and forward to the Mayor for transmittal to the City Council.

Summary

On November 19, 2015, the City of Los Angeles Emergency Operations Center (EOC) was activated as part of a city-wide Functional Exercise (FE). This exercise was planned for eight (8) hours with a primary focus on the City's EOC processes, information sharing and regional coordination capabilities. This exercise was conducted in concert with a broader regional public health exercise focused on Medical Countermeasures (MCM) distribution and dispensing as a result of a biological attack. As such, the City EOC communicated and coordinated with other organizations and operations centers throughout the region that were also participating; particularly the County of Los Angeles Department of Public Health Department Operations Center (DOC) and the Los Angeles County Operational Area EOC.

Many City departments activated their Department Operations Center (DOC) or Bureau Operations Center (BOC) to coordinate and communicate with the City EOC. All impacts of the scenario, an anthrax attack in southern California, were simulated; however, EOC and DOC responders were required to perform their emergency responsibilities, including continuity of operations plan execution, as if the incident were real.

The attached AAR/IP provides a summary of the activation, identifies involved departments and agencies, and details the recommendations for future activations of the EOC. This report was approved by the EMC at its April 6, 2016, meeting. With approval by the EOB, EMD will forward to the Mayor for approval and transmittal to the City Council.

EMD will track areas recommended for improvement and, as appropriate, report back through the Emergency Operations Organization.

Attachment

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: March 29, 2016

To: Anna Burton, Emergency Management Committee Chair
Emergency Management Committee Members

From: Rob Freeman, Operations Division Chief
Emergency Management Department

Subject: **CITY OF LOS ANGELES 2015 FUNCTIONAL EXERCISE
AFTER ACTION REPORT/IMPROVEMENT PLAN**

Recommendation

That the Emergency Management Committee (EMC) approve the attached City of Los Angeles 2015 Functional Exercise After Action Report/Improvement Plan (AAR/IP) and forward to the Emergency Operations Board (EOB) for approval.

Summary

On November 19, 2015, the City of Los Angeles Emergency Operations Center (EOC) was activated as part of a city-wide Functional Exercise (FE). This exercise was planned for eight (8) hours with a primary focus on the City's EOC processes, information sharing and regional coordination capabilities. This exercise was conducted in concert with a broader regional public health exercise focused on Medical Countermeasures (MCM) distribution and dispensing as a result of a biological attack. As such, the City EOC communicated and coordinated with other organizations and operations centers throughout the region that were also participating; particularly the County of Los Angeles Department of Public Health Department Operations Center (DOC) and the Los Angeles County Operational Area EOC.

Many City departments activated their Department Operations Center (DOC) or Bureau Operations Center (BOC) to coordinate and communicate with the City EOC. All impacts of the scenario, an anthrax attack in southern California, were simulated; however, EOC and DOC responders were required to perform their emergency responsibilities, including continuity of operations plan execution, as if the incident were real.

The attached report provides a summary of the activation, identifies involved departments and agencies, and details the recommendations for future activations of the EOC. EMD will track areas recommended for improvement and, as appropriate, report back through the Emergency Management Committee and Emergency Operations Board.

Attachment – City of Los Angeles 2015 Functional Exercise After Action Report/Improvement Plan



City of Los Angeles 2015 Functional Exercise

November 19, 2015

After-Action Report/Improvement Plan

Publication Date: February 16, 2016



This page is intentionally blank.

EXERCISE OVERVIEW

Exercise Name	City of Los Angeles 2015 Functional Exercise
Sponsor	City of Los Angeles Emergency Management Department (EMD)
Exercise Dates/ Times	<p>Thursday, November 19, 2015</p> <p>Start of Exercise (StartEx): 8:00 a.m.</p> <p>End of Exercise (EndEx): 4:00 p.m.</p>
Scope	<p>This exercise was a city-wide Functional Exercise (FE) planned for eight (8) hours with a primary focus on the City Emergency Operations Center (EOC) at 500 E. Temple Street, Los Angeles, CA 90012. Many City Departments activated their respective Department Operations Centers (DOCs) at various locations throughout the City to coordinate and communicate with the City EOC during the exercise. Exercise play included EOC and DOC responders and liaisons from respective stakeholder groups and partner agencies that reported to the EOC or appropriate DOCs (e.g., Non-Governmental Organizations [NGOs], private industry, neighboring jurisdictions). This exercise was conducted in concert with a broader regional public health exercise focused on Medical Countermeasures (MCM) distribution and dispensing as a result of a biological terrorist attack. As such, the City EOC communicated and coordinated with other organizations and operations centers throughout the region that were also participating; particularly the County of Los Angeles Department of Public Health DOC. As a functional exercise, the event did not include the actual mobilization of resources to simulated incident locations. While all impacts of the scenario were notional; EOC and DOC responders were expected to perform their emergency responsibilities in accordance with plans and procedures as if the incident were real.</p>
Mission Area	Response
Core Capabilities	<ul style="list-style-type: none"> • Operational Coordination • Operational Communications • Situational Assessment • Planning • Public and Private Services and Resources • Public Health and Medical Services • Public Information and Warning

Objectives

- Demonstrate an effective Level 3 “Alpha” Activation of the City EOC appropriate and proportionate for the public health emergency and medical countermeasures response anticipated.
- Rehearse the EOC’s documented planning/coordination process for the “managed phase” of a public health emergency.
- In coordination with City DOCs and partner agencies, evaluate the City EOC’s ability to collect, prioritize, document, maintain, and disseminate situational awareness and a common operating picture regarding the City’s medical countermeasures response and the community-wide impacts of a public health emergency.
- Evaluate the ability of the City of Los Angeles to communicate with the Los Angeles County Department of Public Health (DPH) DOC to coordinate (including the integration of a Public Health Technical Specialist in the EOC Planning and Intelligence Section) and implement an effective medical countermeasures (MCM) response during a public health emergency; specifically, the dispensing of mass prophylaxis at eighty-nine (89) Points of Dispensing (PODs) in the City of Los Angeles.
- Evaluate the ability of the City of Los Angeles to coordinate, request resources, and share and receive situational information with the Operational Area EOC through a County of Los Angeles Office of Emergency Management (OEM) Agency Representative in the City EOC.
- Demonstrate an EOC resource management capability that facilitates the identification of resource needs, prioritization of competing requests, acquisition of appropriate resources, effective mobilization and tracking, and involves effective communications among relevant stakeholders throughout the process.
- Proclaim a Local Emergency and establish appropriate jurisdiction-wide priorities, strategies, policies, ordinances, rules, and regulations to address the current and foreseeable complexities of a public health emergency and to support or enhance mitigation and response measures.
- Implement an effective and customized emergency public information campaign that addresses the medical countermeasures response, mitigates community-wide impacts of a public health emergency, and solicits the input of the Los Angeles County Department of Public Health and other relevant partners.
- Demonstrate the ability of City DOCs to coordinate information, resources, and response priorities to address the impacts of a public health emergency on their specific department’s operations and in accordance with directives from the City EOC.
- Evaluate the ability of City of Los Angeles departments and agencies to select and implement appropriate continuity strategies as a result of personnel absenteeism rates between 30% - 50%.
- Effectively demonstrate the activation of the Disaster Service Worker (DSW) program across all city departments/agencies; and have each

Threat or Hazard

department support the mobilization of one thousand eight hundred (1,800) personnel per twelve (12)-hour shift in accordance with the “Activation of the Disaster Service Worker Program Standard Operating Procedure” (dated 10/10/2014).

Threat or Hazard

Biological Terrorist Attack (Anthrax)/Public Health Emergency

Scenario Synopsis

Approximately thirteen (13) hours before the start of the exercise, BioWatch Actionable Results (BARs) confirmed the presence of anthrax throughout Los Angeles County and Southern California. In addition, epidemiological reporting linked a number of people arriving at hospitals to potential anthrax symptoms. Based on intelligence received from law enforcement and through the Joint Regional Intelligence Center (JRIC), a correlation was made between the BAR detections and the plans of a terrorist organization to disperse dry anthrax spores (similar to the weapons-grade Ames strain) over Southern California using multiple aircraft. Due to anthrax’s extreme virulence and the widespread exposure, the Los Angeles County Public Health Officer, in coordination with Public Health Officers from across Southern California and the California Department of Public Health, declared health emergencies and requested medical countermeasures through the Strategic National Stockpile (SNS) in accordance with the Medical Countermeasures Plan for the Los Angeles County Operational Area (Annex 6 of the Los Angeles County Operational Area [LACOA] All-Hazards Emergency Response Plan [ERP]). In accordance with the plan, the population of Los Angeles County (approximately ten [10] million people) had to be provided prophylactic medications within forty-eight (48) hours of the decision to activate the SNS.

At the start of the exercise, medical and logistical supplies had arrived at all eighty-nine (89) Points of Dispensing (PODs) sites in the City of Los Angeles (simulated) and PODs were scheduled to open to the public within two (2) hours of the start of exercise (10:00 hours). Over the course of the exercise many challenges to medication distribution efforts at PODs were addressed: traffic management, infrastructure outages, illicit activity, organized protests, staffing and resource shortages, public inquiry and messaging, animal illnesses and concerns, Emergency Medical Services (EMS) and hospital surge, worried well, secondary contamination, etc.

Participating Organizations

The government of the City of Los Angeles is comprised of an Executive (the Mayor), City Council, and forty-three (43) City Departments and Bureaus. Collectively, these agencies comprise the City’s Emergency Operations Organization (EEO), a “department without walls,” responsible for the City’s emergency preparations (planning, training, exercising, and mitigation), response, and recovery operations. Each member of the EEO was invited to participate in the 2015 Citywide Functional Exercise by either

activating its respective DOC or deploying staff to the City EOC as appropriate. In addition, relevant stakeholders and emergency partners were invited to rehearse their respective roles in the City EOC in accordance with agreements and procedures (e.g., NGOs, private sector).

During the exercise, the City EOC was activated to a Level 3 (Full Activation) Alpha (Fire Department Lead) with approximately 100 EOC responders.

Eleven (11) DOCs and/or Bureau Operations Centers (BOCs) were also activated for the exercise, with each having various staffing levels depending on its individual protocols and objectives.

As previously stated, this exercise was conducted in concert with a broader regional public health exercise that included dozens of other response organizations at local, county, State, and Federal levels. This After-Action Report only addresses the participation of City of Los Angeles agencies.

The full list of participating City of Los Angeles agencies/organizations is included in Appendix B.

City of Los Angeles:

Rob Freeman
Emergency Management Coordinator II
City of Los Angeles Emergency Management Department
500 E. Temple Street
Los Angeles, CA 90012
(213) 484-4804 Office
Rob.Freeman@lacity.org

**Points of
Contact**

Contractor Support:

Nick Lowe, CEM, CBCP, MEP
Partner/Chief Operating Officer
Critical Preparedness and Response Solutions
(CPARS Consulting, LLC)
9552 Via Venezia
Burbank, CA 91504
(626) 320-0218 Office
NLowe@CPARSconsulting.com

ANALYSIS OF OBJECTIVES AND CORE CAPABILITIES

Aligning objectives and core capabilities for evaluation purposes transcends individual exercises to support ongoing and consistent preparedness reporting and trend analysis. Table 1 below includes the exercise objectives, aligned core capabilities, and a summary performance rating for each objective as determined by the evaluation team. The following sections then provide an overview of performance to justify the summary rating, highlighting strengths and areas for improvement.

Table 1. Summary of Objective and Capability Performance

(P – Performed Without Challenge, S – Performed with Some Challenge, M – Performed with Major Challenge, U – Unable to Perform)

Objective	Core Capability	Summary Rating			
		P	S	M	U
Demonstrate an effective Level 3 “Alpha” Activation of the City EOC appropriate and proportionate for the public health emergency and medical countermeasures response anticipated.	Operational Coordination Public Health and Medical Services		S		
Rehearse the EOC’s documented planning/coordination process for the “managed phase” of a public health emergency.	Operational Coordination Planning Situational Assessment Public Health and Medical Services		S		
In coordination with City DOCs and partner agencies, evaluate the City EOC’s ability to collect, prioritize, document, maintain, and disseminate situational awareness and a common operating picture regarding the City’s medical countermeasures response and the community-wide impacts of a public health emergency.	Situational Assessment Public Health and Medical Services			M	
Evaluate the ability of the City of Los Angeles to communicate with the Los Angeles County DPH DOC to coordinate (including the integration of a Public Health Technical Specialist in the EOC Planning and Intelligence Section) and implement an effective MCM response during a public health emergency; specifically, the dispensing of mass prophylaxis at eighty-nine (89) PODs in the City of Los Angeles.	Operational Communications Operational Coordination Situational Assessment Public Health and Medical Services			M	
Evaluate the ability of the City of Los Angeles to coordinate, request resources, and share and receive situational information with the Operational Area EOC through a County of Los Angeles OEM Agency Representative in the City EOC.	Operational Coordination Public and Private Services and Resources Situational Assessment			M	
Demonstrate an EOC resource management capability that facilitates the identification of resource needs, prioritization of competing requests, acquisition of appropriate resources, effective mobilization and tracking, and involves effective communications among relevant stakeholders throughout the process.	Operational Coordination Public and Private Services and Resources		S		
Proclaim a Local Emergency and establish appropriate jurisdiction-wide priorities, strategies, policies,	Planning	P			

Objective	Core Capability	Summary Rating			
		P	S	M	U
ordinances, rules, and regulations to address the current and foreseeable complexities of a public health emergency and to support or enhance mitigation and response measures.	Operational Coordination				
Implement an effective and customized emergency public information campaign that addresses the medical countermeasures response, mitigates community-wide impacts of a public health emergency, and solicits the input of the Los Angeles County DPH and other relevant partners.	Public Information and Warning			M	
Demonstrate the ability of City DOCs to coordinate information, resources, and response priorities to address the impacts of a public health emergency on their specific department’s operations and in accordance with directives from the City EOC.	Operational Coordination Planning Situational Assessment Public and Private Services and Resources			M	
Evaluate the ability of City of Los Angeles departments and agencies to select and implement appropriate continuity strategies as a result of personnel absenteeism rates between 30% - 50%.	Planning			M	
Effectively demonstrate the activation of the Disaster Service Worker (DSW) program across all city departments/ agencies; and have each department support the mobilization of one thousand eight hundred (1,800) personnel per twelve (12)-hour shift in accordance with the “Activation of the Disaster Service Worker Program Standard Operating Procedure” (dated 10/10/2014).	Operational Coordination Planning Public and Private Services and Resources		S		
<p>Ratings Definitions:</p> <p>1. Performed without Challenges (P): The critical tasks associated with the objective were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.</p> <p>2. Performed with Some Challenges (S): The critical tasks associated with the objective were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.</p> <p>3. Performed with Major Challenges (M): The critical tasks associated with the objective were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.</p> <p>4. Unable to be Performed (U): The critical tasks associated with the objective were not performed in a manner that achieved the objective(s).</p>					

Objective 1: Demonstrate an effective Level 3 “Alpha” Activation of the City EOC appropriate and proportionate for the public health emergency and medical countermeasures response anticipated.

The critical tasks associated with this objective were completed in a manner that achieved the objective; however, opportunities to enhance effectiveness and/or efficiency were identified. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, but in some cases it was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 1.1: The value of the Emergency Management Department’s (EMD’s) personnel in key leadership and supporting roles continued to be evident during this exercise. Of particular note, EOC personnel acknowledged the value of the EOC Coordinator and Deputy EOC Coordinator in helping to clarify processes and responsibilities, and as catalysts for actions needing to be taken. Likewise, the entire staff of the “Emergency Management Pod” was recognized for providing immediate technical assistance with WebEOC and other EOC systems/displays. EOC personnel also noted the value of the EMD EOC Deputy Director, Operations Section Deputy Coordinator, Liaison Officer (related to Agency Representatives), and EMD Assistant Public Information Officer (PIO), in serving as EOC subject-matter experts and providing advice and guidance throughout the exercise.

Strength 1.2: The addition of appropriate technical specialists (including representatives from the Los Angeles County Department of Public Health and the City of Los Angeles Department on Disability [regarding individuals with disabilities and others with access and functional needs]) dramatically increased the capabilities of the EOC and improved its resulting policies by complementing the City’s experience with additional relevant expertise. More importantly, these technical specialists were fully integrated into the EOC’s operations and decision-making, rather than being isolated to a specific area or task. Technical specialists may not have agreed with every decision made by the City, but their involvement at least ensured those decisions were fully informed.

Strength 1.3: The Liaison Officer did an excellent job of briefing Agency Representatives following every update he received and following coordination and planning meetings. The Liaison Officer’s briefings covered essential elements of information and ensured Agency Representatives maintained situational awareness (at least to the same degree of the Liaison Officer).

Strength 1.4: The Business Operations Center (BOC) employed an effective process for communicating relevant information to the BOC staff as well as making and tracking assignments. The BOC Director would diplomatically get BOC staff to listen, would then brief them on situation updates or incoming requests, and would then assign

responsibility to a suitable/available staff member. A dry/erase board was used to record the time and tracking number of each action, its requirements, the responsible position, and status updates over time. A spreadsheet was then generated to mirror the dry/erase board to memorialize the actions of the BOC.

Strength 1.5: The Department of Water and Power (DWP) staff assigned to the Utilities Branch came to the exercise with DWP laptops, which they used to directly access the three (3) DWP DOCs and real-time data on water and power systems.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 1.1: Selection of an EOC Director should be based on qualifications rather than discipline/department.

Reference(s): EOC Policy and Procedures Manual

Analysis: As a public health emergency, the scenario used for this exercise presented a unique situation that did not fit typical categories for classifying a disaster situation. At various points during the exercise and at post-exercise debriefings, participants questioned whether the lead should have been the Fire Department because of its medical/health responsibilities, the Police Department because the consequences of the emergency primarily resulted in crowd and traffic management/control issues, or the Emergency Management Department or another entity with a more “all hazards” focus. A very effective EOC Director was in place for the exercise; however, discussions of the alternatives concerned the evaluation team because each discussion focused on the EOC Director’s discipline rather than his/her capabilities. This is likely the result of an institutionalized culture that views the representatives from the Police and Fire Departments as the only qualified responders. The evaluation team collectively agreed an EOC Director should be selected based on capability over discipline/department. With appropriate subject-matter advisers, an EOC Director from any discipline/department can be successful so long as they have the appropriate understanding of EOC purpose and procedures, leadership skills, and associated capabilities. The City has a limited number of qualified EOC Directors and an extended emergency may tax those few resources, which will likely require qualified individuals to manage incidents not traditionally associated with their discipline/department.

Area for Improvement 1.2: Section Coordinators and Branch Directors tend to become involved in the individual tasks or minutiae assigned to their Sections/Branches at the cost of effective Section/Branch leadership and communications.

Reference(s): EMD EOC 301 Training (and future 400-level training courses)

Section Coordinator and Branch Director Position Checklists

EOC Policy and Procedures Manual

Analysis: During a full EOC activation it is the responsibility of the Section Coordinators and Branch Directors to delegate assignments to their Section’s/Branch’s staff and

transition their focus from individual tasks to management and leadership of the Section/Branch. During most of the City's past real-world EOC activations, which have all been a Level 1 or 2, the Section Coordinators and Branch Directors are responsible for fulfilling all the tasks of vacant units under them. As a result, they become accustomed to carrying out many of the individual tasks of the Section/Branch. In a Level 3 activation when the Section/Branch is fully staffed, the Section Coordinator/Branch Director should transition his/her focus from individual tasks to the management of the Section/Branch as a whole. This includes oversight of assignments, ensuring communications within and among Sections/Branches, monitoring adherence to procedures/policies/priorities, maintaining situational awareness, reassigning personnel and responsibilities as necessary, ensuring all necessary resources are being provided to Section/Branch staff, proactively establishing Section/Branch objectives, identifying shortfalls and areas of concern, conducting load balancing, and ensuring continuity of leadership (Section Coordinators, Branch Directors, and even the Management Section often left the EOC for extended durations without assigning an alternate to oversee operations in their absence). As observed during the exercise, all Section Coordinators and many Branch Directors struggled to some degree with these broader leadership responsibilities. As a result of leadership/management positions becoming sidetracked by minutiae, Sections and Branches failed to maintain situational awareness, tasks were delayed or not completed, and information was not communicated within or across Sections or Branches. This continues to be a perennial issue during the City's annual EOC exercises.

Area for Improvement 1.3: The role, composition, functionality, and coordination of Area (Bureau) Commands during widespread emergencies requires further development to achieve effective results.

Reference(s): City of Los Angeles Emergency Operations Master Plan and Procedures
EOC Policy and Procedures Manual
Department-Specific Emergency Operations Plans

Analysis: This exercise was used as an opportunity to test a new multi-agency Area Command concept for supporting tactical operations during widespread emergencies in the City of Los Angeles. The concept is very familiar within the Police and Fire Departments; however, even those two departments have little experience with multi-agency Area Commands that may include representatives from nearly every City department with a response function. The concept is virtually unknown to the other departments of the City. Based on the magnitude of the scenario (89 PODs) and geographic distribution of POD operations, this event was seen as an excellent opportunity to test the multi-agency Area Command concept. The four Area Commands (Central, South, Valley, and West) were simulated as an exercise artificiality; however, there was still a significant lack of clarity within DOCs and at the EOC, regarding how the Area Commands would operate (including role, composition, and functionality) and with whom and how they would communicate/coordinate (i.e., via which DOCs, directly with EOC Management, etc.). Through the exercise, the multi-agency Area Command concept demonstrated clear potential; however, a concerted planning, concept familiarization, training and exercise program will need to be created to facilitate effective multi-agency Area Command involvement in future real-world incidents.

This page is intentionally blank.

Objective 2: Rehearse the EOC’s documented planning/coordination process for the “managed phase” of a public health emergency.

Objective 3: In coordination with City DOCs and partner agencies, evaluate the City EOC’s ability to collect, prioritize, document, maintain, and disseminate situational awareness and a common operating picture regarding the City’s medical countermeasures response and the community-wide impacts of a public health emergency.

Objectives Two (2) and Three (3) are closely related and interdependent. As such, the evaluations of the two (2) have been listed together in this section. The critical tasks associated with these objectives were completed in a manner that achieved the objectives, but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with these objectives are described in this section.

Strengths

The following strengths related to these objectives were demonstrated during the exercise and contributed to the objectives being met:

Strength 2/3.1: Agendas, time limits, and intended outcomes were adhered to during the conduct and facilitation of EOC Coordination and Planning Meetings. With particular credit to the Planning and Intelligence Section Coordinator and EOC Coordinator, the Coordination and Planning Meetings were effectively managed and facilitated and resulted in the desired outcomes in the time allotted.

Strength 2/3.2: The Planning and Intelligence Section Coordinator, Deputy Section Coordinator, and Situation Analysis Unit Leader did an excellent job of following up with units throughout the EOC when clarity was needed regarding situation reports, additional information was needed, or critical information updates needed to be shared with EOC personnel. They promptly engaged relevant personnel in face-to-face communications to gather or share critical information.

Strength 2/3.3: Most Planning and Intelligence Section staff knew their jobs and performed them well (e.g., Situation Analysis Unit Leader, Documentation Unit Leader, Recovery Unit Leader), completing assignments quickly. The negative consequence of this was that they then often sat idle rather than being assigned by the Planning and Intelligence Section Coordinator to support other functions in need of support (See Area for Improvement 1.2).

Strength 2/3.4: By the end of the exercise, the Planning and Intelligence Section produced an EOC Coordination Plan for the next Operational Period which included Incident Objectives (EOC Form 902), Organization List (EOC Form 903), Communications List (EOC Form 905 and attachments), Organization Chart (EOC Form

907), Incident Summary (EOC Form 909; albeit cumbersome – see area for improvement 2/3.2), and supporting documents (list and map of POD sites). This was not only accomplished in a compressed timeframe, but also after strategic response strategies were changed multiple times during the exercise to adapt to the changing situation.

Strength 2/3.5: Showing improvement from the 2014 Functional Exercise, EOC Sections did a better job of utilizing break-out rooms to facilitate coordination and planning within their Sections. Break-out rooms were significantly underutilized during the 2014 exercise; however, during this exercise, rooms were pre-assigned to Sections in need of them (e.g., Planning and Intelligence, Operations) and were frequently used for internal Section meetings and updates.

Strength 2/3.6: The Business Operations Center (BOC) did an excellent job of reaching out into the EOC to connect with the other EOC Sections. Through those engagements, the BOC made the EOC aware of the resources to which it may have access and shared with the EOC the status of its constituents and their needs and expectations to inform decision-making.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with the objectives:

Area for Improvement 2/3.1: A lack of Section and Branch briefings to subordinates and insufficient information display/dissemination strategies resulted in a lack of awareness of critical information some EOC Sections had throughout the rest of the EOC (as appropriate).

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

EOC Coordination Process Forms and Procedures

EOC Branch/Section/Department Reports

EOC Display Plan

Analysis: 1) While situation updates were rendered during EOC coordination process meetings that included the Management and Coordination/General Staff, 2) while the Planning and Intelligence Section produced an EOC 909 Situation Report, and 3) while the Geographic Information System (GIS) Unit produced valuable maps; the information was not relayed to the EOC responders (as appropriate) nor displayed for their viewing. This is a perennial challenge for the City's EOC.

According to generally accepted ICS protocols, each EOC Section Coordinator, and in turn Branch Director, is to brief their Sections and Branches, respectively, on critical situation information and objectives/expectations following each briefing/meeting or as major developments occur. In many cases, these Section/Branch briefings did not occur or were limited to only a few staff. When they did occur, the content was often inconsistent and/or incomplete. In almost no case, was essential information relative to the Section/Branch, the status of other Sections (as appropriate), or EOC priorities and objectives regularly communicated to EOC responders (as appropriate) through the appropriate chain of command. One cause of these inconsistencies may be that few

Section Coordinators took notes during briefings/meetings despite being instructed to do so. Another cause may be that the Planning and Intelligence Section's 909 Incident Summary Report was not released to Section Coordinators/Branch Directors to assist with subsequent briefings. Another cause may be that position checklists for Section Coordinators and Branch Directors only reference briefing personnel under the initial activation activities. Those prompts are not repeated, nor do checklists identify what content should be included in those briefings (essential elements of information).

Although Section/Branch briefings would have made the most significant contribution to situational awareness/common operating picture, displays in the EOC could have helped mitigate the issue, but were not effectively used. A few of the EOC's large monitors were updated with static maps at various intervals, meeting times, and Branch/Section Report submission deadlines, but little else of much value was displayed. The GIS Unit could not keep maps updated in real-time because their workstations were not linked to the EOC's display system. The EOC Coordinator, for example, requested updated maps of POD sites and their status be posted on the large displays, but it only happened twice and the status information was inaccurate. In addition, each "pod" has a television that can be used by the Section Coordinator or Branch Director to display important information, tasks, maps, video, or other data. None of the "pods" used the television for any valuable purpose. Whether data is displayed on large displays, individual hard copies printed and handed out, documents placed on WebEOC for individual access, or information displayed on "pod" televisions; consistent and equal attention must be placed on providing EOC Sections and Branches with relevant and up-to-date information through any and all means available.

Area for Improvement 2/3.2: WebEOC has improved the reporting process for front-end users (e.g., Sections, Branches, Departments), but poses significant challenges to the compilation, validation, and production of synthesized macro-level intelligence on the back-end.

Reference(s): WebEOC

Analysis: The City has significantly increased the build out of the WebEOC boards and visual display interface since the 2014 Functional Exercise. Recent upgrades were tested for the first time during the 2015 exercise. One of the goals of the first phase work on WebEOC was to make the automated Branch and Section boards fast and easy-to-use for front-end users to upload situational information into template Section, Branch, and Department reports. During the exercise, the upgraded WebEOC did provide a faster and easy front end method to input situation information.

A second goal of the development phase was to provide the Planning and Intelligence Section the ability to draft the comprehensive, macro-level situation report for all meetings to support Management's critical decision making. Once incident information was entered, Branch and Section reports would be immediately accessible to the Planning and Intelligence Section. The final deliverable of the Section is to produce the Situation Report (EOC Form 909) from the inputs of individual Sections, Branches, and DOCs. Additionally, the Situation Report and Branch Report displays on WebEOC-boards is then an information sharing resource to ensure EOC responders are getting timely incident information.

During the exercise it was discovered that once entered into the system, Branch and Section inputs on the Situation Report could not be edited by the Situation Analysis Unit Leader. In addition, the Situation Analysis Unit Leader could not work on the input while it was being used by the front end-user. As a result, the reports included pages upon pages of situational information that was not redacted into a viable summarized Situation Report. To compensate, situational briefings from the Planning and Intelligence Section had to be quickly pulled together in the half-hour before the meetings from verbal talking points provided by EOC Section Coordinators and other leadership. The current version of WebEOC's information sharing boards did not support the Planning and Intelligence Section's role to: 1) dissect, validate, and vet raw incident reporting; and 2) provide good situation reporting through all resources including the displays. The technology challenges had a significant impact on the Section's process to develop a useful, significant, prioritized, and synthesized incident picture for management.

During the 2014 exercise, the EOC's approach to developing incident reports involved manually adding information to an MS Word document. While that was time consuming, it provided the Planning and Intelligence Section with direct capability to manage situation reporting inputs and to ensure all EOC Responders had guidance on the essential information needed. Working on merging the earlier information reporting resources with the speed and floor accessibility offered by using WebEOC, will significantly improve the reporting capabilities of the Planning and Intelligence Section.

Area for Improvement 2/3.3: Regular deadlines for the submission of situation updates should be established for all EOC Branches, Sections, and Departments regardless of the EOC Coordination Process schedule.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

Planning and Intelligence Section Coordinator Position Checklist

EOC Concept of Operations (ConOps)

Analysis: The exercise began at 08:30 hours, the EOC Coordination Meeting was scheduled for 12:30 hours, and the EOC Planning Meeting for 14:30 hours. Consequently, the Planning and Intelligence Section established 12:00 hours and 14:00 hours, respectively, as the only two deadlines for Branches, Sections, and Departments to submit situation reports. As a result, there was no urgency or action between 08:30 and 12:00 hours for any units to seek out and produce situation status updates. The Planning and Intelligence Section Coordinator instructed all personnel to notify the Planning and Intelligence Section if anything important happened in the interim; however, this request was open to wide interpretation and did not create a sense of urgency, so little to no action was taken. While Branch Directors, Section Coordinators, and Agency Representatives should not require a deadline to seek and maintain information regarding situation status as it is required in EOC procedures, position checklists, and is communicated through training; the EOC staff nonetheless demonstrated a penchant for being reactive versus proactive. This may be a result of exercise artificialities that don't effectively establish the same mindset of urgency and peril among participants as do real-world emergencies. Nonetheless, related to the exercise environment, these deadlines for

situation updates were important. The lack thereof led to limited situational awareness within the EOC and limited action on the part of EOC staff to address the void.

Area for Improvement 2/3.4: The staffing plan for the Situation Analysis Unit must have the capability to surge proportionate to the activation level and conditions.

Reference(s): EOC Staffing Plan (Form 903) and Organization Chart (Form 907)

Analysis: At the start of the exercise, the Situation Analysis Unit was staffed by only three (3) personnel. The Police Department did not staff its assigned support position, which would have made it four (4) and that information was never communicated to the Management Section. Within minutes, the Situation Analysis Unit was overwhelmed by the quantity of raw data it was receiving (e.g., data from all departments related continuity of operations, all Branches/Sections related to dispensing operations, 89 PODs, the County Department of Public Health). As a result, major deliverables were set aside (e.g., EOC 909 Forms, WebEOC Significant Events Lists, WebEOC Executive Dashboard for the Management Section) while the Unit tried to get its arms around its purpose and a process to synthesize raw data. While software issues and deficiencies in Section management exacerbated the issue, even a fully capable Situation Analysis Unit would have struggled with the same volume of data. The Planning and Intelligence Section Coordinator submitted a personnel resource request to the Logistics Section, but due to the exercise artificiality it could only be filled notionally. The capabilities of the Unit had nearly come to a halt when the EOC Coordinator recruited a number of EMD interns to provide support staffing. This was outside the exercise's parameters; however, the additional staff immediately increased the productivity of the Unit and it went on to develop an EOC 909 Incident Summary, POD status maps, and a rudimentary Significant Events List.

This page is intentionally blank.

Objective 4: Evaluate the ability of the City of Los Angeles to communicate with the Los Angeles County DPH DOC to coordinate (including the integration of a Public Health Technical Specialist in the EOC Planning and Intelligence Section) and implement an effective MCM response during a public health emergency; specifically, the dispensing of mass prophylaxis at eighty-nine (89) PODs in the City of Los Angeles.

The critical tasks associated with this objective were completed in a manner that achieved the objective, but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 4.1: The in-person involvement of County of Los Angeles Department of Public Health representatives in the City of Los Angeles' EOC created a rare and invaluable opportunity to enhance communications and understanding between the two entities. A Public Health Agency Representative provided process and policy guidance to the Management Section and a Technical Specialist provided detailed advice on plans and procedures to the Planning and Intelligence and Management Sections.

Strength 4.2: While ongoing and more frequent joint preparedness efforts are still necessary, this exercise's planning process presented an opportunity for the City of Los Angeles and County of Los Angeles Department of Public Health to collaborate on more emergency management than is the norm. Both entities demonstrated an eagerness to work together and collaborate beyond the exercise to improve planning and response capabilities.

Strength 4.3: Through coordination with the Public Health Technical Specialist and Disabilities and Access and Functional Needs (DAFN) Technical Specialist, the Animal Services Unit was able to establish two free-standing PODs for individuals with service animals.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 4.1: A process should be developed to fully define and inform EOC personnel of the role, chain of command, and location of Technical Specialists when activated.

Reference(s): EOC Staffing Plan (Form 903) and Organization Chart (Form 907)

Analysis: The inclusion of the Public Health Technical Specialist in the exercise was a tremendous strength; however, EOC Responders struggled to identify, engage, and understand the role of the Public Health Technical Specialist. The Public Health Technical Specialist was assigned to the Planning and Intelligence Section, but was seated at a workstation at the “Emergency Management Pod.” In addition, the Technical Specialist was assigned a generic “Technical Specialist” vest and no announcement was made that a Public Health Technical Specialist was available in the EOC, which made it difficult for those unfamiliar with him to identify him or know of his presence. Those that were aware of his presence were frequently confused as to his role. Although assigned to her Section, the Planning and Intelligence Section Coordinator took no responsibility for integrating the Public Health Technical Specialist or his expertise into the operations of that Section and its products (this was also true for the Disabilities, Access and Functional Needs [DAFN] Technical Specialist). The Public Health Technical Specialist was also called into most Management Section meetings (which was a strength); however, as a result, he was frequently absent from the EOC floor when consultations were needed and it gave EOC responders the impression he reported to the Management Section and his role might be policy-related and not technical. EOC responders were also unsure as to whether they could directly approach the Technical Specialist or whether formal requests for input had to go through a chain of command (e.g., the Planning and Intelligence Section Coordinator) or through WebEOC (e.g., information requests). As a result, the Technical Specialist was well engaged by the Management Section, but significantly underutilized by the rest of the EOC.

Area for Improvement 4.2: The Los Angeles County Department of Public Health must engage the City of Los Angeles in a thorough critique of its existing Medical Countermeasures and Mass Prophylaxis Plans.

Reference(s): Medical Countermeasures Plan for the Los Angeles County Operational Area (Annex 6 of the Los Angeles County Operational Area All-Hazards Emergency Response Plan) and supporting annexes and procedures

Analysis: The Medical Countermeasures Plan that was tested during the exercise was developed by the Los Angeles County Department of Public Health primarily without the input of the City of Los Angeles. As described with Area for Improvement 4.2, a public health emergency can leave the City of Los Angeles’ response at the mercy of the Health Officer or in conflict with Health Department’s policies/procedures. During both the planning for and conduct of the exercise, the City of Los Angeles identified a number of issues with the Public Health Department’s current Medical Countermeasures strategy. The City of Los Angeles would like to work with the Los Angeles County Department of Public Health to address the following items:

- Drive-through PODs should be a viable option and tool used for dispensing operations in the City of Los Angeles. Drive-through PODs have proven effective in other jurisdictions and the City of Los Angeles has the infrastructure and many viable POD locations to dramatically enhance throughput via drive-through PODs.

- The current POD locations selected by the Department of Public Health for the City of Los Angeles have not been vetted or approved. Approximately half of the City of Los Angeles' PODs are identified as Los Angeles Unified School District (LAUSD) sites. Neither the City nor the County have agreements with LAUSD to use their sites as PODs, and all LAUSD sites must be reconsidered. In addition, most of the PODs identified by the Public Health Department that are owned by the City of Los Angeles are facilities with minimal capabilities (e.g., limited parking, limited ingress/egress, non-ADA compliant, etc.). A vetting of all sites must be conducted to ensure they can support the intended POD objectives.
- The County's planning assumes the public will comply with all directives and few to no operational impediments (e.g., congestion, logistical delays, limited resource availability [including personnel]) will interfere with distribution or dispensing operations. The City of Los Angeles believes an incident of this magnitude, requiring activation of the Medical Countermeasures Plan for the Operational Area, will be a near catastrophic situation defined by major resource shortages, public misbehavior, extreme misinformation and rumors, major congestion, and distribution impediments, etc. As a result, the plan must realistically address these challenges and apply the appropriate resources, communication, and coordination necessary to achieve objectives.
- The current Medical Countermeasures Plan requires more than 45 staff at each POD for dispensing operations (this does not include ancillary functions such as traffic management, crowd management, mass care, public information, security, etc.). Future POD and Medical Countermeasure Plans should acknowledge potential staffing shortages and address the parameters for operating PODs with limited staffing or different staffing combinations. Future POD and Medical Countermeasure Plans should identify potential sources for personnel resources.
- The Medical Countermeasures Plan must include a pre-defined strategy for providing all emergency personnel involved with distribution and dispensing operations and the broader public safety and health community, and their families, with prophylactic medication in advance of their assignments to ensure assigned personnel will be willing and able to assist with emergency operations. The City of Los Angeles cannot guarantee any of its personnel, including sworn public safety staff, will be available to support mass prophylaxis activities without such assurances.
- PODs will report information to the Department of Public Health via multiple Service Planning Areas (SPAs). Data will then be summarized by the Public Health Department by SPA. The SPAs do not correlate to geographic or geopolitical boundaries. Portions of the City of Los Angeles are included in multiple SPAs; many of which also include other jurisdictions/territories beyond the City of Los Angeles. The SPA data Public Health reports to the City of Los Angeles will be of little to no value unless it is translated to City of Los Angeles boundaries.

This page is intentionally blank.

Objective 5: Evaluate the ability of the City of Los Angeles to coordinate, request resources, and share and receive situational information with the Operational Area EOC through a County of Los Angeles OEM Agency Representative in the City EOC.

The critical tasks associated with this objective were completed in a manner that achieved the objective, but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

No strengths were identified by the evaluation team related to this objective.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 5.1: There was either reluctance or an inability by the Operational Area (Office of Emergency Management) to assign a representative to the City of Los Angeles EOC in preparation for the exercise.

Reference(s): Joint City and County of Los Angeles (JCCLA) Memorandum of Understanding

Analysis: In preparation for the exercise, multiple requests were submitted to the Los Angeles County Office of Emergency Management (OEM) for an Operational Area liaison to staff a position in the City's EOC during the exercise. The Operational Area demonstrated a reluctance or inability to assign a liaison in advance of the exercise. Approximately fifteen (15) minutes after the start of the exercise, an OEM representative arrived at the City EOC – until that moment, the City was unsure if a representative would be participating and who that representative would be. According to the Joint City and County of Los Angeles (JCCLA) Memorandum of Understanding (JCCLA §3.b.3) the County will always and automatically assign an Operational Area liaison to the City EOC whenever it is activated. A formal request should not be required and there should be no debate on the subject. Likewise, whenever the City and County EOCs are activated for a common purpose, the City of Los Angeles is poised to send a City liaison to the County EOC without a formal request or undue delay (JCCLA §3.c). The County EOC was not activated for this exercise so that portion of the agreement was not demonstrated.

Area for Improvement 5.2: There was a missed opportunity to rehearse information sharing, strategy coordination, and resource management between the City of Los Angeles and Operational Area.

Reference(s): 2015 City of Los Angeles Functional Exercise, Exercise Plan (ExPlan)

Joint City and County of Los Angeles (JCCLA) Memorandum of Understanding

Analysis: The Operational Area EOC was ultimately unavailable to participate. The City of Los Angeles crafted this objective in the early stages of the exercise planning process with the anticipation of rehearsing information sharing, strategy coordination, and resource management between the City and Operational Area during the exercise. This objective could not be demonstrated because the Operational Area/OEM liaison assigned to the City EOC was not able to communicate with the County/Operational Area EOC to then provide back to the City EOC any information of value, offer OA policy/leadership input, or fulfill resource requests.

Area for Improvement 5.3: Because of the Operational Area’s limited participation, the potential consequences of the City’s strategic decisions and public information on other OA Members were not brought to its attention.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

EOC Coordination Process Forms and Procedures

Analysis: Credit is given to the City’s leadership for proactively making strategic decisions under pressure and in the absence of other guidance. However, many of the City’s decisions and public information releases would have had cascading impacts on neighboring jurisdictions experiencing the same incident and challenges. For example, during the exercise, the EOC Management Section instructed Area Commands to manage traffic in anyway necessary to improve throughput (e.g., re-route traffic, close streets, turn roads into one-way routes) and authorized “drive-through” PODs where necessary. These decisions would have likely had impacts on neighboring jurisdictions or other regional implications. For example, many of the City’s PODs are located along City borders with neighboring jurisdictions. Changing traffic patterns around those PODs could create traffic consequences in the neighboring jurisdiction. Likewise, word of “drive-through” PODs in the City of Los Angeles could drastically change the public’s reaction to dispensing operations at “walk up” PODs throughout the rest of the Operational Area. It is the role of the Operational Area to identify, communicate, and adjudicate these cross-jurisdictional issues to ensure the resilience of the entire region not just the City of Los Angeles. As stated in Area for Improvement 5.2, the lack of participation by the Operational Area was a missed opportunity to rehearse this adjudication process between the City of Los Angeles and the Operational Area (on behalf of all other OA Members).

Objective 6: Demonstrate an EOC resource management capability that facilitates the identification of resource needs, prioritization of competing requests, acquisition of appropriate resources, effective mobilization and tracking, and involves effective communications among relevant stakeholders throughout the process.

The critical tasks associated with this objective were completed in a manner that achieved the objective; however, opportunities to enhance effectiveness and/or efficiency were identified. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, but in some cases it was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 6.1: Upgrades to WebEOC and subsequent trainings on WebEOC since the 2014 Functional Exercise allowed EOC responders to use the system for relaying three (3) types of resource requests: 1) information requests between individual positions; 2) mission taskings between Branches in the Operations Section; and 3) tangible resources from any EOC Section to the Logistics Section. In addition, WebEOC now allows request originators to attach files to the resource request within WebEOC, which not only saves transcription time, but ensures clarity. Use of the system helped improve the communication of essential elements of information and ensured resource requests reached intended recipients.

Strength 6.2: Demonstrating marked improvement from the 2014 Functional Exercise, the Logistics Section had a better grasp on the entire resource management process, particularly related to receiving and acknowledging resource requests from various Sections, vetting resource requests for essential elements of information, identifying internal city resources, and prioritizing resource requests when limited resources were available. In a number of cases the Logistics Section Coordinator was able to take a step back from individual tasks to provide just-in-time refresher training on the resource management process to section personnel.

Strength 6.3: The Finance and Administration Section developed an informative policy document providing detailed guidance on how to track costs for cost recovery purposes. The guidance document included information on the Cost Accounting System (i.e., disaster accounting codes) established by the Finance and Administration Section within two (2) hours of the start of the exercise. The guidance document was then conveyed to EOC Section Coordinators verbally, a hard copy was printed and handed out, and a copy was emailed to all EOC responders via WebEOC.

Strength 6.4: The EOC Coordinator, Deputy EOC Coordinator, and Emergency Management Department staff were helpful in consulting with Branches and Sections to

de-conflict resource requests and identify the appropriate channels through which to direct resource requests (i.e., mass care related requests that were elevated through the Fire/EMS Branch were properly directed to the Mass Care Branch with the input of the EOC Coordinator).

Strength 6.5: The three (3) Logistics Section Units staffed by the General Services Department (Supply, Ground Support, and Facilities) were proactive in identifying and inventorying city resources that may have been available to support the mass prophylaxis campaign.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 6.1: The capability to track resource fulfillment from the submission of a resource request to the mobilization and delivery of non-city resources was insufficient.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

Analysis: There was no observed interaction between the Logistics Section and the Resource Status Unit within the Planning and Intelligence Section. The Resource Status Unit should be notified when a resource request is received, when it is fulfilled and arrives, and if and when it is submitted to the Operational Area. In addition, the Resource Status Unit should be notified if the Logistics Section or others identify resource-related trends or potential shortfalls so those issues can be addressed through the EOC's planning/coordination process. This communication may occur with the assistance of technology (e.g., WebEOC) or in a manual process so long as the communication is maintained. Likewise, resource status information is of little value if it is not communicated to those with a need to know. Resource requestors (e.g., Operations Section Branches) should know how to review the status of their resource requests via WebEOC. In addition, communications between resource requestors and the Logistics Section should be improved on both sides: 1) the resource requestor should be more proactive in seeking updates from the Logistics Section; and 2) the Logistics Section should be more forthcoming with the dissemination of resource fulfillment updates.

Area for Improvement 6.2: The Finance and Administration Section needs to be more familiar with and able to manage the City's disaster procurement authorities.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

City of Los Angeles Emergency Procurement Authorities/Policies

Analysis: During the exercise, the Finance and Administration Section was presented with multiple prompts that should have triggered staff to identify and explain the City's emergency procurement authorities (e.g., circumvent the bid process, waive contracting requirements and licenses, increase/exceed spending limits, enter into non-traditional agreements, make cash purchases, etc.). While the Finance and Administration Section demonstrated some awareness of elements of the City's overall policy (e.g., spending limits) it failed to demonstrate a complete understanding of the entire process and

authorities. An awareness of that process should have then triggered closer coordination with the Logistics Section in the pursuit of resources.

In addition, the continuity of the City's procurement authority (systems and processes) falls on the Finance and Administration Section. The Section was unable to address multiple requests for information on the delegation of procurement authorities among City personnel. Complete awareness of the City's procurement capabilities (particularly the procurement flexibilities granted under a Proclamation of Local Emergency) and an ability to manage and maintain the process by the Finance and Administration Section is critical to the City's resource fulfillment abilities.

Area for Improvement 6.3: Coordination between the Logistics Section and Finance and Administration Section must be improved to support effective resource acquisition and financial tracking.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

Analysis: Within the first ten (10) minutes of the exercise, the Logistics and Finance and Administration Section Coordinators held a joint briefing which addressed the responsibilities of both Sections and introduced staff across Sections. Unfortunately, this level of coordination was not carried throughout the rest of the exercise. At no point did the Logistics and Finance and Administration Sections meet to discuss the process for acquiring non-city resources, available financial tools, and procurement flexibilities and limitations. As demonstrated through their side-by-side placement in the EOC, the Logistics and Finance and Administration Sections are mutually dependent; not only related to fulfilling resource requests, but also related to financial tracking, cost recovery, and supporting personnel needs (e.g., claims/compensation).

This page is intentionally blank.

Objective 7: Proclaim a Local Emergency and establish appropriate jurisdiction-wide priorities, strategies, policies, ordinances, rules, and regulations to address the current and foreseeable complexities of a public health emergency and to support or enhance mitigation and response measures.

The critical tasks associated with this objective were completed in a manner that achieved the objective; however, opportunities to enhance effectiveness and/or efficiency were identified. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, but in some cases it was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 7.1: Within the first hour of the exercise, the Management Section recognized the magnitude of the situation/scenario and promptly proclaimed a Local State of Emergency for the City of Los Angeles; acknowledging the necessity of a proclamation and the multiple benefits it offers the City's response and recovery efforts.

Strength 7.2: The EOC Director, with consultation from the two Deputy Directors, did not hesitate to make difficult decisions regarding the City's priorities, policies, or provide authorizations. Again recognizing the urgency and magnitude of the situation, the Management Section quickly addressed impediments to the mass prophylaxis campaign.

Strength 7.3: The Management Section proactively began considering the possible short- and long-term implications of the incident and response operations. They did not get caught up in only the current situation, but rather began to consider issues for the next and future Operational Periods; including the potential need for decontamination, medical and fatality management surge capabilities once prophylactic medications are no longer effective, and the long-term mental health impacts on City personnel and the community as a whole.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 7.1: Certain EOC personnel, particularly in the Operations and Management Sections, need to be more familiar with the City's emergency powers and authorities so they can recognize situations that may warrant their activation and thereby proactively request action.

Reference(s): City of Los Angeles Administrative Code (LAAC), Division 8 - Special Authorities, Chapter 3 - Local Emergencies

Analysis: A Proclamation of Emergency gives the Mayor, and thereby the emergency organization of the City of Los Angeles, a great deal of authority to take actions that could mitigate challenges and benefit response and recovery activities. Some of those authorities may include:

- Controlling and directing the entire emergency organization of the City
- Requiring emergency service of any City officer or employee (Disaster Service Workers)
- Requisitioning necessary personnel or material of any City department or agency
- Binding the city to the fair value of any resource or, if urgent, commandeering the same for public use
- Population control measures (e.g., curfews, evacuations, restricted areas)
- Prevention of price gouging
- Restrictions/parameters on certain sales (e.g., alcohol, fuel, firearms, food)
- Approval of tactics with political/legal ramifications
- Permit/license/requirement suspensions

This exercise and its scenario offered an excellent opportunity for the Operations Section to proactively request the implementation of emergency powers to mitigate potential complications and support the mass prophylaxis campaign. However, EOC responders did not demonstrate a thorough understanding of the potential policies, ordinances, rules, and regulations that could benefit their efforts. As a result, the Management Section was not approached to implement those special authorities. Based on overall EOC performance, it can also be assumed that if EOC responders were aware of the authorities, they may not have known the process by which they should submit policy requests to the Management Section for consideration.

Area for Improvement 7.2: Awareness of City-wide priorities, proclamations, and policies (e.g., Common Operating Picture) was not communicated as necessary throughout the EOC.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

EOC Coordination Process Forms and Procedures

Analysis: This issue directly relates to the root cause identified in Area for Improvement 2.1 associated with Objective 2. While the City Proclaimed a Local State of Emergency in the first few hours of the response, notification of the proclamation was not made to necessary positions in the EOC. The Proclamation affects many EOC Sections, for example:

- It must be communicated to the Operational Area via the Operational Area Agency Representative or Planning and Intelligence Section.
- It activates the emergency powers/authorities of the Mayor, which the Planning and Intelligence and Operations Section must be aware of when identifying policies that could benefit tactical operations.
- It creates legal and liability protections and flexibilities, which affect the Finance and Administration Section.
- It authorizes the City to request resources from the Operational Area and creates procurement flexibilities, which both the Logistics and Finance and Administration Sections must be aware of as they pursue resources.

The Proclamation, however, was not the only policy not communicated to necessary groups in the EOC. The Management Section authorized the Disaster Service Worker (DSW) program, but that information was only shared with the Logistics Section. During the exercise, the Management Section directly authorized the four Area Commands to use any methods necessary to enhance throughput at PODs (including converting walk-through PODs to drive-through PODs, altering traffic patterns, increasing security, etc.). Those decisions had cascading impacts on the Operations Section and respective DOCs, but it was not communicated to appropriate positions in the EOC. During the initial floor briefing by the EOC Director, a shelter-in-place order from the Operational Area Policy Group was conveyed to the EOC, but no further briefings or information releases addressed other policies or provided updates.

This page is intentionally blank.

Objective 8: Implement an effective and customized emergency public information campaign that addresses the medical countermeasures response, mitigates community-wide impacts of a public health emergency, and solicits the input of the Los Angeles County DPH and other relevant partners.

The critical tasks associated with this objective were completed in a manner that achieved the objective, but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 8.1: The Public Information staff was knowledgeable of the major public information task requirements. Upon activation, major tasks such as media monitoring, rumor control, media outlet identification, message development, WebEOC entry, and media briefing area set-up were listed on the group's dry/erase board and identified as tasks that needed to be accomplished by the team.

Strength 8.2: During the exercise, WebEOC was used to publish/share at least three (3) public information messages. The content of the messages was intended to reassure the public with respect to the actions the City of Los Angeles was taking to address the situation, facts about the hazard/threat, information regarding the location of PODs, and what do with pets/service animals as coordinated with the Mass Care Branch.

Strength 8.3: The Public Information staff recognized the need for regular media briefings and scheduled hourly media briefings (nationalized) for the duration of the event.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 8.1: The Public Information function was not adequately staffed for the magnitude of the public information campaign and used that as a reason to notionalize all its functions.

Reference(s): EOC Staffing Plan (Form 903) and Organization Chart (Form 907)

Analysis: During the exercise there were only three (3) agency representatives staffing the Public Information function. This led the Public Information staff to make a decision to notionalize all exercise activities instead of performing tasks and actions as if the incident were real as instructed by Exercise Control staff. This created a missed

opportunity to play through the challenges, prioritize activities using the staff available, propose/discuss priorities with the Management Section, and request additional support. Since the Public Information function reports to the EOC Director and Deputy Directors, it was an oversight on the part of management that the public information function lapsed and was not set on a corrected course.

With the 30-50% projected absenteeism rate associated with this scenario, performance of all desired public information functions would be challenging if the incident had been real. This exercise artificiality turned out to be a reality with only three (3) staff members present. In a real world emergency, notionalizing the public information functions would not be an option. Regardless of known or perceived staff availability, the Public Information staff needs to request resources required to do all the essential public information functions and do its best to produce in the interim. Creative staffing options (using non-technical personnel to monitor the media, for example) and requesting assistance from all potential sources (e.g., mutual aid) should be considered whenever a staffing shortfall occurs.

Area for Improvement 8.2: A thoughtful and strategic Public Information Plan was not developed to guide the overall public information campaign/strategy.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

PIO Position Checklists

Analysis: Developing an overall strategy for the public information campaign would have allowed the PIO and the public information staff to develop a strategic approach for managing emergency public information, handling rumor control, coordinating messages, identifying the functions required, and prioritize messages and activities. It is an efficient way to articulate the overall public information approach to the Management Section. Although Public Information procedures, checklists, and training all address the need, timing, and content for said plan, no such plan was developed during the exercise. As a result, the public information function failed to make functional assignments, track actions and progress, and consistently share information as a group regarding the functions and actions that each other were taking. This eventually led to a reactionary operation where staff only tackled the issues they were directly presented verses being proactive. In addition, the lack of process and information management would make it difficult for staff from the next operational period to transition and track trends and operational progress.

Area for Improvement 8.3: Crisis information was not gathered from or shared with the EOC or DOCs and was not coordinated with the Los Angeles County Joint Information Center (JIC).

Reference(s): City of Los Angeles Emergency Operations Master Plan and Procedures

Analysis: Public information is a critical function of the EOC. The mismanagement of public information can have a devastating impact on both the jurisdiction as well as the public. It is essential that accurate, timely, and consistent information be disseminated to the public. It is also essential that the Public Information group work closely with all EOC Section Coordinators as part of the EOC information gathering and sharing process.

The public information group did not have a handle on the types of messaging required to have a successful public information campaign. Although initially the group produced three (3) relevant press releases, the operation became reactionary and did not include advance planning or anticipation of message needs based on communication and situational awareness that would have come from communicating with other EOC Section, appropriate DOCs, and the County JIC.

The only messages coordinated and approved for release during the exercise were generic (e.g., “what is government doing,” POD locations, and some information about the hazard/threat). No messages were published with respect to public safety, employee safety, directions regarding the shelter-in-place order, or any “one message/many voices” in concert with the Los Angeles County JIC or Public Health Department regarding POD access, hours, resources, where to find medication instructions, etc.

Although regular media briefings were scheduled, the messaging and the coordination to determine the appropriate messenger (Mayor, Police/Fire Chief, joint conferences with Los Angeles County Department of Public Health, etc.) were not developed with information from EOC Sections, DOCs, or other public information partners.

This page is intentionally blank.

Objective 9: Demonstrate the ability of City DOCs to coordinate information, resources, and response priorities to address the impacts of a public health emergency on their specific department’s operations and in accordance with directives from the City EOC.

The critical tasks associated with this objective were completed in a manner that achieved the objective, but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 9.1: During the exercise, DOCs and BOCs with pre-existing Standard Operating Procedures (SOPs) worked through those documented processes and actively adapted those that were not effective by adding or modifying elements to include operationally appropriate steps. DOCs generally did an exceptional job of identifying procedural deficiencies or inaccuracies within understood or documented processes. For example, when the Department of Recreation and Parks (RAP) identified gaps, inconsistencies, or inefficiencies in information flow between the field, DOC and EOC, it immediately altered the process, information or communication flow to resolve the issue. Similarly, when the Los Angeles Police Department’s Real-Time Analysis and Critical Response (RACR) Division determined that additional information or training was required to accompany its pre-established policies, it catalogued the gaps, and altered standard reporting charts to more accurately represent useful situational awareness.

Strength 9.2: Many DOCs reported strong leadership from their DOC staff. This included taking proactive steps to improve DOC efficiency by establishing communication processes with staff, conducting meetings/briefings, reviewing DOC and position responsibilities as a group, adjudicating roles where confusion existed, and providing a common direction for the DOC.

Strength 9.3: Many DOCs utilized a myriad of available tools to track and share information as well as track task status. For example, RAP, the Housing and Community Investment Department (HCIDLA), and the Information Technology Agency (ITA) reported the creation of activity logs and tracking sheets that were shared in real-time on “Google Drives” throughout the DOC. Department representative(s) in the EOC also had access to the Google Drives and shared documentation. This tracking showed itemized lists of Department priorities and activities that allowed for real-time status tracking, “load balancing,” and adjustments to the delegation of assignments as necessary during the exercise.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 9.1: The City of Los Angeles' DOC-centric emergency operations model is dependent on the successful performance of DOCs; however, each DOC has its own understanding of its purpose and the degree of DOC capabilities varies widely in the absence of a centralized policy and framework.

Reference(s): City of Los Angeles Emergency Operations Master Plan and Procedures
DOC Operations Manual or Framework

Analysis: Under the emergency operations structure used in the City of Los Angeles, each Department is responsible for establishing and operating a DOC to manage and coordinate response and recovery efforts for its internal operations as well as to the community relevant to its discipline. The success of the City's overall response is dependent on the performance of each DOC in its area of service. DOCs are, in essence, their own EOCs, responsible for establishing department/discipline priorities and policies, communicating and coordinating with relevant stakeholders, and managing information and resources for the department. The City EOC then exists to support the needs of those individual DOCs and adjudicate issues across DOCs when they arise.

From the DOCs that participated in the exercise, frustration was shared regarding the lack of consistency and general understanding between DOCs and the EOC regarding the mission and purpose of each entity. While some operational nuances are to be expected among DOCs, the need/desire for a consistent understanding of purpose, structure, and communications was evident. While a number of DOCs had established their own processes prior to the exercise, the exercise made evident that a number of DOCs were not staffed with appropriate personnel (either quantity or expertise), did not understand the overall City structure or roles associated with the field (including Area Commands), and critical information pathways were not established or utilized between the EOC and DOCs. Significant challenges were present in coordinating objectives, situational information, communicating appropriate information, accounting for Department personnel, and the status of essential functions.

Area for Improvement 9.2: Departments do not have enough trained staff to perform DOC functions for full DOC activations or to cover operations lasting more than one Operational Period.

Reference(s): City of Los Angeles Administrative Code (LAAC), Division 8 - Special Authorities, Chapter 3 - Local Emergencies
City of Los Angeles Emergency Operations Master Plan and Procedures
Mayor's Executive Order #15 and #17
DOC Operations Manual or Framework

Analysis: Even DOCs with robust plans, equipment, and capabilities fall short with their numbers of trained and qualified staff to operate DOCs, particularly in large scale

incidents or over multiple Operational Periods. This exercise demonstrated a number of perennial issues regarding department priorities related to emergency preparedness, in particular, not proactively assigning and training a sufficient number of staff to be DOC responders, and not mandating those individuals access the tools and participate in events necessary to successfully fill the position assigned. This issue is equally true of department approaches for staffing the City EOC.

Area for Improvement 9.3: A Common Operating Picture (COP) and Citywide priorities were not communicated to each DOC from the EOC.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

EOC Coordination Process Forms and Procedures

Analysis: This evaluation directly relates to Area for Improvement 2/3.1. Because situational information and the status of policies and priorities were not effectively communicated throughout the EOC, they were not then relayed from the EOC to DOCs. Most DOCs commented that the EOC felt like a “black hole.” Information (relevant or not) was shared from DOCs to the EOC, but very little information was provided back to each DOC. The briefings and situational updates that were provided to the EOC Management Section needed to be shared with all EOC Sections and positions, as well as with each DOC, as appropriate. Of particular concern was a lack of employee health and safety information, the anthrax threat, or any plans for distributing medication to agencies other than the Police Department and Fire Department.

Area for Improvement 9.4: WebEOC is not currently available at DOCs, but could help improve DOC/EOC communications if made available.

Reference(s): WebEOC Software, Policies, and Training

Analysis: WebEOC (like other emergency management information systems) is a highly customizable and robust communications platform that has the ability to support situational awareness, resource management, action/coordination planning, and communications across many organizations and user-groups in different locations. With more than 40 departments, bureaus, and offices, the City of Los Angeles would benefit from universal accessibility throughout the Emergency Operations Organization (EOO). Reinforcing the corrective actions from the After Action Reports for the City’s 2013 and 2014 Functional Exercises, WebEOC enhancements still need to be done to improve the system’s use among DOCs and the EOC. While DOCs should not be trained to be solely dependent on a computer-based information system, it can significantly contribute to the efficiency and effectiveness of emergency operations when it is available and fully utilized by all elements of the City’s response network.

This page is intentionally blank.

Objective 10: Evaluate the ability of City of Los Angeles departments and agencies to select and implement appropriate continuity strategies as a result of personnel absenteeism rates between 30% - 50%.

The critical tasks associated with this objective were completed in a manner that achieved the objective, but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 10.1: Despite departments not officially activating their Continuity of Operations Plans (COOP), a few departments evaluated essential functions and the use/assignment of staff for the chosen priority functions.

Strength 10.2: During the planning for and conduct of the exercise, HCIDLA took the opportunity to prepare/review COOP checklists and used them to prioritize essential functions during the exercise, and thereby make decisions on the suspension of functions and assignment of staff.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 10.1: The importance of activating Department COOP Plans or implementing continuity strategies was not recognized as a priority by the EOC or most DOCs despite the scenario.

Reference(s): City of Los Angeles Department COOP Plans

Analysis: While the need for additional staff was recognized as a priority by the activation of the Disaster Services Worker (DSW) program, further acknowledgement of other strategies to prioritize City functions to free up resources were not. The EOC Management Section did not make a recommendation to the Mayor to direct the activation of COOP Plans, nor did it encourage City departments to assess their essential functions and reduce operational capacity to minimum levels to free up resources for emergency functions. In addition, there was no discussion of EMD Bulletins (a common tool for recommending emergency measures) be used to recommend that Department's implement continuity strategies. Even without an executive-level recommendation, the scenario (and associated absenteeism rates) should have made it obvious that continuity plans were necessary. However, no DOC recognized the indicators and officially activated their COOP Plans. Most DOC responders acknowledged a lack of familiarity

with continuity concepts and many noted their departments either do not have a current COOP Plan or are not familiar enough with the plan to exercise/use it.

Area for Improvement 10.2: DOC personnel were unaware of the process for requesting additional staff (non-emergency, emergency, DSW, and otherwise) from the EOC.

Reference(s): City of Los Angeles EOC Policy and Procedures Manual

City of Los Angeles Department COOP Plans

Analysis: While DOC responders were challenged with the lack of personnel resources, they were equally perplexed regarding the process to fill personnel gaps. They were unaware that the DOC/EOC resource request process is the same for personnel as it is for all other types of resources. In addition, they failed understand the DOC/EOC resource request process is not limited to field activities, but is available to support any and all essential functions of the City. The root cause for this confusion lays in a general lack of understanding of the tenants of the COOP, resource management, and DSW programs and how they complement each other.

Objective 11: Effectively demonstrate the activation of the Disaster Service Worker (DSW) program across all city departments/agencies; and have each department support the mobilization of one thousand eight hundred (1,800) personnel per twelve (12)-hour shift in accordance with the “Activation of the Disaster Service Worker Program Standard Operating Procedure” (dated 10/10/2014).

The critical tasks associated with this objective were completed in a manner that achieved the objective; however, opportunities to enhance effectiveness and/or efficiency were identified. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, but in some cases it was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 11.1: The Management Section immediately recognized the need to activate the DSW program to support operational needs. During the Management Section’s initial organizing meeting at 08:40 hours, the EOC Deputy Director instructed an assistant to review the DSW procedures, arrange to send an EMD bulletin, and connect with the Personnel Department to initiate the process. The Mayor’s Liaison was tasked with seeking the Mayor’s approval. The Mayor’s Liaison was aware of the draft policy memorandum and quickly sought approval from the Mayor (simulated) to implement the program. The approval process was informed and timely.

Strength 11.2: The EOC Personnel Unit Leader and Personnel DOC staff was very knowledgeable about the tasks required to implement the DSW program. The Personnel Unit Leader had a mastery of the process and shared it with other key stakeholders (e.g., Logistics Section Coordinator, Public Information Officer, Management Section) to ensure the program’s proper activation. In addition, the Personnel DOC staff understood all the steps needing to occur to seek out DSWs from the City’s departments/agencies/bureaus to satisfy the resource request once the program was activated.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 11.1: Awareness of, and training on, the DSW activation Standard Operating Procedure (SOP) is limited and may currently result in single points of failure. The exercise demonstrated there are insufficient resources to implement the program to acquire large numbers of personnel.

Reference(s): “Activation of the Disaster Service Worker Program” Standard Operating Procedure and Training

Analysis: While it was very clear the Personnel Unit Leader understood his responsibilities related to the activation of the DSW program; the process and individual roles in the process were not as clear to the other key stakeholders involved, particularly the role and involvement of Department DOCs. The DSW Activation SOP was developed in 2014 and most of the past SOP training has been limited to Department Personnel Officers (DPOs). At the time of the exercise, it appeared the successful implementation of the program was dependent on a few informed individuals within the Personnel Department and only the DPOs from each Department. Awareness of the SOP and training on it for all involved positions will be essential to future activations.

As articulated in the City’s 2014 Functional Exercise After-Action Report, activating the DSW program is not straightforward and requires significant resources. As demonstrated during the exercise, when the DSW program was activated it required many more individuals (Personnel DOC cadre, DPOs, and supervisors) to notify, identify, and activate available personnel and match skill sets to the need. As a result of the intensity of the task, only one hundred and eighty seven (187) DSWs were identified for the first shift and three hundred and thirty eight (338) for the second shift, during the entire exercise (1,800 were needed for each shift).

Area for Improvement 11.2: DOCs were not made aware of the activation of the DSW program.

Reference(s): “Activation of the Disaster Service Worker Program” Standard Operating Procedure and Training

Analysis: While the need for the DSW program was recognized early in the exercise; because situational information, policies, and priorities were not effectively communicated throughout the EOC and DOCs, information regarding the activation of the DSW program was not properly communicated. Activation of the DSW program is something that affects every City Department, whether they provide the Department an avenue to find additional personnel or the Department is selected to provide resources to another Department whose operations are impacted. In either case, every Department must be made aware of the activation of the program.

Area for Improvement 11.3: The functionality of the DSW program and its personnel resources were misunderstood by many elements in the EOC.

Reference(s): “Activation of the Disaster Service Worker Program” Standard Operating Procedure and Training

Analysis: Those aware of the DSW program activation (e.g., the Management Section, Section Coordinators) presumed DSWs were the solution for every personnel resource

gap without understanding the skillsets, process, or availability. This led to a failure to recognize a serious personnel shortage when only one hundred and eighty seven (187) of eighteen hundred (1,800) DSWs were identified for the first shift and three hundred and thirty eight (338) for the second. Leadership positions improperly assumed all personnel shortages would be filled by DSWs without further consideration. No follow-on discussions ensued to create strategies to compensate for the lack of available personnel resources.

In addition, the DSW request that was initiated by the Los Angeles County Department of Public Health was summarily rejected by the Management Section, who indicated, “the City will use City staff to support City operations.” The request from Los Angeles County clearly stated the request for personnel was intended to support operations at the eighty-nine (89) PODs within the City. In addition to root causes identified in Area for Improvement 4.2 (regarding DPH and City coordination), these cases appear to result from a general lack of familiarity with the DSW process, how requests are processed, and the intended purpose and use of DSW personnel.

This page is intentionally blank.

APPENDIX A: IMPROVEMENT PLAN

Based on the evaluations contained in this After-Action Report, this Improvement Plan (IP) has been developed to capture the corrective actions agreed to by the participating organizations and identifies information relevant to the monitoring of progress related to each corrective action.

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
Objective 1: Demonstrate an effective Level 3 "Alpha" Activation of the City EOC appropriate and proportionate for the public health emergency and medical countermeasures response anticipated.	1.1: Selection of an EOC Director should be based on qualifications rather than discipline/department.	EMD will continue to pursue Corrective Actions 1.1.2 (Staffing Requirements) and 1.1.4 (EOC Staff Credentialing) from the 2014 Functional Exercise Improvement Plan.	Planning Organization	High	EMD	Operations Division	Ongoing	April 2017
		1.1.1. Upon development of a credentialing program, EMD will develop a list of qualified/credentialed EOC Directors.	Organization	Medium	EMD	Operations Division	Dependent on the completion of Corrective Actions 1.1.2 and 1.1.4 from the 2014 Improvement Plan	Within 6 Months
	1.2: Section Coordinators and Branch Directors tend to become involved in the individual tasks or minutiae assigned to their Sections/Branches at the cost of effective Section/Branch	EMD will continue to pursue Corrective Actions 1.1.2 (Staffing Requirements) and 1.1.4 (EOC Staff Credentialing) from the 2014 Functional Exercise Improvement Plan.	Planning Organization	High	EMD	Operations Division	Ongoing	April 2017
		1.2.1. Training for Section Coordinators and Branch Directors will continue to emphasize the importance	Training	Medium	EMD	Operations Division, Training Unit	Ongoing	Ongoing

¹ Capability Elements are: Planning, Organization, Equipment, Training, or Exercise.

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	leadership and communications.	of managing the effectiveness and efficiency of the Section/Branch as a whole and future trainings (e.g., 400-level) will also emphasize this role.						
		1.2.2. Position checklists will be revised to better capture the leadership/management responsibilities of Section Coordinators and Branch Directors to include more direct prompts for such activities.	Planning	High	EMD	Operations Division	June 2016	June 2017
		1.2.3. EMD will develop a strategy for offering more frequent and accessible (e.g., online) trainings, drills, and exercise opportunities for EOC personnel to rehearse their skills more often than once a year.	Training Exercise	High	EMD	Operations Division	Ongoing	August 2016
	1.3: The role, composition, functionality, and coordination of Area (Bureau) Commands during widespread emergencies requires further development to achieve effective results.	1.3.1. The Fire, Police, and Emergency Management Departments will reaffirm the value and intended ongoing use of the Bureau/Area Command model for wide-scale incident management.	Planning Organization	Medium	Fire Department	TBD	February 2016	August 2016
		1.3.2. Upon a decision to continue the Bureau/Area Command model, the Fire Dept. will engage all departments that may play a	Planning Training Exercise	Medium	Fire Department	TBD	Dependent on the results of Corrective Action 1.3.1	Within 1 Year

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		role in multi-agency Area Commands in a formal planning and concept development process, along with the creation of a training and exercise program to address the role, composition, functionality and coordination of multi-agency Area Commands.						
<p>Objective 2: Rehearse the EOC's documented planning/coordination process for the "managed phase" of a public health emergency.</p> <p>Objective 3: In coordination with City DOCs and partner agencies, evaluate the City EOC's ability to collect, prioritize, document, maintain, and disseminate situational awareness and a common operating picture regarding the City's medical countermeasures</p>	<p>2/3.1: A lack of Section and Branch briefings to subordinates and insufficient information display/dissemination strategies resulted in a lack of awareness of critical information some EOC Sections had throughout the rest of the EOC (as appropriate).</p>	EMD will continue to pursue Corrective Actions 1.1.2 (Staffing Requirements) and 1.1.4 (EOC Staff Credentialing) from the 2014 Functional Exercise Improvement Plan.	Planning Organization	High	EMD	Operations Division	Ongoing	April 2017
		2/3.1.1. EOC checklists and the EOC Concept of Operations Template will be updated to include prompts and content (essential elements of information) for the regular Section and Branch briefings required in the EOC Policy and Procedures Manual.	Planning	High	EMD	Operations Division	June 2016	June 2017
		2/3.1.2. Training for Section Coordinators and Branch Directors will continue to emphasize the importance of Section/Branch Briefings and information sharing and future trainings (e.g., 400-level) will also emphasize this function.	Training	Medium	EMD	Operations Division, Training Unit	Ongoing	Ongoing

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
response and the community-wide impacts of a public health emergency.		2/3.1.3. EMD will review its EOC information dissemination and display strategies, and make enhancements as appropriate, to ensure the strategies include all relevant tools and systems (e.g., hard copies, emails, maps, briefings, video displays [GIS connectivity to displays], “Pod” televisions, WebEOC) available to reduce the workload on EOC personnel and offer the widest and most useful distribution.	Planning	High	EMD	Operations Division	February 2016	August 2016
		2/3.1.4. The EMD will consider expanding the EOC Coordinator function/Emergency Management “pod” to provide a greater capacity for Section Coordinator and Branch Director coaching during real-world activations.	Organization	High	EMD	Operations Division	February 2016	August 2016
	2/3.2: WebEOC has improved the reporting process for front-end users (e.g., Sections, Branches, Departments), but poses significant challenges to the compilation,	2/3.2.1. A comprehensive review of WebEOC will occur to include EMD staff with Planning & Intelligence Section experience to address the needed revisions to WebEOC information sharing boards to facilitate the EOC’s	Equipment	High	EMD	Operations Division Planning Unit	Ongoing	February 2017

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	validation, and production of synthesized macro-level intelligence on the back-end.	process for situational awareness, information sharing, and the needs of the Planning and Intelligence Section.						
		2/3.2.2. The EOC Form 909 reporting feature within WebEOC will be modified to give the Planning and Intelligence Section complete editorial control over the report's contents and formatting without having to change the original inputs.	Equipment	High	EMD	Operations Division, Training Unit	Ongoing	November 2016
	2/3.3: Regular deadlines for the submission of situation updates should be established for all EOC Branches, Sections, and Departments regardless of the EOC Coordination Process schedule.	2/3.3.1. The EOC Concept of Operations and potentially WebEOC boards/notices will be updated to include prompts for regular deadlines for situation reports to contribute to ongoing situational awareness, regardless of the EOC Coordination Process schedule.	Planning Equipment	Low	EMD	Planning Unit Operations Division	August 2016	February 2017
		2/3.3.2. EMD EOC Training (particularly its 301 course and future 400-level courses) will continue to reinforce the need for each unit to seek out and maintain information on situation status regardless of whether it's been	Training	Low	EMD	Operations Division, Training Unit	Ongoing	Ongoing

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		assigned that responsibility or a deadline.						
	2/3.4: The staffing plan for the Situation Analysis Unit must have the capability to surge proportionate to the activation level and conditions.	2/3.4.1. EMD EOC Training (particularly its 301 course and future 400-level courses) will continue to reinforce the need for each unit to assess staffing needs and proactively request personnel resources as needed.	Training	Low	EMD	Operations Division, Training Unit	Ongoing	Ongoing
Objective 4: Evaluate the ability of the City of Los Angeles to communicate with the Los Angeles County DPH DOC to coordinate (including the integration of a Public Health Technical Specialist in the EOC Planning and Intelligence Section) and implement an effective MCM response during a public health emergency; specifically, the dispensing of mass prophylaxis at eighty-nine (89)	4.1: A process should be developed to fully define and inform EOC personnel of the role, chain of command, and location of Technical Specialists when activated.	4.1.1. A simple checklist or procedure will be developed detailing the process by which a Technical Specialist is on-boarded, where they are positioned (i.e., as a Technical Specialist assigned to a Section, Agency Representative assigned to the Liaison Officer, etc.), how the EOC is made aware of their presence, and the process for EOC personnel to engage the Technical Specialist.	Planning	Medium	EMD	Operations Division	February 2016	August 2016
	4.2: The Los Angeles County Department of Public Health must engage the City of Los Angeles in a thorough critique of its existing Medical Countermeasures and Mass	4.2.1. The EMD and Los Angeles County DPH will jointly review, critique, and identify solutions to improve the Medical Countermeasures Plan for the Operational Area to ensure practicality and address the concerns	Planning	High	LA County DPH EMD	EPRP Policy and Planning Division Planning Unit	February 2016	February 2017

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
PODs in the City of Los Angeles.	Prophylaxis Plans.	identified in this report. The DPH will ultimately revise the Medical Countermeasures plan as appropriate.						
		4.2.2. Los Angeles County DPH will provide the EMD with the position papers DPH is authoring related to the Medical Countermeasures Plan for review and comment.	Planning	High	LA County DPH	EPRP Policy and Planning Division	February 2016	February 2017
Objective 5: Evaluate the ability of the City of Los Angeles to coordinate, request resources, and share and receive situational information with the Operational Area EOC through a County of Los Angeles OEM Agency Representative in the City EOC.	5.1: There was either reluctance or an inability by the Operational Area (Office of Emergency Management) to assign a representative to the City of Los Angeles EOC in preparation for the exercise.	5.1.1. The Los Angeles County OEM should institutionalize a process and capability to identify and automatically deploy a qualified Operational Area liaison to the City of Los Angeles EOC whenever it is activated.	Planning Organization	High	LA County OEM	Administrator	February 2016	Ongoing
		5.1.2. The EMD will continue to invite Operational Area liaisons to the City's EOC training courses to ensure their familiarity with and ability to operate within the City's EOC.	Training	Medium	EMD	Operations Division, Training Unit	In Progress	Ongoing
	5.2: There was a missed opportunity to rehearse information sharing, strategy coordination, and resource management	5.2.1. The City and County of Los Angeles should jointly agree to participate in future regional training and exercise events to take advantage of as many opportunities as possible to	Training Exercise	High	EMD LA County OEM	General Manager Administrator	In Progress	Ongoing

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	between the City of Los Angeles and Operational Area.	rehearse information sharing, strategy coordination, and resource management.						
	5.3: Because of the Operational Area's limited participation, the potential consequences of the City's strategic decisions and public information on other OA Members were not brought to its attention.	There are no additional correction actions beyond those associated with Area for Improvement 5.2.						
Objective 6: Demonstrate an EOC resource management capability that facilitates the identification of resource needs, prioritization of competing requests, acquisition of appropriate resources, effective mobilization and tracking, and involves effective communications among relevant stakeholders	6.1: The capability to track resource fulfillment from the submission of a resource request to the mobilization and delivery of non-city resources was insufficient.	6.1.1. The EOC Policy and Procedures Manual will be updated, or a supporting Standard Operating Procedure will be developed, to define the process and assignments for resource status tracking.	Planning	Medium	EMD	Planning Unit	September 2016	February 2017
		6.1.2. A quick reference checklist or guide will be developed for the Logistics Section that provides prompts for the resource status tracking procedure.	Planning	Low	EMD	Planning Unit	Contingent Upon Corrective Action 6.1.1	TBD
		6.1.3. The EMD and GSD will review the capabilities of WebEOC to determine how best it can be used for resource status tracking and associated information sharing.	Equipment	High	EMD GSD	Operations Division Emergency Management Coordinators	June 2016	February 2017

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
throughout the process.		6.1.4. EOC trainings will continue to describe the resource status tracking process and future 400-level EOC trainings will provide additional details and opportunities to rehearse the process.	Training	Medium	EMD	Operations Division, Training Unit	In Progress	Ongoing
	6.2: The Finance and Administration Section needs to be more familiar with and able to manage the City's disaster procurement authorities.	6.2.1. The EOC Policy and Procedures Manual will be updated, or a supporting Standard Operating Procedure will be developed, to define the Finance and Administration Section's role in the resource acquisition process; including the roles of the Procurement Unit, Contract Administration Unit, and potentially the Legal and Compensation/ Claims Units in the resource management cycle.	Planning	Medium	EMD	Planning Unit	September 2016	February 2017
		6.2.2. The EOC Policy and Procedures Manual and appropriate EOC position checklists will be revised to include references to the City's emergency procurement authorities/policies and associated procedures.	Planning	Medium	EMD	Planning Unit	September 2016	February 2017
		6.2.3. Future 400-level Finance and Administration Section training will be	Training	Medium	EMD	Operations Division, Training Unit	TBD	TBD

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		designed to address the Section's role and procedures in facilitating emergency procurements.						
	6.3: Coordination between the Logistics Section and Finance and Administration Section must be improved to support effective resource acquisition and financial tracking.	Either future trainings or separate drills for the Logistics and Finance and Administration Sections (e.g., 400-level or potentially joint trainings or drills) will address the symbiotic relationship between the two Sections related to resource acquisition.	Training Exercise	Low	EMD	Operations Division, Training Unit	TBD	TBD
Objective 7: Proclaim a Local Emergency and establish appropriate jurisdiction-wide priorities, strategies, policies, ordinances, rules, and regulations to address the current and foreseeable complexities of a public health emergency and to support or enhance mitigation and response measures.	7.1: Certain EOC personnel, particularly in the Operations and Management Sections, need to be more familiar with the City's emergency powers and authorities so they can recognize situations that may warrant their activation and thereby proactively request action.	7.1.1. Either the EOC Policy and Procedures Manual will be revised or a supplemental fact sheet developed that identifies the menu of potential emergency authorities of the City and a process by which said authorities may be requested within the EOC.	Planning	Medium	EMD	Operations Division Planning Unit	February 2016	August 2016
		7.1.2. Appropriate EOC position checklists (e.g., Operations and Management Sections) will be updated to list the potential emergency authorities of the City, or at a minimum, provide a prompt for personnel to consider the need to request emergency authorities.	Planning	Low	EMD	Operations Division Planning Unit	June 2016	June 2017

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	7.2: Awareness of City-wide priorities, proclamations, and policies (e.g., Common Operating Picture) was not communicated as necessary throughout the EOC.	There are no additional corrective actions beyond those associated with Area for Improvement 2/3.1.						
Objective 8: Implement an effective and customized emergency public information campaign that addresses the medical countermeasures response, mitigates community-wide impacts of a public health emergency, and solicits the input of the Los Angeles County DPH and other relevant partners.	8.1: The Pubic Information function was not adequately staffed for the magnitude of the public information campaign and used that as a reason to notionalize all its functions.	There are no additional corrective actions beyond those associated with Area for Improvement 2/3.4.						
	8.2: A thoughtful and strategic Public Information Plan was not developed to guide the overall public information campaign/strategy.	EMD will continue to pursue Corrective Actions 1.1.2 (Staffing Requirements) and 1.1.4 (EOC Staff Credentialing) from the 2014 Functional Exercise Improvement Plan.	Planning Organization	High	EMD	Operations Division	Ongoing	April 2017
		8.2.1. A template for a Public Information Plan will be developed for quick reference and population during a real-world incident.	Planning	Medium	EMD	Public Information	February 2016	August 2016
	8.3: Crisis information was not gathered from or shared with the EOC or DOCs and was not	EMD will continue to pursue Corrective Actions 1.1.2 (Staffing Requirements) and 1.1.4 (EOC Staff Credentialing) from the	Planning Organization	High	EMD	Operations Division	Ongoing	April 2017

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	coordinated with the Los Angeles County Joint Information Center (JIC).	2014 Functional Exercise Improvement Plan. 8.3.1. Current and future PIO trainings (e.g., 301 and 400-level) will continue to communicate the importance of working with the EOC Section Coordinators and Management to maintain situational awareness, provide the EOC with data from media/public-sources, and the importance of proactive messaging.	Training	Low	EMD	Public Information Operations Division, Training Unit	Ongoing	Ongoing
Objective 9: Demonstrate the ability of City DOCs to coordinate information, resources, and response priorities to address the impacts of a public health emergency on their specific department's operations and in accordance with directives from the City EOC.	9.1: The City of Los Angeles' DOC-centric emergency operations model is dependent on the successful performance of DOCs; however, each DOC has its own understanding of its purpose and the degree of DOC capabilities varies widely in the absence of a centralized policy and framework.	9.1.1. Departments/agencies in need of DOC guidance will continue to proactively contact the EMD for support and information on best practices. EMD will provide support, including for the development of DOC ConOps Plans (9.1.4), upon request.	Planning Organization Training	High	All Departments/Agencies/Bureaus with DOCs/BOCs	Emergency Management Coordinators	In Progress	Ongoing
		9.1.2. EMD will distribute its "DOC Training" materials to all departments via the EMC Operations Subcommittee.	Training	High	EMD	Operations Division, Training Unit	February 2016	March 2016
		9.1.3. The EMD will host a Train-the-Trainer session for its "DOC Training" open to all departments.	Training	High	EMD	Operations Division, Training Unit	February 2016	August 2016
		9.1.4. All departments with DOCs will develop a DOC Concept of Operations	Planning	High	All Departments/Agencies/Bureaus with DOCs/BOCs	Emergency Management Coordinators	February 2016	February 2017

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		(ConOps) if one doesn't exist covering all critical elements addressed in SEMS and in EMD's "DOC Training."						
	9.2: Departments do not have enough trained staff to perform DOC functions for full DOC activations or to cover operations lasting more than one Operational Period.	9.2.1. All departments with DOCs will develop a recommended staffing plan for their DOC (positions and depth) for approval by their respective department's leadership.	Planning Organization	Medium	All Departments/Agencies/Bureaus with DOCs/BOCs	Emergency Management Coordinators	February 2016	August 2017
	9.3: A Common Operating Picture (COP) and Citywide priorities were not communicated to each DOC from the EOC.	9.3.1. Checklists for Agency Representatives, Branch Directors, and Unit Leaders (as appropriate), will be revised to include prompts for providing briefings/updates from the EOC to DOCs on a regular basis and shall identify essential elements of information to include in those updates. (Similar to how EOC Section Coordinator checklists will provide the same for their Section staff).	Planning	Medium	EMD	Planning Unit	February 2016	August 2016
		9.3.2. EOC training will continue to, and be enhanced as necessary to emphasize, the importance of providing two-way information between the	Training	Medium	EMD	Operations Division, Training Unit	In Progress	Ongoing

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		DOCs and EOC, and emphasize the role of Agency Representatives, Branch Directors and Unit Leaders (as appropriate) in relaying information back to DOCs and not just from DOCs to the EOC.						
		Per Corrective Action 1.1.4 from the 2014 Functional Exercise AAR, the EMD continue to pursue the development of a formal program to certify/credential EOC responders through a combination of testing, training, exercise, and/or real-world experience (e.g., formalizing existing efforts and filling in gaps as necessary over time) and issue said policy through appropriate channels (e.g., Mayoral Memo) to maintain a capable cadre of EOC responders and a constant state of EOC readiness.	Planning Organization	High	EMD	Operations Division	Ongoing	April 2017
	9.4: WebEOC is not currently available at DOCs, but could help improve DOC/EOC communications if made available.	9.4.1. The EMD will continue its efforts to acquire funding for the expansion of WebEOC to the City's DOCs.	Equipment	High	EMD	Operations Division	In Progress	August 2016
		9.4.2. Through the EMC Operations Subcommittee, the EMD will seek guidance from DOCs on how to	Equipment	High	EMD	Operations Division	June 2016	February 2017

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		customize WebEOC for DOC use and how to structure the system to best facilitate the interface between the EOC and DOCs.						
		9.4.3. When and if WebEOC is expanded to DOCs, then EMD will expand its WebEOC training offerings (both content and frequency) to address DOC responders.	Training	High	EMD	Operations Division	Contingent Upon Corrective Action 9.4.1	Ongoing
Objective 10: Evaluate the ability of City of Los Angeles departments and agencies to select and implement appropriate continuity strategies as a result of personnel absenteeism rates between 30% - 50%.	10.1: The importance of activating Department COOP Plans or implementing continuity strategies was not recognized as a priority by the EOC or most DOCs despite the scenario.	10.1.1. As a supplement to the City-wide COOP Plan Template issued by the EMD, the EMD will develop guidelines or suggested trigger points that better explain under what conditions a General Manager should consider activation of their department COOP plan.	Planning	Medium	EMD	Planning Unit	February 2016	August 2016
		10.1.2. Associated with Corrective Action 9.1.4, Departments will include trigger points for or references to the activation of department COOP Plans in their DOC ConOps Plans.	Planning	High	All Departments/ Agencies/Bureaus with DOCs/BOCs	Emergency Management Coordinators	February 2016	February 2017
	10.2: DOC personnel were unaware of the process for requesting additional staff (non-	10.2.1. EMD training will continue to address the resource request process applicable to all resource types.	Training	Low	EMD	Operations Division, Training Unit	February 2016	August 2016

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	emergency, emergency, DSW, and otherwise) from the EOC.	10.2.2. EOC/DOC training materials will be revised to include at least one example of a personnel resource request to reinforce that personnel requests follow the same process as all other tangible resource requests.	Training	Low	EMD	Operations Division, Training Unit	February 2016	August 2016
11: Effectively demonstrate the activation of the Disaster Service Worker (DSW) program across all city departments/agencies; and have each department support the mobilization of one thousand eight hundred (1,800) personnel per twelve (12)-hour shift in accordance with the "Activation of the Disaster Service Worker Program Standard Operating Procedure" (dated 10/10/2014).	11.1: Awareness of, and training on, the DSW activation Standard Operating Procedure (SOP) is limited and may currently result in single points of failure. The exercise demonstrated there are insufficient resources to implement the program to acquire large numbers of personnel.	11.1.1. The DSW SOP will be revised to include procedures for coordination between Department DPOs and their respective DOCs or Department Leadership.	Planning	High	EMD	Special Projects Division	February 2016	August 2016
		11.1.2. The DSW SOP will be revised to include procedures for how DPOs will properly mobilize DSW personnel.	Planning	High	EMD	Special Projects Division	February 2016	August 2016
		11.1.3. Department DPOs should pre-establish job classification lists (per the DSW SOP) for the personnel of their respective department.	Planning Organization	Medium	Personnel Department	All DPOs	February 2016	February 2017
		11.1.4. The "Implementation and Training" section of the DSW SOP will be enhanced to include a more robust training and exercise strategy that includes a list of types of trainings and exercises to be conducted, an inclusive list of all individuals/ positions that	Planning Training Exercise	High	EMD	Special Projects Division	February 2016	August 2016

Objective	Issue/Area for Improvement	Corrective Action	Capability Element ¹	Priority	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		need training, the target audience for each type of training, and the frequency of offerings. The training and exercises will reflect a building-block approach that grows in complexity and capability with each offering. The EMD and Personnel Department will apply the appropriate resources to implement the enhanced training and exercise strategy identified.						
	11.2: DOCs were not made aware of the activation of the DSW program.	11.2.1. The EOC 909 Form will be revised to include a check box to identify whether the DSW program has been activated.	Planning	Medium	EMD	Planning Unit	February 2016	March 2016
	11.3: The functionality of the DSW program and its personnel resources were misunderstood by many elements in the EOC.	11.3.1. EMD will develop a one-page fact sheet explaining the DSW program's purpose, authorities, and general process.	Planning	Low	EMD	Special Projects Division	August 2016	February 2017
		11.3.2. The EOC 301 training will be revised to mention and quickly explain the DSW program.	Training	Low	EMD	Operations Division, Training Unit	August 2016	February 2017

This page is intentionally blank.

APPENDIX B: EXERCISE PARTICIPANTS

Participating Organizations	Level of Play
City of Los Angeles	
Animal Services	City EOC Staffing, DOC Activation and Drill Activities
Department of Building and Safety (DBS)	City EOC Staffing
Department on Disability	City EOC Staffing
Department of Public Works/Bureau of Contract Admin (BCA)	City EOC Staffing
Department of Public Works/Bureau of Engineering (BOE)	City EOC Staffing (GIS only)
Department of Public Works/Bureau of Sanitation (BOS)	City EOC Staffing, BOC Activation
Department of Public Works/Bureau of Street Lighting (Street Lighting)	City EOC Staffing
Department of Public Works/Bureau of Street Services (BSS)	City EOC Staffing
Department of Recreation and Parks	City EOC Staffing, DOC Activation
Department of Transportation	City EOC Staffing, DOC Activation
Department of Water and Power	City EOC Staffing
Emergency Management Department	City EOC Staffing
Fire Department	City EOC Staffing, DOC Activation
General Services Department (GSD)	City EOC Staffing, DOC Activation
Harbor Department/Port of Los Angeles	City EOC Staffing
Housing & Community Investment Department (HCIDLA)	City EOC Staffing, DOC Activation
Housing Authority (HACLA)	City EOC Staffing
Information Technology Agency (ITA)	City EOC Staffing, DOC Activation
Los Angeles World Airports	City EOC Staffing, DOC Activation
Office of the Chief Legislative Analyst	City EOC Staffing
Office of the City Clerk	DOC Simulation
Office of the City Administrative Officer	City EOC Staffing
Personnel Department	City EOC Staffing, DOC Activation
Police Department	City EOC Staffing, DOC Activation
County	
Los Angeles County Office of Emergency Management	City EOC Staffing
Los Angeles County Department of Public Health	City EOC Staffing
Other Stakeholders	
American Red Cross (ARC) - Greater Los Angeles Chapter	City EOC Staffing, EOC Activation
Los Angeles Unified School District	City EOC Staffing
Los Angeles Emergency Preparedness Foundation	City EOC Staffing, BOC Activation

This page is intentionally blank.

APPENDIX C: PARTICIPANT FEEDBACK SUMMARY

Number of Respondents	Ninety-five (95)
% Who had participated in prior EOC trainings	76% of respondents had taken EOC 101 71% of respondents had taken EOC 201 61% of respondents had taken EOC 301
Summary of Demonstrated Strengths	<ul style="list-style-type: none">• Teamwork (78%)²• EOC processes worked well (69%)• Use of WebEOC (16%)• Resources were helpful (9%)• Facility capabilities facilitated functions (4%)•
Summary of Areas for Improvement	<ul style="list-style-type: none">• Section coordination (41%)• Information sharing and flow (33%)• Resource request coordination and process (24%)• Understanding of EOC roles (21%)• Streamlining of paperwork required to complete processes (8%)• Ability to maintain situational awareness (7%)
Summary of Recommended Improvements	<ul style="list-style-type: none">• Equipment and facilities (40%)• WebEOC (35%)• Smoother processes (32%)• More exercises and training (20%)• Real-time mapping capabilities (3%)

FEEDBACK DETAILS

The feedback details contained here include an analysis and consolidation of the feedback received on all ninety-five (95) Participant Feedback Forms. Both paper and electronic (Survey Monkey) responses were reviewed. All comments were not included verbatim in this analysis; however, all comments were considered and consolidated into representative and like feedback entries. Specific and detailed comments were included as appropriate. Illegible comments were not included. In addition, comment modifiers are not included (e.g., if “staff support” was listed

² Percentages show the percentage of total respondents that shared the same or similar comment.

as a strength that is how it is listed below). Comments that received multiple responses were noted with a percentage indicating the percentage of the total respondents that made a similar comment.

DEMONSTRATED STRENGTHS

Teamwork (78%)

- Open communication between agencies. (21%)
- Collaborative environment made information sharing a success. (8%)
- Branch leaders are excellent, knowledgeable resources. (2%)
- Strong collaboration with BOC. (2%)
- Smooth phone communication with LADWP.
- Creative problem solving.
- Good communication with LAFD DOC.
- LAPD successfully communicated within and across sections.
- Smooth DOC to EOC communication for both Recs and Parks and Mass Care.
- Coordination between Section Coordinators much improved.
- Excellent communication between LAPD/DOT/LAFD.
- Proximity of so many different agencies allows for efficiency in coordinating response.
- Strong teamwork made up for individual lack of familiarity.
- Experienced RACR personnel assisted with the success of Law Branch.
- Very engaged CLA representative.
- Increased BOC integration.
- Increase in awareness of DAFN issues, positions, and responsibilities.
- Communication with Mass Care DOC was strong.
- Communication with LAAS DOC was strong.
- LAWA DOC staff was very well prepared.
- Effective communications support between PIO DOC and Operations DOC.
- Strong team dynamic across groups.
- Flexibility demonstrated in response to changing needs.
- BOC partnerships with VOADs and the private sector.
- Recs and Parks had great communication with GSD.

Process (69%)

- Successful problem-solving and policy-level decisions made across the board. (3%)
- Increased knowledge of ICS. (3%)
- Learned the importance of prioritizing needs. (2%)
- Strong command presence demonstrated by EOC Director. (2%)
- Processing of injects in a timely manner. (2%)
- Resource request and tracking systems greatly improved. (2%)
- Vetting of information. (2%)
- Effective area coordination and management response.
- Smooth check-in.
- Great test of the City's resources; incident showed where challenges would occur.

- Efficient cost accounting.
- Strong staff delegation of work.
- Knowledge of Nixle System.
- Successful management of a major incident JIC.
- Successful rumor control.
- Management of EOC objectives.

WebEOC (16%)

- Much more intuitive than previous years. (3%)
- Support from EMD was welcome for WebEOC.
- Allowed for easy follow-ups.
- Very helpful tool to track DOC and resource requests.
- Liaison representatives that did not have DOCs open continued to use WebEOC to simulate communications.

Resources (9%)

- Seating chart was very useful. (3%)
- Map of local declaration early in operational period. (2%)
- Staff coordination made possible by availability of personnel contact information.
- Dry erase boards provided a great resource for Situational Awareness.
- Vests made identification of team members much easier.
- Successful radio communication.

Facility (4%)

- Camera feeds were very helpful.

AREAS FOR IMPROVEMENT

Section-Specific Coordination (41%)

- Not enough input from Public Health. (5%)
- Need for LADOT Mutual Aid agreement. (3%)
- LAFD DOC integration needs improvement.
- Liaison section would benefit from the addition of a Deputy Liaison Officer.
- There is not enough staff in the Planning section to handle the critical planning tasks.
- Mass Care would benefit from the addition of a Deputy Section Coordinator.
- LAUSD communication needs improvement.
- Everbridge notifications were not received (LAWA).
- Public Health seemed out of line with the reality of the situation.
- Recs and Parks DOC lacked SOP knowledge.
- PIO had difficulty coordinating with outside agency PIOs in the absence of OA JIC.
- Information sharing between Area Commands and LAFD DOC was lacking.
- The BOC would benefit from an additional BOC Controller for comprehensive tracking purposes.

- LAUSD needs to investigate the status of MOU/MOAs already in place.
- Agency reps felt very disconnected.
- DWP felt they could prepare better.
 - Pre-populate a list of facility addresses and phone numbers in the event access to DWP intranet is unavailable.
 - Pre-load key documents, plans, phone-lists, etc. on to thumb drives.
- The Donation & Resource Coordination process is a two-person job.

Information Sharing and Flow (33%)

- Better configuration of WebEOC for BOC use.
- Communication at all levels can be improved.

- Distilling and vetting information proved difficult.
- Visible lack of information sharing within sections.
- Need more staff for information management and capturing of data.
- Consider creating a chart/graph to show how information flows in the EOC.

Resource Request Coordination and Process (24%)

- Delay on return of rejected requests made correction of forms difficult.
- No confirmation of DSW request being received and/or fulfilled.

- Many requests went unfulfilled.
- Locating resources was challenging.
- Follow-up was slow or lacked closure. (4%)
- Logistics failed to provide resource request updates. (3%)
- Lack of ability to coordinate and document need-assessment with donation specifications.
- Unclear where to get information regarding DSW activation.

Understanding of Roles (21%)

- General lack of understanding of role/responsibilities limited player coordination. (4%)
- Many were unaware of their roles/responsibilities because they were first-time players. (2%)
- Law Branch was inundated with requests not related to their positions.
- Need to determine which requests are handled by the Logistics Section and which are handled by other sections.

Streamline Paperwork Process (8%)

- The overall process needs to be more organized. (4%)
- Change “New Item” on ICS-214 form to “New Op Period” for more clarity. (3%)
- Overwhelming bottleneck regarding resource requests.

Situational Awareness (7%)

- Lack of real-time updates displayed in EOC.

- BOC members severely lacked Situational Awareness.
- Management lacked situational awareness due to lack of Planning Section updates.

Other (5%)

- City employees need to be assured that they will receive prophylactic medications. (2%)
- Personnel list should include “other languages spoken.”
- Every City department should participate in these exercises.
- Alternate EOC members were not well-prepared/experienced.

APPLICABLE PLANS/POLICIES/PROCEDURES, EQUIPMENT, ORGANIZATION/STRUCTURE, AND/OR TRAINING THAT SHOULD BE REVISED, DEVELOPED, OR ACQUIRED TO IMPROVE EMERGENCY MANAGEMENT IN THE CITY.

Equipment and Facility (40%)

- Difficulty using/understanding Google Drive. (4%)
- Poor internet connection. (3%)
- Insufficient bandwidth available for large groups. (3%)
- Printing was difficult. (3%)
- Technical malfunctions need quick alternative solutions.
- Video conferencing systems did not function well.
- Some phones did not work.
- BOC needs a high-speed scanner and copier.
- BOC requests two additional wall-mounted LCD screens.
- Forms being displayed on large monitors need to be large enough for all to read.
- More communication equipment needed.

- In previous years the main screen projected major incidents.

WebEOC (35%)

- BOC members need individual and wider WebEOC access. (4%)
- More IT staff needed. (4%)
- WebEOC training should be made mandatory. (4%)
- Lack of training in WebEOC led to poor communication and hindered EOC process. (2%)
- Email/messaging is too cumbersome.
- Unable to easily forward resource requests.
- Message notification system is inefficient.
- Not flexible enough for situation reporting.
- Need more training.
- Applying communications protocols within WebEOC was confusing.

Process (32%)

- Chain of command was unclear. (4%)
- PIO messages were delayed. (3%)
- Difficult to process injects in a timely manner.
- Lack of familiarity regarding report processing.
- Difficult to track completed tasks.
- DPH protocols were unclear.

Need More Exercise and Training (20%)

- More training will lead to higher levels of role proficiency. (7%)
- LADOT needs wider EOC and DOC training.
- Training requested for EOC procurement policies.
- Future trainings should include information on the capabilities of the BOC.

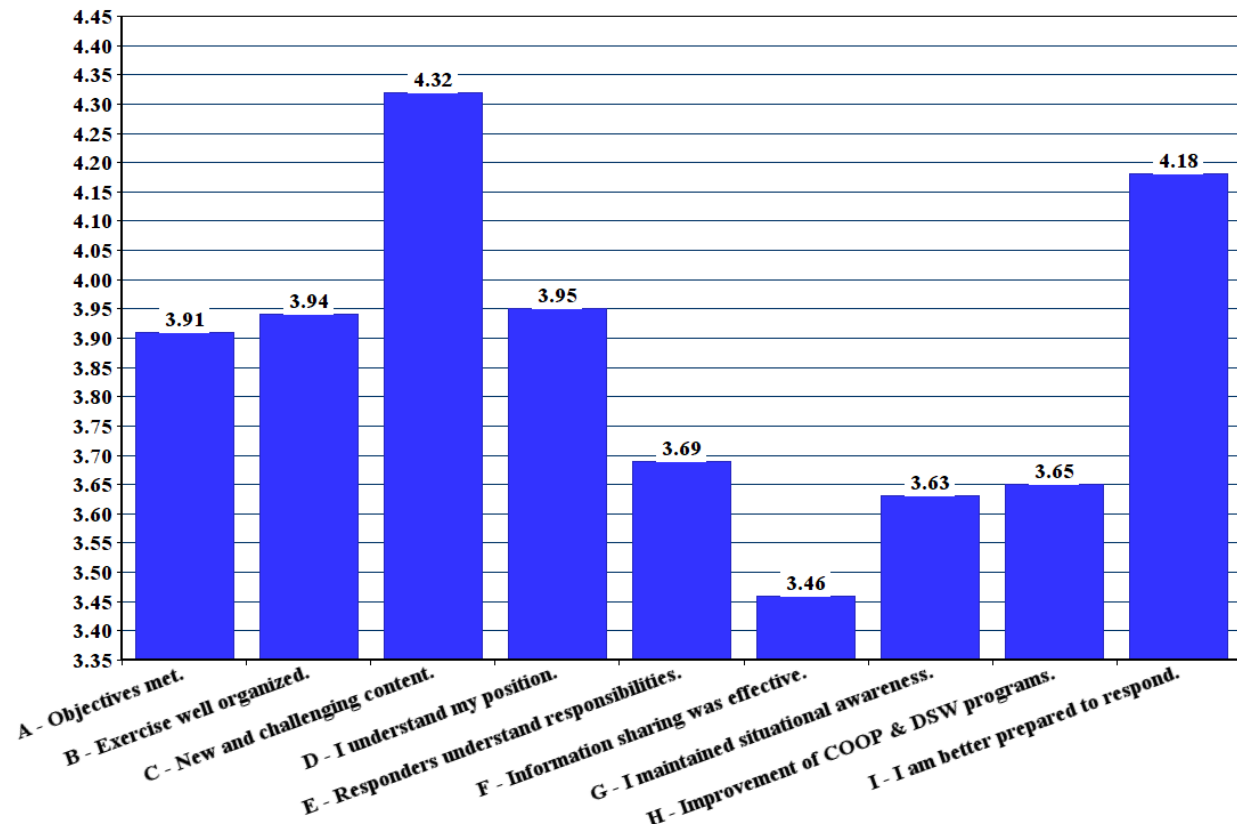
Mapping (3%)

- GIS maps were not universally available. (2%)
- Printing maps slows down the EOC process.

EXERCISE ASSESSMENT

Survey Data	Strongly Disagree		3	Strongly Agree		Total Respondents*	Average Rating
	1	2		4	5		
A. The exercise objectives associated with my position, Section, or location were achieved.	2	6	14	47	24	92	3.91
B. The exercise was well structured and organized.	2	6	12	49	24	91	3.94
C. The public health scenario presented a new and challenging content for the exercise.	1	0	14	33	47	95	4.32
D. I understood how to perform the functions and tasks associated with my position and section.	1	6	17	41	27	92	3.95
E. EOC/DOC responders, including me, understood each other's responsibilities and worked collectively to achieve EOC/DOC objectives.	6	6	20	35	22	89	3.69
F. Information sharing within and among the EOC, DOCs, and with other emergency partners was effective.	6	13	27	26	21	93	3.46
G. I maintained Situational Awareness throughout the exercise because procedures were clearly communicated and followed.	4	7	31	27	23	92	3.63
H. My department/organization needs to improve its Continuity of Operations (COOP) and Disaster Service Worker (DSW) protocols to better weather a similar incident.	2	7	31	35	18	93	3.65
I. As a result of this exercise, I have a better understanding of how to respond in accordance with LA City procedures in an emergency.	2	1	8	49	33	93	4.18

2015 LA Functional Exercise Assessment Factors



EXERCISE CONDUCT FEEDBACK

Strengths:

- Great, well-developed exercise.
- Injects felt realistic.
- Very believable Level 3 incident.
- Very realistic experience.
- This exercise presented unique challenges.
- Participants were much better about interacting with each other.

Areas for Improvement:

- High amount of duplicate work/communications.
- Spreading the exercise over two days (a full operational period) would be beneficial.
- Dispensing of injects needs improvement.
- Controllers seemed unclear on how to respond to injects.
- EOC infrastructure needs improvement (phones, computers, printers, etc.).
- The importance of updating logs needs to be addressed.
- Software interface needs to be more functionally based.
- Wireless connectivity needs improvement.

- Weather conditions should be mentioned at some point during the exercise.
- This should have been a police-led exercise.
- No “all-clear” message was issued for City employees.
- The most significant challenge is always the flow of information.
- Establish MOUs with clear deliverables.
- The amount of information that needed analysis quickly became overwhelming.

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: July 12, 2016

To: Charlie Beck, Chair
Emergency Operations Board

Emergency Operations Board Members

From: Anna Burton, Executive Assistant
Emergency Operations Board

A handwritten signature in black ink, appearing to read "Anna Burton", written over the printed name in the "From:" field.

Subject: **2016 LOS ANGELES MARATHON EMERGENCY OPERATIONS
CENTER ACTIVATION AFTER ACTION REPORT/CORRECTIVE
ACTION PLAN**

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee (EMC), approve the attached 2016 Los Angeles Marathon Emergency Operations Center (EOC) Activation After Action Report/Corrective Action Plan (AAR/CAP) and forward to the Mayor for transmittal to the City Council.

Summary

The EOC was activated to provide effective citywide coordination of information and to support the Unified Command Post and Multi-Agency Coordination Center for the Sunday, February 14, 2016, Los Angeles Marathon. This annual event brings thousands of athletes and spectators from all over the world.

EMD consulted with the Los Angeles Police Department, the Los Angeles Fire Department and the Office of the Mayor prior to the LA Marathon and determined that at a minimum, this event would warrant an EOC Level I activation. The EOC was activated to provide support to field response agencies and to ensure effective Citywide coordination and response in the event of significant race related incidents or other unrelated activities occurring in the City during the hours of the LA Marathon.

The attached AAR/CAP provides a summary of the activation, identifies involved departments and agencies, and details the recommendations for future activations of the EOC. This report was approved by the EMC at its May 4, 2016, meeting. With approval by the EOB, EMD will forward to the Mayor for approval and transmittal to the City Council.

EMD will track areas recommended for improvement and, as appropriate, report back through the Emergency Operations Organization.

Attachment

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: April 19, 2016

To: Anna Burton, Chair
Emergency Management Committee
Emergency Management Committee Members

From: Carol Parks, Special Projects Division Chief
Emergency Management Department

Subject: **2016 LOS ANGELES MARATHON EMERGENCY OPERATIONS
CENTER ACTIVATION AFTER ACTION REPORT/CORRECTIVE
ACTION PLAN**

Recommendation

That the Emergency Management Committee (EMC) approve the attached LA Marathon Emergency Operations Center (EOC) Activation After Action Report/Corrective Action Plan (AAR/CAP) and forward to the Emergency Operations Board (EOB) for approval.

Summary

The EOC was activated to provide effective citywide coordination of information and to support the Unified Command Post and Multi-Agency Coordination Center for the Sunday, February 14, 2016, Los Angeles Marathon. This annual event brings thousands of athletes and spectators from all over the world.

EMD consulted with the Los Angeles Police Department, the Los Angeles Fire Department and the Office of the Mayor prior to the LA Marathon and determined that at a minimum, this event would warrant an EOC Level I activation. The EOC was activated to provide support to field response agencies and to ensure effective Citywide coordination and response in the event of significant race related incidents or other unrelated activities occurring in the City during the hours of the LA Marathon.

The attached AAR/CAP provides a summary of the activation, identifies involved departments and agencies, and details the recommendations for future activations of the EOC.

Attachment

- DRAFT -



**After Action Report/Corrective Action Plan
2016 LOS ANGELES MARATHON
EOC Activation**

February 14, 2016



TABLE OF CONTENTS

I.	Executive Summary	2
A.	Statement of Purpose.....	2
B.	Event Name	2
C.	Event Date	2
D.	Event Location	2
E.	EOC Activation Duration	2
F.	EOC Activation Lead Agency	2
G.	EOC Activation Level	2
H.	EOC Activation Participating Agency	3
I.	EOC Activation Chronology.....	3
II.	Synopsis.....	4
A.	Major Developments	4
B.	Core Capabilities	5
C.	EOC Objectives.....	5
III.	Findings	6
A.	Practices to Sustain.....	6
B.	Area Requiring Improvement	7
IV.	Conclusion	7
V.	Improvement Plan Matrix.....	7

I. Executive Summary

A. Statement of Purpose

The Emergency Management Department (EMD) is responsible for preparing a formal After Action Report/Corrective Action Plan (AAR/CAP) following all activations of the City's Emergency Operations Center (EOC). AAR/CAPs are intended to assist the City of Los Angeles analyze its EOC activation, staffing and management processes in order to document the following:

- Procedures and protocols to sustain and build upon,
- EOC operational elements and processes to improve, and
- Improvement plan with recommended corrective actions, responsibilities and timelines.

The AAR/CAP should be viewed as suggestions for improving the effectiveness of future EOC activations. Recommended corrective actions identify steps to be taken and assign specific City agencies with responsibility for their coordination and implementation. Timetables are also established for implementation against the benefits in determining resource allocation. In some cases, agencies may determine the benefits of implementation are insufficient to outweigh the costs. In other cases, agencies may identify alternative solutions that are more effective. Each agency should review the recommendations and determine the most appropriate action and time needed for implementation.

B. Event Name

2016 LA Marathon

C. Event Date

Sunday, February 14, 2016

D. Event Location

Citywide

E. EOC Activation Duration

0500 – 1445 hours

F. EOC Activation Lead Agency

EMD

G. EOC Activation Level

Level I (EMD Lead)

H. EOC Activation Participating Agency

EMD

I. EOC Activation Chronology

The EOC was activated to ensure information sharing was maintained between the EOC and the Unified Command Post, Multi-Agency Coordination Center (MACC), and any activated Department Operations Centers (DOCs); to provide support to the UCP in the event emergency services were needed and to gather information and intelligence from appropriate resources. Based on discussions with the Los Angeles Police Department (LAPD), the Los Angeles Fire Department (LAFD) and the Office of the Mayor prior to the LA Marathon; there was an EOC Level I (EMD Lead) activation to support field response agencies and the Unified Command Posts (UCPs). The following factors weighed into this decision:

- To ensure the safe movement of event attendees.
- Provide crowd management, and if necessary, crowd control measures.
- Deploy law enforcement resources to deter criminal activity.
- Provide Basic and Advance Life Support treatment and transportation.

The activation of the EOC occurred at 0500 hours on February 14, 2016. The EOC was activated at Level 1. The EOC was deactivated for this event at 1445 hours on February 14, 2016. Staffing for this activation included the EMD Duty Officer and Duty Team. Other City response and support agencies performed field response, MACC and UCP duties.

EMD's Duty Team staffed the following EOC positions:

- EOC Director
- Planning and Intelligence Section Coordinator
- Public Information Officer

The Planning and Intelligence Section used an Event Action Plan that was developed by the Unified Command staff. The Unified Command staff consisted of LAFD, LAPD and DOT. EMD staff attended all planning meetings for this event.

Initial Briefing and Coordination Meetings

The Planning and Intelligence Section Coordinator briefed the EOC responders on the advance EOC Coordination Plan and the anticipated schedule of events. EMD also staffed the Liaison Officer position at the UCP located in the LAFD Metro Fire Communications Center (500 E. Temple Street). This Liaison Officer provided the EOC with regular status briefings based on information received at the UCP and MACC briefings and planning meetings.

Planning Meetings

The Planning and Intelligence Section Coordinator provided an updated situation report and implemented the pre-established, advanced event EOC management and coordination objectives that were approved by the EOC Director (See Section C – Objectives on page 5).

Coordination Meetings

The Planning and Intelligence Section Coordinator provided an updated situation report and confirmed status of the established objectives. The EOC coordinated with the LAFD DOC to monitor life safety issues. The EMD Liaison Officer position in the UCP also provided the EOC with regular situation status updates on the event.

Final Coordination and EOC Demobilization Meeting

The Planning and Intelligence Section Coordinator provided a final update on event status. No specific requests were directed to the EOC by the UCP.

No significant incidents or unusual occurrences were reported. Final EOC 909 report was approved and released on February 14th at 1430 with demobilization of the EOC at 1445 hours.

II. Synopsis

The EOC was activated on Sunday, February 14, 2016, at 0500 hours, and was de-activated at 1445 hours, to provide support to the UCP and the MACC located at the City of Los Angeles EOC (500 E. Temple Street). The decision to activate the EOC was made by EMD and supported by LAPD, LAFD and the Office of the Mayor.

This Level I activation was staffed by EMD personnel. Level I activation level requires (at minimum) staffing of the EOC Director, Planning and Intelligence Section Coordinator, Situations Status Unit Leader, Documentation Unit Leader, and Public Information Officer positions. EMD personnel maintained regular communications with LAPD's DOC, the MACC and the UCP. EMD assigned a Liaison Officer to work at the UCP. These representatives attended all UCP briefings and provided the EOC with regular situation status reports which were utilized to prepare EOC situation updates for City-wide use.

The EOC monitored the activities of the runners and spectators associated with LA Marathon. This monitoring included mitigating traffic, providing basic and/or advanced life support treatment and transportation. The EOC was not tasked to provide any significant resources or services. All logistical needs were met through the UCP.

A. Major Developments

The EOC Director and Planning and Intelligence Section Coordinator provided overall leadership of the EOC organization and the process of management by objectives. EMD developed advanced EOC coordination objectives as described in Section C below. These objectives were consistent with and supported field level advanced event plan objectives

developed by the Unified Command. The EMD Public Information Officer coordinated the EOC's emergency public information process with the UCP.

The Planning & Intelligence Section collected analyzed and disseminated information from field, DOC, EOC and media and social media sources. The Section maintained situational awareness, coordinating the assembling of section situation reports, setting meeting agendas and facilitating all meetings conducted in the EOC Management Room.

Planning and Intelligence focused specifically on the safety of the LA Marathon runners/spectators, the City's traffic situation and monitoring the overall City footprint for any threats, disruptions, or impacts to City services. This monitoring included using social media outlets and other information related to the event.

EOC deactivation occurred and the EOC transitioned its operations to the EMD Duty Officer.

B. Core Capabilities

This event provided an opportunity to assess the following EOC core capabilities:

- Intelligence and Information Gathering and Sharing
- Recognition of Indicators and Warnings
- EOC Management and Coordination Planning Processes including development of advanced event EOC coordination objectives
- Staffing a Liaison Officer position at the UCP

C. EOC Objectives

The EOC developed the following advanced event plan objectives based on the Unified Command's Advanced Event Plan.

Management Objectives

- Ensure information sharing is established and maintained between the EOC, any activated DOCs and the Los Angeles County EOC.
- Provide support to the UCP in the event citywide emergency services are required.
- Gather information and intelligence from appropriate resources.
- Monitor the event and be ready to advise City leadership if the EOC activation level needs to be increased.

Coordination Objectives

- Maintain situational awareness regarding the LA Marathon and any impacts to the City.
- Monitor media reports and coordinate public information related to the LA Marathon.
- Facilitate policy direction as needed.
- Coordinate/share information with the UCP and MACC; activate DOCs and other applicable jurisdiction EOCs.
- Provide resource support to the UCP, if requested.
- Keep City executives and elected officials informed of any significant event related incidents.

III. Findings

A. Practices to Sustain

The following EOC practices were reported as effective by responders and are recommended to be sustained:

1. Level I EOC Activation Policies and Procedures

EMD has developed a set of policies and procedures for EOC Level I activations. During Level I activations, the EOC is staffed by an EMD Duty Officer and Duty Team members. A system of primary and back-up Duty Officers and Duty Teams ensures sufficient depth of coverage for key positions such as EOC Director, Planning and Intelligence Section Coordinator and Situation Status Unit Leader as well as support positions such as Documentation Unit Leader, Management Staff Support and Public Information Officer. Typical Level I staffing requires that these six (6) positions are filled.

This model relies on liaison with representatives from other operating departments and effective communication with activated DOCs for situational awareness and resource coordination. Should the event or incident escalate, the activation level can be increased to II or III which requires staffing of various positions by other departments. Most of the recent EOC activations have been at Level I using this model which has proven to be efficient and cost effective. It is recommended that these policies and procedures be sustained.

2. Advanced Event EOC Coordination Planning Process

EMD plays an active role in advanced event planning with LAPD, LAFD, LADOT and other field response agencies. An EMD planning liaison is assigned to work with advanced event planning teams to ensure that inter-agency coordination issues are managed proactively from a Citywide perspective. Their role includes recommending appropriate EOC activation levels, assignment of an EMD Liaison Officer to UCPs or Incident Command Posts, and development of an advanced event EOC Coordination Plan that is based on objectives of the field level Advanced Event Plan.

3. EMD Staffing of UCP Liaison Officer Position

EMD has a standing practice of staffing the UCP Liaison Officer position for major planned events. This position ensures effective interagency coordination and cooperation, especially between the established Unified Command agencies and City support agencies such as the Department of General Services, the Department of Transportation, etc. This practice is especially valuable for Level I EOC activations where the Liaison Officer also provides the EOC with regular informational briefings to ensure good situational awareness and a “common operating picture” with the Unified Command staff.

B. Area Requiring Improvement

The following area was reported as requiring improvement.

Further Development of the EOC 909 Situation Report Process

A key component of the established, successful Level I EOC Activation Process and Procedures has been the enhancements to the MCR Management Room and use of the EOC 909 form for standardized Situation Status Reporting. The Management Room is currently equipped with a manual that can assist EMD staff during the EOC activation. While this process has become standard for Level I events, it is recommended that the EMD EOC Task Force continue to refine and further develop this process for information gathering and reporting and refining the recipient list to ensure all appropriate department representatives are informed and updated.

The EOC 909 was provided electronically to key City agencies and decision makers. EMD should evaluate expanding the scope of distribution and areas for overall improvement.

IV. Conclusion

EMD continues to improve on the staff efficient and cost effective set of processes and procedures for Level I activations of the City's EOC. The improvement over past practices will proceed with Level I staffing of EOC activations with trained emergency managers from EMD. These staff provide core EOC position capabilities and maintain situational awareness and coordinate available resources by communicating with personnel from other response and support agencies at the DOC and UCP/ICP level.

EMD staffs the physical EOC; other departments are brought to bear in a "virtual" EOC environment through effective communication and use of technology. Physical staffing of EOC positions by these agencies is generally required for Level II and III activations only.

V. LA Marathon EOC Activation Corrective Action Plan (Improvement Plan Matrix)

The following matrix identifies specific recommended corrective action.

Required Improvement	Corrective Action	Lead Agency	Timeframe	Resources Required
Continue enhancement of the EOC 909 Situation Reporting Process	Continue to refine and further develop this process to ensure effective information flow, management and distribution.	EMD	On-going	EMD staff resources, EOC Task Force, and public safety department representatives, as needed

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: July 12, 2016

To: Charlie Beck, Chair
Emergency Operations Board

Emergency Operations Board Members

From: Anna Burton, Executive Assistant
Emergency Operations Board

A handwritten signature in cursive script, appearing to read "Anna Burton", written over the printed name in the "From:" field.

Subject: **CITY OF LOS ANGELES 2016 CYBER SECURITY TABLE TOP EXERCISE AFTER ACTION REPORT/IMPROVEMENT PLAN**

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee (EMC), approve the attached City of Los Angeles 2016 Cyber Security Table Top Exercise (TTX) After Action Report/Improvement Plan (AAR/IP) and forward to the Mayor for transmittal to the City Council.

Summary

On February 23, 2016, the City of Los Angeles conducted its second Cyber Security TTX. This was a two part event consisting of a discussion-based tabletop exercise followed by presentations by, and question and answer period with, cyber security policy and technical thought-leaders. The tabletop exercise portion was intended to test the City of Los Angeles' current planning and response capabilities related to a cyber-terrorism attack on city technology.

The attached report provides a summary of the exercise, identifies involved departments and agencies, and details the recommendations for improving the City's capabilities to mitigate, prepare for, respond to and recover from cyber security threats or attacks. This includes how the consequences of such events will be managed by the City's Emergency Operations Center (EOC) in concert with the new Information Security Operations Center (ISOC) and the existing Cyber Intrusion Command Center (CICC) group.

The attached AAR/IP provides a summary of the activation, identifies involved departments and agencies, and details the recommendations for future activations of the EOC. This report was approved by the EMC at its June 1, 2016, meeting. With approval by the EOB, EMD will forward to the Mayor for approval and transmittal to the City Council.

EMD will track areas recommended for improvement and, as appropriate, report back through the Emergency Operations Organization.

Attachment

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: May 25, 2016

To: Anna Burton, Emergency Management Committee Chair
Emergency Management Committee Members

From: Rob Freeman, Operations Division Chief
Emergency Management Department

Subject: **CITY OF LOS ANGELES 2016 CYBER SECURITY TABLE TOP EXERCISE
AFTER ACTION REPORT/IMPROVEMENT PLAN**

Recommendation

That the Emergency Management Committee (EMC) approve the attached City of Los Angeles 2016 Cyber Security Table Top Exercise (TTX) After Action Report/Improvement Plan (AAR/IP) and forward it to the Emergency Operations Board (EOB) for approval.

Summary

On February 23, 2016, the City of Los Angeles conducted its second Cyber Security TTX. This was a two part event consisting of a discussion-based tabletop exercise followed by presentations by, and question and answer period with, cyber security policy and technical thought-leaders. The tabletop exercise portion was intended to test the City of Los Angeles' current planning and response capabilities related to a cyber-terrorism attack on city technology.

The attached report provides a summary of the exercise, identifies involved departments and agencies, and details the recommendations for improving the City's capabilities to mitigate, prepare for, respond to and recover from cyber security threats or attacks. This includes how the consequences of such events will be managed by the City's Emergency Operations Center (EOC) in concert with the new Information Security Operations Center (ISOC) and the existing Cyber Intrusion Command Center (CICC) group. EMD will track areas recommended for improvement and, as appropriate, report back through the Emergency Management Committee and Emergency Operations Board.

Attachment – City of Los Angeles 2016 Cyber Security Table Top Exercise After Action Report/Improvement Plan

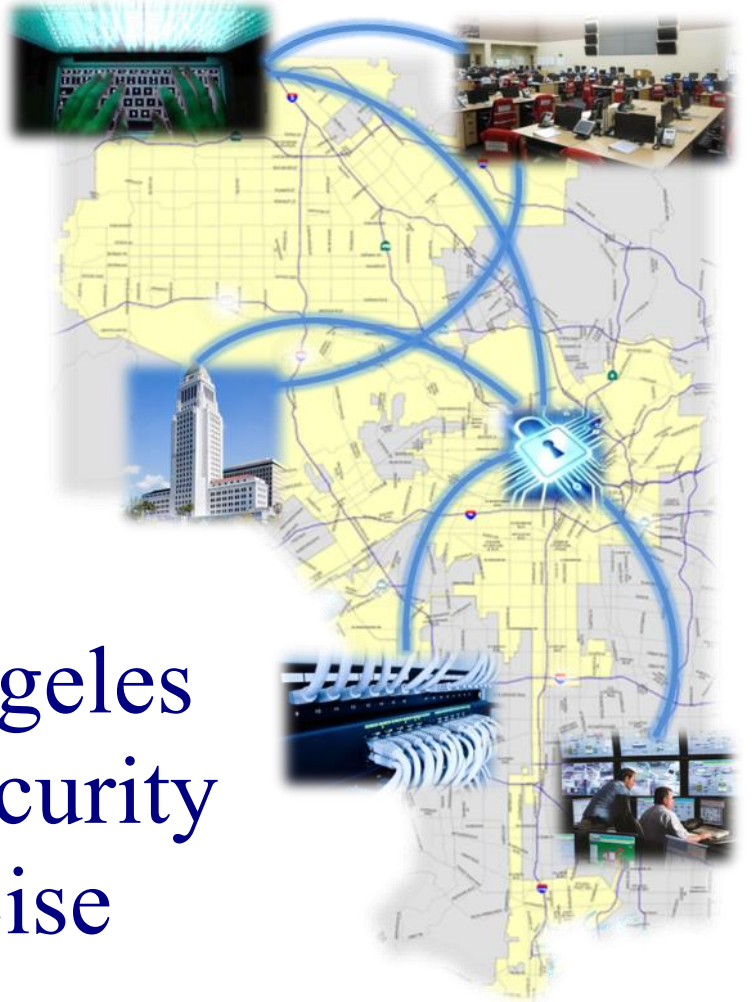


City of Los Angeles 2016 Cyber Security Tabletop Exercise

February 23, 2016

After-Action Report/Improvement Plan

Publication Date: April 25, 2016



This page is intentionally blank.

EXERCISE OVERVIEW

Exercise Name	City of Los Angeles 2016 Cyber Security Tabletop Exercise
Exercise Dates/ Times	Tuesday, February 23, 2016 Start of Exercise (StartEx): 8:00 a.m. End of Exercise (EndEx): 12:00 p.m. Expert Presentations and Panel Discussion: 12:30 p.m. - 3:00 p.m.
Sponsor	City of Los Angeles Emergency Management Department (EMD)
Scope	<p>This was a two part event consisting of a discussion-based tabletop exercise followed by presentations by, and question and answer period with, cyber security policy and technical thought-leaders.</p> <p>The tabletop exercise portion was intended to test the City of Los Angeles' current planning and response capabilities related to a cyber-terrorism attack on city technology. Specifically, the exercise included two groups: 1) the City's cyber security technical teams, including its Cyber Intrusion Command Center (CICC) Working Group, Cyber Incident Response Team (CIRT) members, and Tier 1 Department Cyber Incident Response Team members, all operating under the protocols of the City's 2016 <i>Cyber Incident Response Policy</i>; and 2) the City's Emergency Operations Center (EOC) policy leadership and EOC planners. The technical group also consisted of individuals that staff the City's Integrated Security Operations Center (ISOC), representatives from the Los Angeles Police Department (LAPD), and supporting law enforcement and investigative agencies such as the U.S. Secret Service (USSS) and the Federal Bureau of Investigation (FBI). In response to the scenario, the technical group talked through the implementation of the City's <i>Cyber Incident Response Policy</i>. At each step of the process, the City EOC group was engaged to discuss the communication and coordination required between the two groups to address the consequences of the cyber-attack on City operations and the community. In particular, the EOC group continued to develop its consequence-management framework addressing the unique coordination and response measures required by a cyber-terrorism incident.</p> <p>The second portion of the event included technical and policy experts from the U.S. Department of Homeland Security's (DHS') Joint Cyber Programs, National Cybersecurity and Communications Integration Center (NCCIC), and the former Chief Information Security Officer (CISO) for the City of Seattle; all of whom spoke to national and local cyber policies, programs, trends, and best practices, the current threat environment, and technical details from recent real-world cyber-attack responses (e.g., U.S. Office of Personnel Management). Formal presentations were followed by a question</p>

	and answer panel discussion open to all participants. A summary of those presentations and discussions is included in Appendix D.
<p>Mission Area</p>	Prevention and Response
<p>Core Capabilities</p>	<ul style="list-style-type: none"> • Cyber Security • Intelligence and Information Sharing • Interdiction and Disruption • Operational Coordination • Planning
<p>Objectives</p>	<ul style="list-style-type: none"> • Evaluate the roles and responsibilities of, and coordination between, the City of Los Angeles’ EOC and the CICC/ISOC during a cyber-incident. • Develop a shared understanding between the City EOC and CICC/ISOC of cyber-incidents (e.g., status, severity), their impacts on City operations and the community, and the expectations of the EOC and CICC/ISOC on each other during prevention and response efforts. • Talk through and continue to explore what, if any, additional modifications are required to the City’s <i>Cyber Incident Response Policy</i>. Discussion will be used to determine the Policy’s effectiveness to coordinate the City’s cyber incident response by assessing the level of awareness of cyber-security roles across City departments, information sharing and coordination requirements, and the City’s cyber command, control, and resource coordination capabilities. • Discuss the capabilities of the City to detect malicious activity, conduct countermeasures, accomplish mitigations, and perform operations in response to a cyber-attack according to the <i>Cyber Incident Response Policy</i> and department-specific protocols. • Continue to explore what, if any, hazard-specific modifications are required to supplement the City’s <i>EOC Policy and Procedures Manual</i> to effectively address the unique consequence-management efforts resulting from a cyber-attack (e.g., EOC objectives, role, staffing, organization, information management, resource management, City policies).
<p>Threat or Hazard</p>	Cyber-Terrorism Attack
<p>Scenarios</p>	<p>Module 1 (Tuesday, February 23, 2016): Over the past week, the City of St. Louis, Missouri has been plagued by random, widespread, and repetitive power outages widely covered by the media. While the media has been linking the outages to aging infrastructure at Ameren Missouri (the power company servicing the greater St. Louis area), a number of sources have confirmed the problems being experienced by Ameren are the result of a serious cyber-attack that Ameren is still working to neutralize. This information was shared with Los Angeles’ CICC by way of the FBI’s Cyberwatch Program and the National Cybersecurity and Communications Integration Center (NCCIC). The Department of Water and Power (DWP)</p>

Scenarios
(Cont.)

received similar information from the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC).

Those sources confirm Ameren experienced a highly destructive malware used to gain a foothold into multiple company systems, which allowed hackers to then trip circuit breakers to randomly shut down power throughout the region. At various points during the last week, nearly 100,000 customers (60% of the total customers in the City of St. Louis) were affected by power outages ranging from hours to multiple days, including repetitive power outages once the company had initially restored power. The hackers have continued to delay restoration efforts by deleting critical files to deny the use of SCADA systems and waging denial-of-service attacks on the company's telephone, dispatch, and customer outage reporting systems. The cyber-attack appears to be similar to the recent attack on the Ukrainian power system and authorities believe the St. Louis incident and a recent attack on Israel's Electricity Authority may be more than a coincidence. Authorities and regulators are warning infrastructure owners/operators – not just power companies – to evaluate their cyber vulnerabilities and employ all available protective measures.

In Los Angeles, the ISOC has been operating as usual; gathering information on cyber incidents from all City departments and agencies and providing support as necessary. While no particularly abnormal incident reports have been received and no major systems have recently been threatened, the “My LA 311” website has been brought down multiple times in the past month following El Niño storms. The Information Technology Agency (ITA) was able to determine some of the outages were the result of genuine increases in the demand to log service requests after storms and others were well-timed denial of service attacks from an unknown origin. In either case, the prolonged 3-1-1 outages have gained the attention of multiple City Council members as resident and commercial complaints about not being able to file service requests have significantly increased.

In addition, the Port of Los Angeles (POLA), Fire and Police Pensions, and the Bureau of Sanitation (BOS) have reported to the ISOC 40% - 50% increases in the number of cases of unauthorized access, attempted access (e.g., scans, probes), and improper usage over the last three weeks. To date, there have been no known consequences as a result of those incidents.

Module 2 (Thursday, May 12, 2016): With El Niño over, Los Angeles is in the midst of an early summer heat wave with temperatures in triple digits. As is common during these types of heat conditions, power has been in high demand. Three days ago, an unknown cyber-related problem stopped all power generating operations at the Valley Generating Station. Two days later, a similar cyber-related issue stopped generation at the Harbor Generating Station, presenting the City with a serious energy shortfall leading to unplanned blackouts and requiring the use of rolling blackouts to

**Scenarios
(Cont.)**

balance the load. The DWP has been unable to restore power to more than 150,000 customers in the City following both unplanned and rolling blackouts. Power has been out for three days with no anticipated restoration in much of the San Fernando Valley west of the I-405 Freeway, the central portion of the City from 7th Street in Downtown south to Slauson Ave., and the northern part of the Port and most of the Wilmington neighborhood. Unpredictable blackouts are continuing in the City and DWP has acknowledged that it's unsure if its industrial control systems have been compromised.

Due to the extended power outage in parts of the City, the following consequences have been realized:

- Cellular phone towers have begun to lose power as their back-up fuel supplies are consumed.
- The service and timing of Metro trains has been compromised because of their dependence on cellular towers.
- Traffic congestion is extreme as a result of inoperable signals and traffic systems.
- Pumping stations for water and fuel are going off line leaving parts of the city without water in addition to electricity.
- Businesses, schools, and universities in areas without power have been unable to open.
- Critical facilities such as hospitals, police and fire stations, utilities, and the Port are struggling to maintain minimum operations.
- Looting has been reported in neighborhoods that have been without power for 24+ hours.

While the energy related issues have been occurring, the ITA has detected malicious code of an unknown source and nature that is attacking the City's network backbone. Those departments dependent upon on the ITA's network for internet, telecommunications (e.g., Voice-Over-Internet-Protocol [VOIP]), or radio are experiencing complete or sporadic service outages and/or diminished quality and slow speeds resulting in debilitating impacts on the operations of many City departments.

**Participating
Organizations**

The cyber security technical group consisted of the members of the City's CICC Working Group, ISOC staff, and select Department Cyber Incident Response Team members from Tier 1 Departments. There were twenty-four (24) players and two (2) evaluators in this group.

The City EOC group consisted of a select group of emergency management, technology, and public safety leadership and planners responsible for establishing and approving City EOC policy and procedures. There were twenty-three (23) players and two (2) evaluators in this group.

The full list of participants is included in Appendix B.

Exercise Agenda

Time	Activity
07:30	Registration
08:00	Welcome, Introductions, Purpose and Scenario Overview
08:20	Module 1: Scenario 1 and Plenary Discussion
09:45	Break
10:00	Module 2: Scenario 2 and Plenary Discussion
11:40	End of Exercise and Hot Wash
12:00	Working Lunch (Provided)
12:30 - 15:00	Cyber Security Expert Presentations along with a Question and Answer Panel Discussion

Points of Contact	<p>City of Los Angeles:</p> <p>Michelle Riebeling Emergency Management Coordinator I/Planning Officer Emergency Management Department City of Los Angeles 500 E. Temple Street Los Angeles, CA 90012 (213) 484-4816 Office Michelle.Riebeling@LACity.org</p> <p>Contractor Support:</p> <p>Nick Lowe, CEM, CBCP, MEP Partner/Chief Operating Officer Critical Preparedness and Response Solutions (CPARS Consulting, LLC) 9552 Via Venezia Burbank, CA 91504 (626) 320-0218 Office NLowe@CPARSconsulting.com</p>
--------------------------	--

This page is intentionally blank.

ANALYSIS OF OBJECTIVES AND CORE CAPABILITIES

Aligning objectives and core capabilities for evaluation purposes transcends individual exercises to support ongoing and consistent preparedness reporting and trend analysis. The table below includes the exercise objectives, aligned core capabilities, and a summary performance rating for each objective as determined by the evaluation team. The following sections then provide an overview of performance to justify the summary rating, highlighting key discussion elements and areas for improvement.

Summary of Objective and Core Capability Performance

Objective	Core Capability	Summary Rating			
		P	S	M	U
Evaluate the roles and responsibilities of, and coordination between, the City of Los Angeles' EOC and the CICC/ISOC during a cyber-incident.	Intelligence and Information Sharing Operational Coordination			M	
Develop a shared understanding between the City EOC and CICC/ISOC of cyber-incidents (e.g., status, severity), their impacts on City operations and the community, and the expectations of the EOC and CICC/ISOC on each other during prevention and response efforts.	Intelligence and Information Sharing Operational Coordination Planning			M	
Talk through and continue to explore what, if any, additional modifications are required to the City's <i>Cyber Incident Response Policy</i> . Discussion will be used to determine the Policy's effectiveness to coordinate the City's cyber incident response by assessing the level of awareness of cyber-security roles across City departments, information sharing and coordination requirements, and the City's cyber command, control, and resource coordination capabilities.	Cyber Security Intelligence and Information Sharing Interdiction and Disruption Operational Coordination Planning		S		
Discuss the capabilities of the City to detect malicious activity, conduct countermeasures, accomplish mitigations, and perform operations in response to a cyber-attack according to the <i>Cyber Incident Response Policy</i> and department-specific protocols.	Cyber Security Interdiction and Disruption		S		
Continue to explore what, if any, hazard-specific modifications are required to supplement the City's <i>EOC Policy and Procedures Manual</i> to effectively address the unique consequence-management efforts resulting from a cyber-attack (e.g., EOC objectives, role, staffing, organization, information management, resource management, City policies).	Intelligence and Information Sharing Operational Coordination Planning		S		
<p>Ratings Definitions:</p> <p>1. Performed without Challenges (P): The critical tasks associated with the objective were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.</p>					

2. **Performed with Some Challenges (S):** The critical tasks associated with the objective were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.
3. **Performed with Major Challenges (M):** The critical tasks associated with the objective were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.
4. **Unable to be Performed (U):** The critical tasks associated with the objective were not performed in a manner that achieved the objective(s).

Objective 1: Evaluate the roles and responsibilities of, and coordination between, the City of Los Angeles' EOC and the CICC/ISOC during a cyber-incident.

Objective 2: Develop a shared understanding between the City EOC and CICC/ISOC of cyber-incidents (e.g., status, severity), their impacts on City operations and the community, and the expectations of the EOC and CICC/ISOC on each other during prevention and response efforts.

The critical tasks associated with these objectives were completed in a manner that achieved the objective, but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional risks for city operations, the public, or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with these objectives are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 1/2.1: The exercise was a perfect demonstration of how technical responders and emergency management should interact when cyber intelligence becomes available and during responses to actual cyber-attacks. The exercise was designed in such a way as to have emergency managers and technical responders in the same room having a discussion with each other about their relative roles, needs, and functions. Through that interaction, the technical responders and emergency management personnel were able to develop a complete understanding of the situation and the actions required by both parties. However, had it not been for the artificiality of the exercise being a scheduled event those interactions may not occur during real-world incidents. The policy representatives from both groups must work together to ensure the interaction and open communications that occurred during the exercise become a regular occurrence when cyber intelligence information is received and cyber-incidents occur in the real-world.

Strength 1/2.2: The Emergency Management Department has a number of avenues for providing the leadership and emergency management staff of City Departments with situational updates and emergency instructions (e.g., EMD Bulletins, EOC Situation Reports). The EMD offered to make its notification systems available to the CICC to reinforce its messaging and instructions. This would help ensure messages don't just reach technical responders (the focus for CICC notifications), but also Department leadership and emergency management personnel (the focus of EMD/EOC notifications). The CICC need only provide the content of the messages to the EMD Duty Officer and it will quickly relay the messages to its distribution lists as it regularly does with other emergency messages.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 1/2.1: The trigger points and process for engaging emergency management functions (within departments and city-wide) need to be more clearly defined.

Reference(s): City of Los Angeles, *Cyber Incident Response Policy* 2016

Analysis: As previously mentioned in the above strengths, the exercise was a perfect demonstration of how technical responders and emergency management should interact in light of cyber intelligence as well as during responses to actual cyber-attacks. However, had it not been for the artificiality of the exercise being a facilitated event, those interactions may not occur in the same fashion during real-world incidents. First, trigger points for notifying emergency management of the occurrence of a cyber-incident were not followed during the exercise. For example, during discussions of the denial of service attack on the City's 3-1-1 system, some technical responders commented that they may not notify the CICC or Los Angeles Police Department's (LAPD's) Real-Time Analysis and Critical Response (RACR) Unit (per policy) if the problem can be addressed internally and if it is not affecting other systems. However, emergency management participants pointed out when 3-1-1 goes down, the public's immediate alternative is to call 9-1-1, which quickly becomes overwhelmed and thereby interferes with genuine emergency calls. Although notifications to the CICC and RACR of these types of incidents are required in policy; departments may not be following policy per this example. This may have been an anomaly of the exercise, but because of its importance and potential consequences, the lack of notifications has been noted here. Likewise, it was determined the 3-1-1 attack could impact other systems operating on the same platform. There could be significant cascading impacts on department operations and city functions depending on the nature of the attack that would need to be disclosed to emergency management so potential consequences could be mitigated. This failure to communicate during the exercise does not reflect the ability of proprietary departments and technical responders to detect a problem, but instead a need to improve communications and notifications related to the detection.

A process for ensuring emergency management is notified and engaged early for the purposes of consequence management related city operations and physical infrastructure is not currently in place. Even within impacted proprietary departments, emergency management coordinators assumed their technology teams would notify them of an incident, but they could not be sure as policies within proprietary departments are not formally codified. Furthermore, the need for notification of the City's Emergency Management Department (EMD) is currently omitted from the list of stakeholders whom RACR Unit will notify in the *Cyber Incident Response Policy*. Lastly, it would be beneficial for the emergency management community if the notification could convey the severity or potential severity of the cyber-incident on city operations and/or the community (i.e., 1 - 5 severity rating with 1 being minimal and 5 being extremely serious; or "watch," "warning," "alert" classifications); thereby affording emergency management an easier decision regarding how to respond or whether to activate the EOC. It should be the responsibility of affected proprietary departments or the ITA to

communicate the potential impacts of the cyber-attack on their infrastructure and operations to the CICC or RACR, which could then relay the information to emergency management. The *Cyber Incident Response Policy* uses a severity matrix to categorize the impacts on systems (e.g., regular, supplemented, extended, and not recoverable), but the Policy's categories do not relay impacts on city operations and/or the community to emergency management. A supplemental severity matrix could be built upon the existing systems severity matrix that could reflect information received from affected proprietary departments or the ITA regarding potential impacts on city operations or physical infrastructure, and thereby provide emergency management with the information they need to prepare for and address consequences.

Area for Improvement 1/2.2: Proprietary departments and the ITA must ensure information conveyed to the CICC/RACR and ultimately emergency management, addresses the potential consequences of the cyber-incident on physical infrastructure, city operations, and/or the community (essential elements of information necessary for consequence management).

Reference(s): City of Los Angeles, *Cyber Incident Response Policy* 2016

Analysis: The exercise did an excellent job of demonstrating the information needs of emergency management to the technical responders. As the technical responders assessed the scenario they discussed highly technical topics such as confirmation of the attack vector, public facing systems vs. private, cloud-based systems vs. server-based, front-end systems vs. back, etc. The emergency management group was clear those technical details are not their primary concern, but rather what the impacts on systems will mean to city operations, infrastructure, and the public. For example, it was determined the denial of service attack on the City's 3-1-1 system could affect all other systems using the same pathway. The emergency management group asked what the other systems were that could be impacted; voicing concern over traffic management systems, 9-1-1/Computer-Aided-Dispatch, telecommunications, the electric grid, water and sewer systems, etc. The technical group was able to eliminate some emergency management concerns (i.e., 9-1-1 is on a separate, isolated system), but due to the limited information in the scenario they were not able to assess during the exercise the other systems using the same pathway. Nonetheless, for demonstration purposes, that interaction illustrated the information needs of emergency management and their desire for actionable information related to potential physical consequences and impacts on city operations. As relayed from impacted proprietary departments or the ITA (as appropriate), the ISOC and/or CICC must be capable of then communicating to emergency management the essential elements of information for consequence management. Likewise, emergency management must be poised to, and capable of, asking clarifying questions of technical groups when they feel additional information is needed or information currently being provided is insufficient to support consequence management.

Area for Improvement 1/2.3: The role and involvement of the Information Technology Agency (ITA) in the City's EOC needs to be coordinated between EMD and the ITA.

Reference(s): *EOC Policy and Procedures Manual*

Analysis: The current positions for the ITA in the City's EOC are intended for technical assistance to the EOC, not policy coordination or liaison with the department. The

emergency management participants discussed the need and expectation to have the ITA represented in the EOC Management Section (possibly as a Deputy EOC Director), in other Sections as technical specialists to interpret the details of the cyber-incident into laymen's terms and identify potential consequences, and potentially in the Liaison Group (as an Agency Representative) or Operations Section (as a Branch Director or Unit Leader) as a liaison back to the ITA's Department Operations Center (DOC). This involvement would not only require a modification to the *EOC Policy and Procedures Manual*, but would require the consent of the ITA to deploy those personnel during a cyber-related incident and commit those personnel to necessary preparation activities (e.g., training, exercising). In the past, the ITA has been hesitant to commit to filling an EOC Deputy Director position, but the value of such involvement was widely lauded by the emergency management participants. However, the EOC staffing strategy for ITA must practically consider the ITA's other commitments. For example, the EOC cannot expect the CISO to be present if s/he is also responsible for co-chairing the CICC, managing the ISOC, and coordinating ITA's response efforts. In addition, if the ITA is going to be the sole technical advisor to the EOC, its representatives must be familiar with the capabilities and systems of the other proprietary departments (e.g., LAWA, POLA, DWP). This would further justify the need for mandatory coordination, information sharing, and decision-making as addressed in Area for Improvement 3.1.

Objective 3: Talk through and continue to explore what, if any, additional modifications are required to the City's *Cyber Incident Response Policy*. Discussion will be used to determine the Policy's effectiveness to coordinate the City's cyber incident response by assessing the level of awareness of cyber-security roles across City departments, information sharing and coordination requirements, and the City's cyber command, control, and resource coordination capabilities.

The critical tasks associated with this objective were completed in a manner that achieved the objective; however, opportunities to enhance effectiveness and/or efficiency were identified. Performance of this activity did not contribute to additional risks for city operations, the public, or for emergency workers, but in some cases it was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 3.1: Though the City *Cyber Incident Response Policy* was recently finalized prior to the exercise, the four Departments with their own information technology systems (ITA, LAWA, DWP, and POLA) had already established Cyber Incident Response Teams (CIRTs) in accordance with the Policy, including which functions should be staffed (e.g., public affairs). While some were further along than others related to the development of procedures and application of resources in accordance with the Policy, all demonstrated an understanding of the requirements and a strategy to continue building their capabilities.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 3.1: The command, control, and coordination process for decision-making within the CICC needs to be defined (e.g., a centralized, hierarchical structure, Multi-Agency Coordination (MAC) Group principles).

Reference(s): City of Los Angeles, *Cyber Incident Response Policy* 2016

Analysis: The CICC is currently co-chaired by the Mayor's Office and the City's Cyber Information Security Officer (CISO). However, the CISO only has authority over the tactics applied by the ITA and neither has authority over the tactics used by the other three proprietary departments with their own information technology systems (e.g., Dept. of Water and Power, Los Angeles World Airports, Port of Los Angeles). There was concurrence that the City's cyber infrastructure is only as strong as its weakest link and many of the departments share systems and infrastructure. For example, the City's 3-1-1

system is housed on DWP infrastructure, but is operated using ITA software and is maintained by the ITA. Nonetheless, there was some reluctance to share information and coordinate tactics across departments to ensure a coordinated, enterprise-wide response and security strategy. While the CICC serves as a policy body for coordinating the tactical response to a cyber-attack among affected departments there is a rare chance members may not agree to a solution in times of crisis and could then implement tactics that are counterproductive to city-wide objectives. Without a centralized authority on the CICC nothing can currently compel departments with their own systems to fall in line with city-wide objectives, share critical information, or agree to an enterprise-wide tactical solution. Participants voiced opinions for both a centralized authority (e.g., ITA CISO, Mayor's Office) and MAC Group principles applied to the proprietary departments and ITA (built upon respecting the authority of each department while fostering consensus-driven decisions to achieve an enterprise-wide solution). Both approaches can be successful, but a decision-making policy should be selected and codified in the *Cyber Incident Response Policy* for those rare occurrences when proprietary departments and/or ITA may not agree on solutions or tactics. This will help ensure information is shared and tactics are coordinated across departments to achieve city-wide objectives.

Area for Improvement 3.2: The roles, relationship between, and internal functionality of the ISOC and CICC Working Group need to be more clearly defined in policy.

Reference(s): City of Los Angeles, *Cyber Incident Response Policy* 2016

Analysis: Per the description of the Mayor's Office, the ISOC is a centralized database that is populated and monitored by technical experts continuously, with or without an incident. The purpose of the ISOC is to enable analysts City-wide to monitor prospective threats and analyze threats and/or attacks as they come into the City. It is not a participatory, policy-making organization like the CICC Working Group. Meanwhile, the CICC Working Group is responsible for overall cyber-incident coordination, information management, resource coordination, and facilitates tactical cyber-priorities and cyber-related policy/decisions. During the exercise, the technical group had a solid understanding of the differences between the ISOC and CICC. The emergency management group, however, was less clear on the differentiation as their interpretation of the *Cyber Incident Response Policy* was different. For example, the CICC Working Group and its role in managing an incident are not defined in the "IR Stakeholders Roles and Responsibilities" section of the Cyber Policy, nor are its roles in the four phases of the Incident Response Policy Flow. Furthermore, use of the title "operations center" and the inclusion of ISOC responsibilities for "collaboration" have particular meaning in the emergency management community. They translate to more a participatory role that typically includes coordination of information, resources, and policy/decisions. As a result, it was not clear to emergency management participants with whom they would be coordinating resources, information, and city-wide priorities (later determined during the exercise to be the CICC not the ISOC). This then brought participants to question how the CICC Working Group would convene, be organized, and its processes for communicating and operating to perform its management and coordination responsibilities. For example, the City's EOC uses a combination of the Incident Command System (ICS) and Emergency Support Functions (ESFs) to organize

personnel, assign responsibilities, and dictate processes for achieving the EOC's mission. Emergency management participants encouraged the CICC to adopt and codify an organization, assign responsibilities, and employ processes to facilitate its objectives and ensure effectiveness.

Area for Improvement 3.3: Through policy and relationships, the CICC Working Group should continue to facilitate information sharing and tear down information sharing barriers between Departments.

Reference(s): Mayor's Executive Directive #2 - Cyber Security Policy

City of Los Angeles, *Cyber Incident Response Policy* 2016

Analysis: Over the past two years, the CICC has achieved monumental progress related to information sharing across City Departments. Proprietary departments and the ITA have provided access to relevant information proportionate to the capabilities and security of the ISOC. As the capabilities and security of the ISOC continue to improve, those departments will hopefully continue to be forthright with their information. However, the exercise illustrated there may still be some reluctance on the part of some proprietary departments to openly share cyber-related information with the ISOC and the CICC Working Group members. In some cases there appear to be genuine regulatory limitations regarding the sharing of information, but in other cases it appears to be concerns over trust/security or be territorial, bureaucratic, or political in nature. As identified in Area for Improvement 1/2.1, departments that are only looking at situations from their point of view may fail to consider significant ramifications on other departments, physical infrastructure, or city operations. For example, related to the inoperability of the Valley Generating Station (per the scenario), the DWP mentioned there may be no power outages caused by that incident. Although the DWP knew the closing of the station was related to a cyber-incident, exercise participants stated they may not share that information further if there were no consequences of the station going offline. Participants from other departments explained the critical time to prevent attacks on other systems was the time between the Valley Generating Station and Harbor Generating Station failing two days later (per the scenario). However, if not informed of the situation, other departments would not have the ability to monitor and protect their own systems and emergency management would not be able to proactively prepare for other potential consequences. Regarding that latter point, after the Harbor Generating Station failed and power outages began (per the scenario), the DWP explained the problem could hypothetically be the result of a software update from General Electric, which could then effect every DWP generating station and lead to city-wide power outages. That would then lead to catastrophic consequences for emergency management who would be relegated to a reactive posture if never told of the first incident and its potential consequences. The DWP was not the only department less than forthcoming with information; however, the above example was an excellent illustration of the importance of proactive and uninhibited information sharing.

This page is intentionally blank.

Objective 4: Discuss the capabilities of the City to detect malicious activity, conduct countermeasures, accomplish mitigations, and perform operations in response to a cyber-attack according to the *Cyber Incident Response Policy* and department-specific protocols.

The critical tasks associated with this objective were completed in a manner that achieved the objective; however, opportunities to enhance effectiveness and/or efficiency were identified. Performance of this activity did not contribute to additional risks for city operations, the public, or for emergency workers, but in some cases it was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 4.1: The City's strong relationships with the Federal Bureau of Investigation (FBI), U.S. Secret Service (USSS), and Department of Homeland Security's National Cyber and Communications Integration Center (NCCIC) are of tremendous value to its cyber security program. For example, all Federal counterparts offered to share detailed information about incidents occurring elsewhere (i.e., the scenario included a cyber-attack on the St. Louis electric grid and Federal partners offered to provide Los Angeles with the code so they could monitor their systems and information related to the consequences being experienced in St. Louis). In addition, they offered resources and support for the City's response and investigation efforts. Most importantly, they offered a culture of partnership, support, and openness.

Strength 4.2: The City's proprietary departments and the ITA have implemented the latest technologies to enhance detection, prevention, and response capabilities. The CICC has adopted the National Institutes for Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. In addition, the creation and operation of the ISOC has significantly improved cyber security collaboration among city departments and with their partners from the public and private sectors. While there is always additional work to be done, these steps represent significant progress toward improved detection, mitigation, and response capabilities in a short period of time.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 4.1: The City's current staffing levels for information technology and cyber security personnel (within Departments and for the CICC, CIRTs, and ISOC) remain insufficient to combat the growing threat and the capacity needed to respond to a major cyber-incident.

Reference(s): None

Analysis: As referenced in the City’s 2015 Cyber Security Tabletop Exercise After-Action Report, staffing levels related to the technical expertise needed to combat cyber-threats on a daily basis and respond to cyber-incidents remain too low. For example, all of the members of the CICC Working Group, all those that will be pulled to be on City Cyber Incident Response Teams (CIRTs), and all those that will be pulled to support the ISOC and the City EOC are the day-to-day information technology/cyber security personnel of city departments. In light of the scenarios being exercised, each participating Department voiced hesitation about sending their essential technology staff to support other functions when they would be needed to lead or support the protection, mitigation, and response efforts for the department at which they work. At the time of the exercise, nearly every member of the City’s technology community was being double tasked to support department-specific efforts and city-wide response/coordination activities (e.g., CICC, CIRT, ISOC, EOC). The City’s approach for cyber-incident response as captured in the *Cyber Incident Response Policy* is sound, but it may prove to be a theory that cannot be practically applied if current staffing levels don’t have the bandwidth to support the many functions contained within it.

Area for Improvement 4.2: The continued development and sharing of enterprise-wide network and data flow diagrams will help the City in all aspects of cyber prevention, response, and recovery, including providing critical information on consequences to emergency management.

Reference(s): Network and Data Flow Diagrams

Analysis: Since the 2015 Cyber Security Tabletop Exercise, the City took great strides to develop a critical asset inventory. During the exercise, the critical asset inventory helped the City better understand its essential systems and what the consequences may be if those systems are compromised. However, proprietary departments and the ITA are still working to develop and share network and data flow diagrams that identify how those critical systems are related. Accessibility to that information will allow the CICC to predict the possible spread or impacts of a cyber-incident affecting City systems or, at minimum, explain correlations between incidents. In addition, the sharing of network and data flow diagrams will also inform the CICC’s response strategies – whether to isolate systems, block network activity, disable services, reimagine infected systems, enhance monitoring, replace compromised systems/files, etc. – and the sequence of those events and possible ramifications of those decisions. All existing network and data flow diagrams need to be made available to the CICC upon request to support strategic and tactical decision-making. Where network and data flow diagrams do not yet exist, proprietary departments or the ITA should continue their efforts to develop them as quickly as possible.

Area for Improvement 4.3: The role and value of the City-wide Cyber Incident Response Team (CIRT) in light of strong Department-specific CIRTs requires review.

Reference(s): City of Los Angeles, *Cyber Incident Response Policy* 2016

Analysis: The CICC members had difficulty explaining the specific role City-wide CIRTs would play during a response if each proprietary department with its own information technology system has a strong Department-specific CIRT. At multiple times, CICC members discussed deploying a City-wide CIRT in response to multiple,

simultaneous incidents contained in the scenario; however, the participants struggled to determine to which incident(s) a City-wide CIRT would be sent, what the City's capacity is for multiple simultaneous CIRT activations, how the CIRT would be managed, and what specific role(s) it would play once deployed. In addition, as Area for Improvement 4.1 described, the City-wide CIRT concept currently relies on staff from existing Department-specific CIRTs. The departments expressed hesitation to release their technical personnel to other purposes during an incident and explained the current strategy creates a disadvantage for Department-specific CIRTs which are intended to be the on-call and frontline technical responders. If the intention of the City-wide CIRTs is to provide support, surge staffing, investigative support, and/or expertise to Department-specific CIRTs, then those purposes should be reviewed and a viable strategy for meeting those objectives should be determined. For example, the ITA is currently striving to create a CIRT intended to support the response efforts of other impacted departments. This separate team may be the solution to this issue. On the other hand, a robust resource management program operated by the CICC may be a better option than creating City-wide CIRTs in light of strong Department-specific CIRTs. In either case, the role and value of City-wide CIRTs in light of strong Department-specific CIRTs should be reviewed and any changes, if applicable, should be reflected in updated policies and plans.

Area for Improvement 4.4: A formal, enterprise-wide strategy for cyber security-related training and exercising of end-users, management/executives, and technicians needs to be developed.

Reference(s): Cyber Security Training and Exercise Program

Analysis: Nearly 80% of cyber threats can be mitigated if City staff and system users avoid the common mistakes that often expose the City to malware, intrusions, and other cyber threats. While many steps have been taken by the CICC, ITA, and each proprietary department to educate end-users, management/executives, and technicians; more resources and a formal strategic approach need to be applied to this purpose enterprise-wide. All the security technology the City can acquire will never compensate for the risk posed by human cyber behavior. Training on this topic needs to not be limited to annual refresher courses, but rather ongoing and regular training, messaging, organizational culture (e.g., leadership messaging), exercising, and enforcement. If the City finds its training is not successful, then it may need to ultimately consider re-evaluating end-user policies to ensure cyber security (e.g., "de-minimus use" policies).

This page is intentionally blank.

Objective 5: Continue to explore what, if any, hazard-specific modifications are required to supplement the City’s *EOC Policy and Procedures Manual* to effectively address the unique consequence-management efforts resulting from a cyber-attack (e.g., EOC objectives, role, staffing, organization, information management, resource management, City policies).

The critical tasks associated with this objective were completed in a manner that achieved the objective; however, opportunities to enhance effectiveness and/or efficiency were identified. Performance of this activity did not contribute to additional risks for city operations, the public, or for emergency workers, but in some cases it was not conducted in accordance with applicable plans, policies, and procedures. The strengths and areas for improvement, and more importantly, the root causes, associated with this objective are described in this section.

Strengths

The following strengths related to this objective were demonstrated during the exercise and contributed to the objective being met:

Strength 5.1: The *EOC Policy and Procedures Manual* affords the EOC great adaptability for any and all hazards, including cyber-incidents. For example, under its current policies, the EOC is able to accommodate appropriate technical specialists, integrate non-traditional representation into the EOC Management Section to influence policy and direction (e.g., DWP, ITA), gather information from many sources, develop and distribute synthesized and actionable situational awareness, and coordinate highly technical resources. In addition, the EOC has the authority to adjudicate issues among the departments with their own information technology systems in the event agreement cannot be reached at a lower level. No specific modifications to the *EOC Policy and Procedures Manual* were identified during the exercise; however, some of the specifics related to how the policies are applied to a cyber-incident should be codified in supporting documents.

Strength 5.2: The emergency management group demonstrated a strong understanding of how to manage the consequences of the cyber-attack on city operations and the community. In only a few brief moments after reading the Module 2 scenario, the EOC’s leadership was able to establish priorities, identify coordination requirements, and identify resources that would be needed. Multiple departments, especially the Port of Los Angeles, demonstrated similar capabilities for understanding the magnitude of the situation, selecting priorities, and selecting tasks/actions to mitigate and address the physical consequences.

Areas for Improvement

The following root causes require improvement to achieve the full capability level associated with this objective:

Area for Improvement 5.1: Each City Department’s Continuity of Operations (COOP) Plans need to include manual or alternative approaches for all essential functions/processes dependent on information technology.

Reference(s): City of Los Angeles, Continuity of Operations (COOP) Plan Template 2016

Department COOP Plans

Analysis: As determined during the exercise, most City Departments have effectively identified the information technology and communications resources their functions are dependent upon. Most of those Departments have informed their information technology teams of those essential systems/data and necessary recovery time and point objectives. They have instructed the technology teams to protect, back-up, or ensure access to those systems and data through whatever means necessary. What few Departments have done is have those system/data end-users (those responsible for essential functions/processes) determine how they can perform functions if the technology teams are unable to provide the requested systems/data (not to any fault of their own, but potentially because of very sophisticated cyber-attacks). As of this exercise, most departments had not considered other manual or alternative approaches if systems/data are not available; essentially “resting on their laurels” that technology teams will be 100% successful in restoring systems/data within recovery time objectives and to recovery point objectives. In the event of a sophisticated cyber-attack or other incident that impacts systems/data, the consequences on city operations and capabilities will be significantly reduced if COOP Plans include manual and alternative approaches for essential functions dependent on information technology.

Area for Improvement 5.2: The City must be positioned to effectively communicate to the public during cyber-incidents.

Reference(s): *EOC Policy and Procedures Manual*

2015 City of Los Angeles Functional Exercise After-Action Report

Analysis: Emergency public information was not a specific objective of the exercise and was not specifically evaluated; however, discussions had during the exercise and during the expert presentations that followed, illustrated the importance of effectively communicating to the public during a cyber-incident. Once physical consequences of a cyber-attack become evident in the community, the public and media will immediately look to the City for resolution and clarification on the situation. Because of the nature of cyber-attacks, the City may have difficulty predicting the consequences or progression of the attack. The participants agreed it was appropriate to be honest with the public about the nature of the attack and the potential consequences. More so, provide the public with emergency instructions regarding what they can do to protect themselves and how they can support the City’s response efforts (i.e., if 3-1-1 is affected, citizens should not call 9-1-1 as an alternative unless it’s an emergency situation). The EOC’s 2015 Functional Exercise resulted in a number of areas for improvement related to the management and release of public information that will not be reiterated in this report. However, this exercise reinforced the importance of this emergency management function. Likewise, it

reinforces the emphasis and corrective actions related to information sharing between technical responders and the emergency management community found in this report (e.g., precautionary notifications to emergency management, technical specialists in the EOC). As participants stated, an ineffective public information campaign could cause more significant problems for emergency management than the cyber-attack itself.

This page is intentionally blank.

APPENDIX A: IMPROVEMENT PLAN

Based on the evaluations contained in this After-Action Report, this Improvement Plan (IP) has been developed to capture the corrective actions agreed to by the participating organizations and identifies information relevant to the monitoring of progress related to each corrective action.

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
1: Evaluate the roles and responsibilities of, and coordination between, the City of Los Angeles' EOC and the CICC/ISOC during a cyber-incident. 2: Develop a shared understanding between the City EOC and CICC/ISOC of cyber-incidents (e.g., status, severity), their impacts on City operations and the community, and the expectations of	1/2.1: The trigger points and process for engaging emergency management functions (within departments and city-wide) need to be more clearly defined.	1/2.1.1. The Cyber Security Incident Notification protocols will be updated to reflect the City's official, all-hazards incident notification process, which includes the addition of the EMD Duty Officer.	High	Planning	CICC	N/A	4/1/16	Ongoing
		1/2.1.2. The EMD and CICC will review the existing CICC incident classification categories to develop supplemental categories that are informative to emergency management (e.g., Level I, II, or III; "watch," "warning," "alert" classifications) and reflect the potential consequences on physical infrastructure and/or city operations as identified by affected departments.	High	Planning	CICC EMD	N/A Operations Division	4/1/16	10/1/16
		1/2.1.3. The EMD and CICC will institutionalize a process for engaging each other in a conversation (not simply notifying, but hosting	High	Planning	CICC EMD	N/A Operations Division	4/1/16	10/1/16

¹ Capability Elements are: Planning, Organization, Equipment, Training, or Exercise.

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
the EOC and CICC/ISOC on each other during prevention and response efforts.		conference calls, in-person meetings, etc.) regarding the implications of cyber intelligence or cyber-incidents on City operations and physical infrastructure and the potential need for emergency management action (e.g., EOC activation).						
		1/2.1.4. The CICC will invite EMD's Duty Officers (and other EMD staff is deemed appropriate by EMD) to tour the ISOC and orient them with the City's cyber security operations. The CICC and EMD will then work together to host regular discussions and/or tabletop exercises with EMD Duty Officers (and other EMD staff as appropriate) to maintain relationships and familiarity with the subject matter.	High	Planning	CICC EMD	N/A Duty Officers	4/1/16	Ongoing
	1/2.2: Proprietary departments and the ITA must ensure information conveyed to the CICC/RACR and ultimately emergency management, addresses the potential	1/2.2.1. The CICC will identify members from among its ranks that have an understanding of emergency management and the bigger consequence picture and will assign those individuals to serve as liaisons to EMD and/or the City EOC.	Medium	Organization	CICC	N/A	4/1/16	6/1/16
		1/2.2.2. The EMD and CICC will develop a Situation Reporting process and	High	Planning	CICC EMD	N/A Operations	4/1/16	10/1/16

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	consequences of the cyber-incident on physical infrastructure, city operations, and/or the community (essential elements of information necessary for consequence management).	resources to facilitate CICC reporting to the EMD/EOC that includes the essential elements of information for consequence management.				Division		
		1/2.2.3. Per corrective actions 1/2.1.4 and 4.4.1, the EMD and CICC will engage in more regular joint meetings, educational opportunities, trainings, and exercises to improve communications, relationships, and subject matter familiarity.	Medium	Planning Training Exercise	CICC EMD	N/A Multiple Divisions	4/1/16	Ongoing
	1/2.3: The role and involvement of the Information Technology Agency (ITA) in the City's EOC needs to be coordinated between EMD and the ITA.	1/2.3.1. The EMD and ITA will determine what ITA representation is needed in the City EOC during a cyber-incident and how those positions will be organizationally and physically integrated into the EOC.	High	Planning Organization	EMD ITA	Operations Division Executive Leadership	4/1/16	10/1/16
		1/2.3.2. The <i>EOC Policy and Procedures Manual</i> will be updated to codify the roles and responsibilities of the ITA in the EOC during a cyber-incident (and/or other hazards as appropriate).	Medium	Planning	EMD	Operations Division	4/1/16	10/1/16
		1/2.3.3. The ITA will select individuals (at least three deep for each position) to staff the mutually agreed upon positions in the EOC	Medium	Organization	ITA	Executive Leadership	4/1/16	10/1/16

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
		and then commit those individuals to necessary EOC preparedness activities (e.g., training).						
3: Talk through and continue to explore what, if any, additional modifications are required to the City's <i>Cyber Incident Response Policy</i> . Discussion will be used to determine the Policy's effectiveness to coordinate the City's cyber incident response by assessing the level of awareness of cyber-security roles across City departments, information sharing and coordination requirements, and the City's cyber	3.1: The command, control, and coordination process for decision-making within the CICC needs to be defined (e.g., a centralized, hierarchical structure, Multi-Agency Coordination (MAC) Group principles).	3.1.1. The CICC will conduct an assessment of the best decision-making approach to facilitate its purpose (e.g., centralized, hierarchical approach, MAC Group principles).	High	Planning	CICC	N/A	4/1/16	10/1/16
		3.1.2. The CICC will codify the selected decision-making approach in the City's <i>Cyber Incident Response Policy</i> (e.g., centralized, hierarchical approach, MAC Group principles).	High	Planning	CICC	N/A	4/1/16	10/1/16
	3.2: The roles, relationship between, and internal functionality of the ISOC and CICC Working Group need to be more clearly defined in policy.	3.2.1. For the benefit of emergency management, the CICC will update the City's <i>Cyber Incident Response Policy</i> to more clearly reflect the roles of the ISOC and CICC Working Group during a cyber-incident.	Medium	Planning	CICC	N/A	4/1/16	10/1/16
		3.2.2. Along with Corrective Actions 3.1.2 and 4.3.2, the CICC will define in either the <i>Cyber Incident Response Policy</i> or an annex/appendix thereof, the means by which it will manage information, resource coordination,	Medium	Planning	CICC	N/A	4/1/16	4/1/17

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
command, control, and resource coordination capabilities.		priority setting, and policy (including organization, assignment of roles/responsibilities, and processes).						
	3.3: Through policy and relationships, the CICC Working Group should continue to facilitate information sharing and tear down information sharing barriers between Departments.	3.3.1. The CICC will continue to foster positive relationships and uninhibited information sharing while respecting the confidentiality of the information being provided.	Low	Planning Organization	CICC	N/A	Ongoing	Ongoing
		3.3.2. As the capabilities and security of the ISOC improve, proprietary departments will continue to provide access to information and will self-identify and eliminate territorial, bureaucratic, or political inhibitors to information sharing.	Low	Planning Organization	ITA DWP LAWA POLA	N/A	Ongoing	Ongoing
4: Discuss the capabilities of the City to detect malicious activity, conduct countermeasures, accomplish mitigations, and perform operations in response to a cyber-attack	4.1: The City's current staffing levels for information technology and cyber security personnel (within Departments and for the CICC, CIRTs, and ISOC) remains insufficient to combat the growing threat	4.1.1. In association with its cyber-security personnel re-classification process, the Personnel Dept., with the support of the CICC, will develop a Strategic Human Capital Plan for technology/cyber-security personnel comparing current and future staffing needs with current capabilities and lays out a long-term approach to address the gap.	High	Planning Organization	Personnel Dept. CICC	TBD N/A	4/1/16	4/1/17

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
according to the <i>Cyber Incident Response Policy</i> and department-specific protocols.	and the capacity needed to respond to a major cyber-incident.							
	4.2: The continued development and sharing of enterprise-wide network and data flow diagrams will help the City in all aspects of cyber prevention, response, and recovery, including providing critical information on consequences to emergency management.	4.2.1. Each Department will develop or continue to develop and maintain comprehensive network and data flow diagrams.	High	Planning	ITA DWP LAWA POLA	N/A	Ongoing	Ongoing
		4.2.2. Each Department will make its network and data flow diagrams available to the CICC/ISOC for review upon request.	High	Planning	ITA DWP LAWA POLA	N/A	4/1/16	Ongoing
	4.3: The role and value of the City-wide Cyber Incident Response Team (CIRT) in light of strong Department-specific CIRTs requires review.	4.3.1. The CICC will review the role of the City-wide CIRT in light of strong Department-specific CIRTs and will make any changes deemed necessary to policy and plans	Medium	Planning	CICC	N/A	4/1/16	10/1/16
	4.4: A formal, enterprise-wide strategy for cyber	4.4.1. The CICC will develop a formal, enterprise-wide Multi-Year Training and	Medium	Planning	CICC	N/A	4/1/16	4/1/17

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
	security-related training and exercising of end-users, management/executives, and technicians needs to be developed.	Exercise Plan (TEP) detailing the cyber-security related training courses intended to be offered across City Departments (offerings, intended participants, scheduling) and associated Department-specific and city-wide cyber-related exercises (illustrating a building-block approach that progressively builds capabilities).						
5. Continue to explore what, if any, hazard-specific modifications are required to supplement the City's <i>EOC Policy and Procedures Manual</i> to effectively address the unique consequence-management efforts resulting from a cyber-attack (e.g., EOC objectives, role, staffing, organization, information	5.1: Each City Department's Continuity of Operations (COOP) Plans need to include manual or alternative approaches for all essential functions/ processes dependent on information technology.	5.1.1. The EMD will revise its COOP Plan Template (Section 4 and Appendix G) to include more robust instructions for Departments to formulate manual or alternative approaches for essential functions dependent upon information technology.	Medium	Planning	EMD	Planning Unit	9/1/16	12/31/16
		5.1.2. The EMD will continue to communicate to Departments their responsibilities to develop, review, and revise/maintain COOP Plans and viable COOP capabilities per Mayoral Executive Directive #16.	High	Planning	EMD	Planning Unit Operations Division	Ongoing	Ongoing
	5.2: The City must be positioned to effectively communicate to	Please note all corrective actions below are from the 2015 City of Los Angeles Functional Exercise After-Action Report associated with Objective 8 in the Improvement Plan (Appendix A).						
		5.2.1. EMD will continue to pursue Corrective Actions 1.1.2 (Staffing	High	Planning Organization	EMD	Operations Division	Ongoing	4/1/2017

Objective	Issue/Area for Improvement	Corrective Action	Priority	Capability Element ¹	Primary Responsible Organization	Responsible Unit/Division	Start Date	Completion Date
management, resource management, City policies).	the public during cyber-incidents.	Requirements) and 1.1.4 (EOC Staff Credentialing Program) from the 2014 City of Los Angeles Functional Exercise Improvement Plan.						
		5.2.2. A template for a Public Information Plan will be developed for quick reference and population during a real-world incident.	Medium	Planning	EMD	Public Information	2/28/16	8/1/2016
		5.2.3. Current and future PIO trainings (e.g., 301 and 400-level) will continue to communicate the importance of working with the EOC Section Coordinators and Management to maintain situational awareness, provide the EOC with data from media/public-sources, and the importance of proactive messaging.	Training	Low	EMD	Public Information Operations Division, Training Unit	Ongoing	Ongoing

APPENDIX B: EXERCISE PARTICIPANTS

Last Name	First Name	Position	Organization	Group/Role
Players				
Acosta	Maria	Lieutenant	Los Angeles Police Department	EOC
Alexander	David	Director, IT Security	Los Angeles Dept. of Water and Power	Technical
Askey	Mark	Emergency Management Coordinator I	Los Angeles World Airports	EOC
Bell	LaCheryl	Emergency Management Coordinator I	Emergency Management Dept.	EOC
Bhatnagar	Neeraj	Director of Policy and Programs	Office of Mayor Garcetti	Technical
Cai	Tracy	Systems Programmer	Los Angeles Library	Technical
Chen	George	Transportation Engineer	Los Angeles Dept. of Transportation	Technical
Cobos	Daniel	Lieutenant	Los Angeles Port Police	EOC
Datta	Sanjoy	Senior Systems Analyst II	Los Angeles Police Department	Technical
Dominguez	Phil	Captain	Los Angeles Fire Dept.	EOC
Donahue	Daniel	US-CERT Communications	U.S. Dept. of Homeland Security	EOC
Echols	Mike	Director, Cyber Joint Program Office	U.S. Dept. of Homeland Security	NA
Featherstone	James	General Manager	Emergency Management Dept.	EOC
Fletcher	Eric	CIRT Manager	Bureau of Engineering	Technical
Fong	Anson	Airport Chief Information Security Officer	Los Angeles World Airports	Technical
Frazier	Quentin	Emergency Management Coordinator I	Port of Los Angeles	EOC
Freeman	Robert	Emergency Management Coordinator II	Emergency Management Dept.	EOC
Furay	Jack	Senior Special Agent	United States Secret Service	Technical
Garcia	Edward	Inspector	Los Angeles Dept. of Building and Safety	EOC
Gertz	Adam	Policy	Los Angeles Mayor's Office	Technical
Hamilton	Michael	CEO	Critical Informatics Inc.	NA
Hayes	Lisa	Emergency Preparedness Coordinator II	Los Angeles Dept. of Water and Power	EOC
Hillmann	Michael	Assistant Chief of Police	Los Angeles Port Police	Technical
Hire	Douglas	Commander, 195 th Ops Group	California National Guard	EOC
Hosea	Bruce	Lieutenant	Los Angeles Police Dept.	Technical
Ipsen	Chris	Public Information Officer	Los Angeles Emergency Management Dept.	EOC
Jacobsen	Bobbi	Senior Management Analyst	Los Angeles Personnel Dept.	EOC
Jaime	Humberto	Detective	Los Angeles Police Department	Technical
Kitchener	Craig	Sergeant II LAPD	Major Crimes/ Cyber Intelligence	Technical
Lam	Thang	Analyst	Port of Los Angeles	Technical

Last Name	First Name	Position	Organization	Group/Role
Lampe	Matthew	Assistant General Manager	Los Angeles Dept. of Water and Power	Technical
Lashbrook	Traci	ATSAIC	U.S. Secret Service	Technical
Lee	Timothy	Chief Information Security Officer	Information Technology Agency	Technical
Love	Scott	Special Agent	Federal Bureau of Investigation	Technical
Malin	David	Emergency Management Coordinator II	Los Angeles Port Police	EOC
Meyerhofer	Larry	Emergency Management Coordinator II	Los Angeles Emergency Management Dept.	EOC
Munongo	Patrick	Emergency Management Coordinator I	Los Angeles Emergency Management Dept.	EOC
Orellana	Lupe	Management Analyst	Public Works/ LA Sanitation	EOC
Park	Marie	Senior Systems Analyst I	Los Angeles Dept. of Water and Power	Technical
Polychronis	Thalia	Executive Officer	Los Angeles Mayor's Office	EOC
Riebeling	Michelle	Emergency Management Coordinator I	Emergency Management Department	EOC
Robles	Eric	Director of Special Services	Los Angeles General Services Department	EOC
Roebuck	Jermaine	Senior Cyber Security Analyst	U.S. Dept. of Homeland Security	NA
Sales	Arthur	Information Systems Manager	Public Works/LA Sanitation	Technical
Sato	Kurt	DOS	Los Angeles Fire Dept.	Technical
Struyk	James	Special Agent in Charge	Federal Bureau of Investigation	Technical
Thomas	Jennifer	Police Captain	Los Angeles Police Dept./RACR Unit	EOC
Williams	Hank	Senior Load Dispatcher	Los Angeles Dept. of Water and Power	EOC
Wilson	Reuben	Director of Law & Policy	Mayor's Office of Public Safety	Technical
You	Calvin	Police Officer	Los Angeles Police Department	Technical
Exercise Staff				
Lowe	Nick	Chief Operating Officer	CPARS Consulting LLC	Lead Facilitator
Humphrey	Kathryn	President	K-Rise Enterprises Inc.	Supporting Facilitator/ Presentations/Panel Moderator
Gertz	Adam	Policy Director	Los Angeles Mayor's Office of Public Safety	Evaluator (Technical Group)
Kaurlooto	Russell	Assistant General Manager	Los Angeles Information Technology Agency	Evaluator (Technical Group)
Mata	Christine	Deputy Chief	Los Angeles Department of Transportation	Evaluator (EOC Group)
Singer	Gary	Emergency Management Coordinator I	Los Angeles Emergency Management Dept.	Evaluator (EOC Group)
Janmohamed	Meena	Junior Consultant	CPARS Consulting LLC	Data Recorder/Logistics

APPENDIX C: PARTICIPANT FEEDBACK SUMMARY

Number of Respondents	Twenty-five (25)
Summary of Demonstrated Strengths	<ul style="list-style-type: none">• Excellent exercise. (28%)²• Strong desire to improve communications across city agencies. (20%)• Good maintenance of cyber security awareness. (16%)• The necessary cyber policies are in place. (12%)
Summary of Areas for Improvement	<ul style="list-style-type: none">• Information sharing across departments and agencies needs improvement. (32%)• Need more exercises and training. (24%)• City-wide notification process needs improvement. (8%)• Laymen’s terms should be more frequently used. (8%)
Summary of Recommended Improvements	<ul style="list-style-type: none">• Cyber security awareness needs to be increased city-wide. (32%)• Emergency plans need to be modified to include cyber elements. (8%)

FEEDBACK DETAILS

The feedback details contained herein include an analysis and consolidation of the feedback received on all 25 Participant Feedback Forms. All comments were not included verbatim in this analysis; however, all comments were considered and consolidated into representative and like feedback entries. Specific and detailed comments were included as appropriate. Illegible comments were not included. In addition, comment modifiers are not included (e.g., if “staff support” was listed as a strength that is how it is listed below). Comments that received multiple responses were noted with a percentage indicating the percentage of the total respondents that made a similar comment.

² Percentages denote the percentage of total respondents who made similar comments.

DEMONSTRATED STRENGTHS

Process (56%)

- Proactive maintenance of cyber situational awareness. (16%)
- Good information sharing process in place (Nixle, bulletins, daily briefs).
- Internal CICC and ISOC procedures are well developed.
- The four departments that manage cyber assets have good foundations for cyber issues.

Coordination (52%)

- Strong desire to improve communications across city agencies. (20%)
- Strong willingness to leverage diverse resources and work with outside partners. (12%)
- Good coordination between the EOC, CICC, and ISOC.
- Good communication between the Emergency Management group and the Technical group.
- Strong awareness of and linkage to the federal resources that could be helpful.
- Strong public/private sector partnerships.
- Responses and actions from both groups were well vetted and well planned.

Exercise Conduct (52%)

- The exercise provided excellent insight into the relationship between Emergency Management (e.g., EOC) and the Technical responders (e.g., CICC, CIRTs, ISOC) and their joint response planning. (28%)
- Presentations and panel speakers were very informative. (8%)
- Great scenarios and topics of discussion.

Policy (28%)

- For the most part, the necessary cyber policies are well-developed and already in place. (12%)
- The City is demonstrating good preparedness by developing and establishing the CICC and the ISOC. (8%)

AREAS FOR IMPROVEMENT

Information Sharing (72%)

- Information sharing across departments and agencies related to cyber incidents, response actions, and vulnerabilities needs improvement. (32%)
- Communication channels between the EOC and the technical groups need to be refined. (20%)
- Notification process/protocols are unclear.
- Department policies for internal notifications need to be developed.
- Public information was not sufficiently addressed.

Process (48%)

- Additional training and exercising on this topic are necessary. (24%)
- A cyber incident response working group should be put together to address the Emergency Management functions.
- Vital records should be backed up at another location (possibly the alternate EOC in Westchester).
- Future exercises should include the LAPD Communications Division – they would be impacted if CAD/911/telephone services go down.
- Future exercises should include the Chief Information Officer from LAPD – Maggie Goodrich. She is most familiar with independencies with the Information Technology Agency (ITA) and its processes.

Understanding of Roles (44%)

- Laymen's terms should be more frequently employed. (8%)
- Command and control for the technical response needs to be more clearly defined by the CICC. (8%)
- An organization chart needs to be developed for EOC/CICC integration/joint representation.
- Technical representatives in the EOC need to be identified.
- The role of the city ISOC is not clear.
- No common body of knowledge has been defined as minimum standards for being part of an incident response team.
- Roles, responsibilities, and expectations between technical responders and emergency management should be more clearly defined.
- Comprehension of the current cyber policy is lacking.

Policy (36%)

- The citywide notification process for cyber incidents needs improvement. (8%)
- Better coordination is needed between cyber policies and emergency management policies that exist.
- Two factor authentication systems should be implemented for computer logins.
- A cloud-based repository of critical data should be created.
- More grant funding/budget should be made available to support each department's cyber security program.
- A command structure for the *Cyber Incident Response Policy* needs to be developed.

LIST APPLICABLE EQUIPMENT, TRAINING, STAFFING, POLICIES, AND PLANS/PROCEDURES THAT SHOULD BE DEVELOPED, REVISED, OR ACQUIRED (AS APPROPRIATE) TO IMPROVE THE CITY'S CYBER-INCIDENT PREVENTION AND RESPONSE CAPABILITIES.

Process (44%)

- The ISOC and Cyber Incident Response Teams need additional staff.
- Identify members from both the EOC and CICC to be part of a bi-weekly conference call (this would provide the opportunity for cross-training).

Need More Exercise and Training (40%)

- Cyber security awareness city-wide needs to be increased. (32%)
- Additional business continuity training should be held.
- A functional exercise following this tabletop exercise would be beneficial.

Policy (20%)

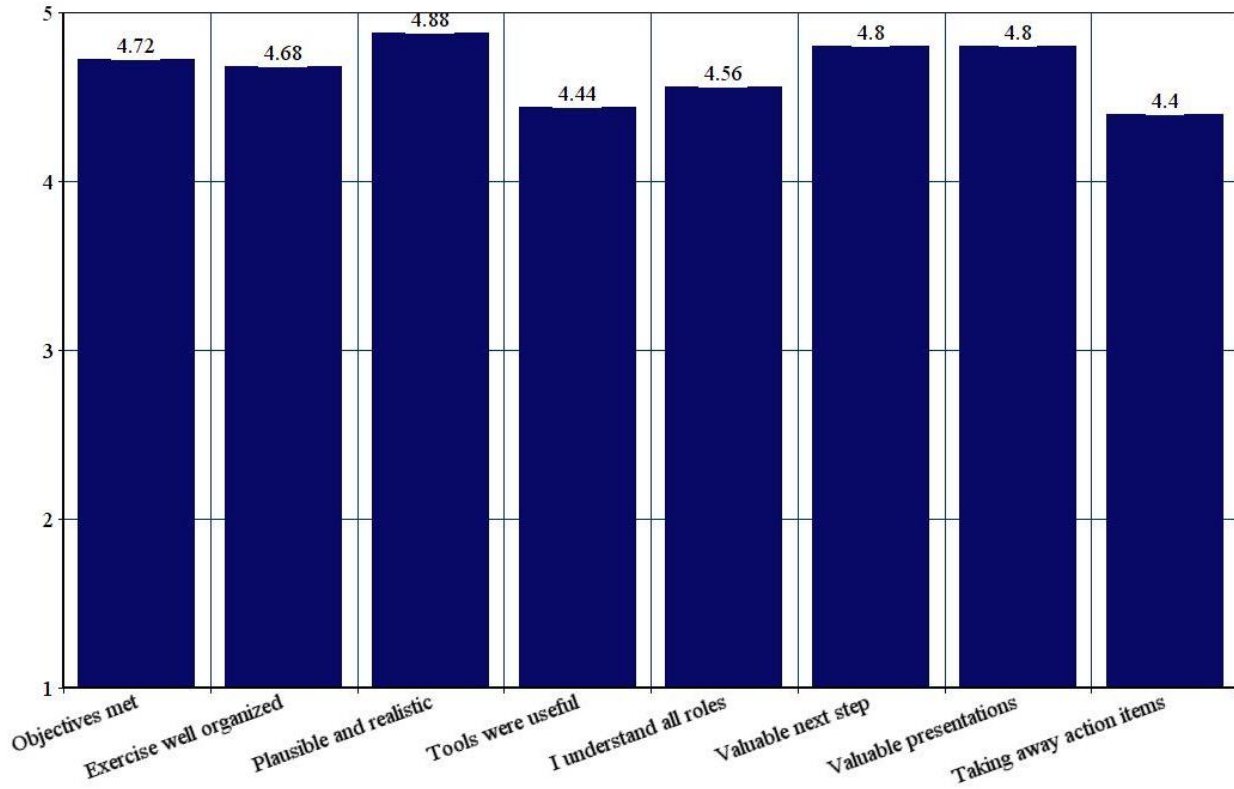
- Emergency plans need to be modified to include cyber elements. (8%)
- Computers are too easily accessible in the city. Login to systems should be done by biometrics or credentials.
- The Information Technology Agency should provide more support for the EOC, more cyber expertise, and have more of a presence in regards to staffing in the EOC.
- The Multi Agency Coordination System needs to be better integrated into the *Cyber Incident Response Policy*.
- Notification protocols need to be better developed.
- Plans to coordinate efforts to assist departments with less mature security programs need to be developed.
- There is a need for centralized IT decision-maker.

Resources (8%)

- The Cyber Incident Response Teams do not have the necessary tools to achieve their objectives (e.g., forensic tools, remediation tools).

EXERCISE ASSESSMENT

2016 Cyber Security TTX Exercise Assessment Factors



Survey Data	Strongly Disagree	Disagree	Neither Disagree nor Agree	Agree	Strongly Agree	Total Respondents*	Average Rating
A. The objectives of the exercise were met.	0	0	1	5	19	25	4.72
B. The exercise was well structured and organized.	0	0	1	6	18	25	4.68
C. The exercise scenario was plausible and realistic.	0	0	2	4	19	25	4.88
D. The Situation Manual, Fact Sheets, and other exercise materials were useful tools for participating in the exercise.	0	0	3	5	17	25	4.44

Survey Data	Strongly Disagree	Disagree	Neither Disagree nor Agree	Agree	Strongly Agree	Total Respondents*	Average Rating
E. As a result of this exercise, I have a better understanding of the roles of the EOC, the CICC, ISOC, and CIRT's and how they will coordinate during a cyber-incident.	0	0	2	7	16	25	4.56
F. The exercise served as a valuable next step in the City's ongoing efforts to develop a coordinated cyber-incident response capability.	0	0	1	3	21	25	4.8
G. The formal presentations and panel discussions presented valuable information/insights that I may not have otherwise received.	0	0	1	3	21	25	4.8
H. As a result of this exercise and the formal presentations, my department/organization is taking away action items to advance the City's cyber security capabilities.	0	0	5	5	15	25	4.4

EXERCISE CONDUCT FEEDBACK

Strengths:

- Outstanding exercise. (16%)

Areas for Improvement:

- Electronically projected notes would be more efficient than writing notes on flipcharts.
- Future exercises and trainings should provide more real-life examples/lessons learned from other government agencies that had cyber issues.
- Request for a future exercise to focus on people with disabilities and others with access and functional needs.


APPENDIX D: SUBJECT-MATTER EXPERT PRESENTATIONS AND PANEL DISCUSSION

Presenter #1: Michael Echols, MBA, CISSP
Director, Cyber Joint Program Management Office
National Protection and Programs Directorate
U.S. Department of Homeland Security

Michael Echols is the Director, Cyber Joint Program Management Office (JPMO) within the Cybersecurity and Communications (CS&C) component at the U.S. Department of Homeland Security (DHS). In this role, he leads two unique cybersecurity information-sharing programs; Enhanced Cybersecurity Services (ECS) and Cybersecurity Information Sharing Collaboration Program (CISCP).

Mr. Echols is developing and implementing cybersecurity strategies to help DHS meet its cyber mission by identifying opportunities to enhance the effectiveness of information sharing operations, technology, and policy. He has also led several White House national security initiatives. In his current role, he is the point person for the rollout of Presidential Executive Order 13691 – *Promoting Private Sector Cyber Information Sharing*.

Mr. Echols is the former Chief of the Government-Industry Planning and Management Branch, National Communications System (NCS). He chaired the Communications Sector’s Communications Government Coordinating Council (CGCC) and the Network Security Information Exchange (NSIE). Additionally, Mr. Echols managed the stand-up of the Joint Program Office under Executive Order 13618 supporting national security and emergency preparedness (NS/EP) communications. He has managed the President’s National Security Telecommunications Advisory Committee (NSTAC) where he coordinated 30 chief executive level NSTAC members representing information technology, defense, and communications companies providing policy recommendations to the President. Mr. Echols is a graduate of the National Preparedness Leadership Initiative – Harvard Kennedy School of Public Health and the Federal Executive Institute. He holds a Masters of Business Administration, a Master of Science in Biotechnology, a Graduate Certificate in Technology Management, and a Bachelor of Science in Criminal Justice; all from the University of Maryland.



Homeland Security


Office of Cybersecurity and Communications

February 2016

U.S. Federal Cybersecurity Operations Team
National Roles and Responsibilities*

ASIRBP
March 5, 2015

DOJ/FBI	DHS	DoD
<ul style="list-style-type: none"> • Investigate, attribute, disrupt and prosecute cyber crimes • Lead domestic national security operations • Conduct domestic collection, analysis, and dissemination of cyber threat intelligence • Support the national protection, prevention, mitigation of, and recovery from cyber incidents • Coordinate cyber threat investigations 	<ul style="list-style-type: none"> • Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents • Disseminate domestic cyber threat and vulnerability analysis • Protect critical infrastructure • Secure federal civilian systems • Investigate cyber crimes under DHS’s jurisdiction 	<ul style="list-style-type: none"> • Defend the nation from attack • Gather foreign cyber threat intelligence and determine attribution • Secure national security and military systems • Support the national protection, prevention, mitigation of, and recovery from cyber incidents • Investigate cyber crimes under military jurisdiction



INTELLIGENCE COMMUNITY: Cyber Threat Intelligence & Attribution

SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS

PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER

Coordinate with Public, Private, and International Partners

* Note: Nothing in this chart alters existing DHS, and DoD roles, responsibilities, or authorities.
UNCLASSIFIED

DHS, Cybersecurity and Communications Responsibilities



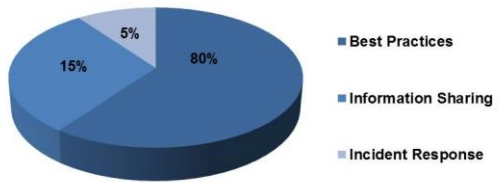
Cyber and Communications Ecosystem for the Future

Today	Future
<ul style="list-style-type: none"> Many unknown vulnerabilities Incidents spread at network speed and defenses are manual Many attacks are undetected Independently defended systems Inconsistent security policies Users do not follow best practices Attacks increasing in number and virulence 	<ul style="list-style-type: none"> Baked in security = fewer vulnerabilities Near real-time response with more automated defenses Many attacks, but less impact Information sharing and increasingly collaborative defenses Consistent security practices Unauthorized activity quickly identified Ability to learn and adapt defenses in near-real time

Emerging nexus between cyber and physical will continue to grow

Adversaries will continue to have robust and evolving capabilities

Cyber Risk Management



*Rule of thumb

SMB ANALYSIS

Review of Scalable and Affordable Solutions

- Across the Federal Government more tools are being created that SMBs can access for free. Even with these affordable and scalable resources, most SMBs continue to manage their enterprise-wide technologies without adequate cyber security solutions or technical support.
- A potential reason for this SMB apathy is a lack of understanding about their cyber risk exposure and negative business consequences that result from a major data breaches.
 - Reputational Loss
 - Loss of Proprietary Data
 - Loss of Intellectual Property
 - Identity Theft



Exercise and Planning

Ransomware

Holding computer network or data hostage. Ransomware is, in short, one of the easiest hacks to avoid.

DDOS

Distributed denial of service attacks have evolved from protest tool to criminal weapon.

Insider Threat

IT Policies that protect what matters, such as PII.

Training and Awareness

IT Professional awareness vs. Cyber Professional approach

Cyber Education

The Nation's One Stop Shop for Cybersecurity Careers and Studies!






National Initiative for Cybersecurity Careers and Studies (NICCS)

Resources for everyone – employees, employers, students, educators, parents, policy makers

- ✓ 5,000+ visitors per month
 - ✓ 1,500+ training courses mapped to the National Cybersecurity Workforce Framework
 - ✓ 100+ links to cybersecurity resources
 - ✓ 15+ tools for managers
 - ✓ 10+ monthly events
 - ✓ 10+ links to customized job searches
- ...and more coming soon!



www.niccs.us-cert.gov

<h3>Cybersecurity Tools</h3> <p>The C3 Voluntary Program is the coordination point within the Federal Government for members of the critical infrastructure community interested in improving their cyber resilience.</p> <p>The C3 Voluntary Program web-site offers an overview of the program, downloadable tools, and outreach materials, including an Outreach and Messaging Kit at the C3 Voluntary Program website at www.us-cert.gov/ccubedvp</p> <ul style="list-style-type: none"> • Over 30 unique offerings currently • The C3 Voluntary Program also features the Cyber Resiliency Review (CRR) tool that helps organizations support Framework adoption, evaluate cybersecurity capabilities and operational resilience. • Downloadable or direct assistance from DHS Established capability, 300+ assessments • Framework mapping, add'l guidance posted - Access at www.us-cert.gov/ccubedvp 	<h3>Information Sharing</h3> <ul style="list-style-type: none"> • The President tasked the Department of Homeland Security (DHS) to build and manage a new Information Sharing and Analysis Organization model (ISAO model), under Executive Order 13691 (ISAO E.O.). • A new ISAO model is the next step in the information sharing maturity process. <ul style="list-style-type: none"> – Enhance the Nations cyber defenses by adding a new layer of network defense, expands sharing relationships beyond traditional CIKR Sectors down into the fabric of America, and expands potential partnerships with private sector entities. – Build upon the foundation established by Executive Order 13636 – Improving Critical Infrastructure Cybersecurity. • The ISAO E.O. advances DHS' Cybersecurity and Communications (CS&C) efforts to assist private sector partners in building their cybersecurity capacity and resilience. 
<h3>Conclusion</h3> <ul style="list-style-type: none"> • The DHS approaches cybersecurity mitigation with an eye of cyber education, Government – Industry partnership and continuous requirements development. • Managing emerging cyber risk is going to require that organizations <ol style="list-style-type: none"> (1) work to understand “what matters,” (2) have better awareness of cyber-physical risk; and (3) create a culture of cybersecurity in their environments. • Municipalities will need to better secure their environments with the understanding cybersecurity is now a business function like physical security or accounting. <p>Successful Risk Management: <i>Consider the “worst circumstance” and put mitigations in place to assure your critical functions will survive them.</i></p> 	 

Questions posed to the first presenter:











- 1) What limits CICC relationships?
 - Nothing can stop you from building these relationships right now; in fact, you should do everything you can to build these relationships. Reach out to the NCCIC whenever you need.
- 2) At what level are the Information Sharing and Analysis Organizations (ISAOs) present?
 - The ISAO is present at all levels (County, Chamber of Commerce, businesses, etc.).
- 3) Where can we see information on best practices, ISAOs, past events, etc.?
 - www.us-cert.gov
- 4) Are there collaborative efforts between the Department of Homeland Security and the Department of Energy?
 - Energy Section Information Sharing and Analysis Center (ES-ISAC) has worked for the Department of Homeland Security and the Department of Energy for years. There is a very strong relationship between the two entities.
- 5) Does training offered online cover general cyber security information/best practices?
 - Yes. There is something available for everyone. The federal Virtual Training Environment (VTE) is a wonderful tool that should be utilized. Interested groups are encouraged to reach out and request trainings.

Presenter #2: Jermaine Roebuck, CISSP
Director, Cyber Joint Program Management Office
National Protection and Programs Directorate
U.S. Department of Homeland Security

Jermaine Roebuck has over 15 years of information technology experience in a wide variety of cybersecurity disciplines. Mr. Roebuck began his government service in 2013 as a lead incident responder for the Department of Homeland Security US-Computer Emergency Readiness Team (US-CERT). During his public service at US-CERT, Mr. Roebuck has responded to, and led the response effort for, several large-scale cyber breaches involving the U.S. Government and private sector entities.

Mr. Roebuck began his career as a contractor installing cable plant infrastructure for multiple government agencies in the National Capital Region to include being part of the restoration effort at the Pentagon soon after the attacks of September 11th, 2001. As his career developed, Mr. Roebuck became a network engineer responsible for supervising network engineers and maintaining routers, switches and firewalls for the DoD and the FBI. Recognizing the need to maintain the security of government networks, Mr. Roebuck transitioned his career into protecting and defending national networks in 2013.

Mr. Roebuck graduated from the University of Maryland, University College Magna Cum Laude with a Bachelor's Degree in Cyber Security.

 <p>Homeland Security</p> <p>UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT) INCIDENT RESPONSE TEAM (IRT)</p>	<h3>Disclaimer</h3> <p>This presentation is intended for informational and discussion purposes only.</p> <p>The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.</p> <p>The display of the DHS official seal or other DHS visual identities, including the US-CERT or ICS-CERT name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT and ICS-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, ICS-CERT or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.</p> <p>This presentation is Traffic Light Protocol (TLP): GREEN. Recipients may share TLP: GREEN  information with peers and partner organizations within their sector or community, but not via publicly accessible channels. For more information on the TLP, see http://www.us-cert.gov/tlp.</p> <p>DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.</p>  
<h3>Agenda</h3> <ul style="list-style-type: none"> • US-CERT Overview • Case Study • Incident Response (IR) • Mitigations • Questions  	  <p>The US-CERT, established in 2003, serves as a partnership between DHS and public/private sectors with the responsibility to:</p> <ul style="list-style-type: none"> • Improve computer security preparedness and response to cyber attacks • Protect the Nation's Cyber infrastructure • Coordinate defense against and responses to cyber attacks across the nation  

Case Study: OPM



OPM made aware of the breach through third-party reporting (US-CERT).

-February 2014

- Initial breach discovered in early 2014.
- Adversary was aware of the response.
 - Continued reconnaissance
 - New malware dropped
- Joint agency response to the incident.



US-CERT
United States Computer
Emergency Readiness Team

Case Study: OPM cont...



OPM announced that it had once again been the target of a massive data breach potentially affecting millions of Americans.

- June 2015

- Initial breach discovered in early 2014 and compromised information about OPM servers, but no PII.
- This recent breach compromised the PII of approximately 21.5M people, according to the agency.
 - 19.7M personnel that applied for security clearances
 - 1.8M family members
- OPM discovered the most recent intrusion on its own using tools that were recommended by US-CERT following the initial intrusion.



US-CERT
United States Computer
Emergency Readiness Team

Case Study: OPM cont...



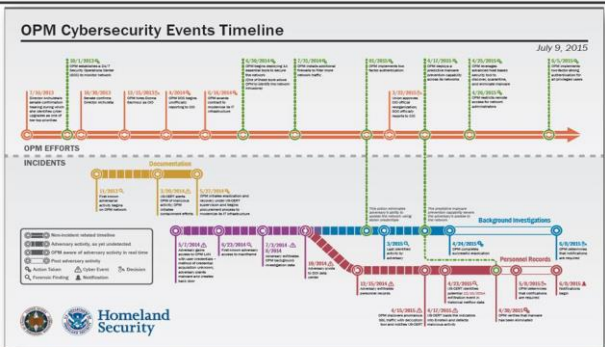
Based on guidance provided by US-CERT during mitigation of an earlier cybersecurity incident, the organization began implementing improved cybersecurity capabilities across its networks.

- US-CERT substantiated the compromise using EINSTEIN and assessed the potential damage. SMEs from US-CERT provided guidance in numerous specialized areas such as IBM mainframe and web applications.
- US-CERT was provided with digital media for analysis. Analysis of these artifacts contributed to the identification of the tools used for remote access and lateral movement by the advanced persistent threat (APT) actor.
- US-CERT developed indicators of compromise (IOCs) that were shared with other agencies and other organizations. IOCs were also used to develop signatures for EINSTEIN.



US-CERT
United States Computer
Emergency Readiness Team

Event Timeline



US-CERT
United States Computer
Emergency Readiness Team

IR Best Practices – Prior

- **Develop comprehensive incident response plan**
 - Types of incidents
 - Assign roles and responsibilities of the response team (and have backups)
 - Establish a communication decision tree
 - Procedures to follow
- **Exercise incident response procedures**
 - Table Top Exercises
 - Simulate incident response scenarios– practice collecting forensic data
 - Allows teams to be familiar with tools and be comfortable using them under high-pressure scenarios













US-CERT
United States Computer
Emergency Readiness Team







IR Best Practices – During

- **Incident Identification**
 - Fully scope the incident before making any mitigation efforts
 - Capture live forensic data and collect logs
 - Analyze data to understand lateral movement and persistence mechanisms
 - Determine business impact
 - Is the adversary still present?
 - Establish a single point of contact throughout the incident.



US-CERT
United States Computer
Emergency Readiness Team

<h3>IR Best Practices – <i>During (cont.)</i></h3> <ul style="list-style-type: none"> • Incident Containment <ul style="list-style-type: none"> • Closely monitor compromised systems • Possibly network isolate compromised systems • Limit scope and magnitude of intrusion • Gain visibility into the adversary’s foothold <ul style="list-style-type: none"> • Setup alerts for known malicious network infrastructure • Setup alerts for known compromised accounts • Setup alerts for known host-level TTPs • Create containment & eradication strategy 	<h3>IR Best Practices – <i>During (cont.)</i></h3> <ul style="list-style-type: none"> • Incident Eradication <ul style="list-style-type: none"> • Remove compromised machines • Alert/Block known malicious network infrastructure • Reset user account passwords • De-privilege user accounts • Reset service account passwords (difficult!) • Implement additional controls • All steps need to be executed in chorus 
<h3>IR Best Practices – <i>During (cont.)</i></h3> <ul style="list-style-type: none"> • Incident Recovery <ul style="list-style-type: none"> • Rebuild compromised hosts offline • Validate and restore data • Continue to monitor compromised systems and accounts 	<h3>IR Best Practices – <i>Post</i></h3> <p>After the Incident</p> <ul style="list-style-type: none"> • Conduct an after action assessment (lessons learned) • Identify what worked during the IR process and identify breakdowns or gaps • Create comprehensive post-incident report • Revise policies, procedures, IR plans, etc. • Create new signatures to detect this type of malicious activity • Identify areas to improve security posture • Submit incident and recommendations report to leadership 
<h3>Mitigations</h3> <div style="display: flex;"> <div style="flex: 1;">  <p>Two-Factor Authentication</p> <ul style="list-style-type: none"> • Can minimize attacker moving laterally through network </div> <div style="flex: 1;">  <p>Netflow / Full Packet Capture</p> <ul style="list-style-type: none"> • Critical for tracking attack movement • Finding other compromised hosts • Tells the story </div> <div style="flex: 1;">  <p>Server Discipline</p> <ul style="list-style-type: none"> • Not hardened or standardized • Unnecessary web access / programs / services running • Outdated OS • Sys admin or leadership reluctant/afraid to change “what’s currently working” </div> </div> 	<h3>Mitigations</h3> <div style="display: flex;"> <div style="flex: 1;">  <p>Basic Cyber Hygiene</p> <p>Basic cyber hygiene would address or mitigate a vast majority of the security breaches security practitioners deal with today.</p> <ul style="list-style-type: none"> • Minimizing Administrative Privileges • Application Directory White listing • Application Patching • System Patching • Proper Network Segmentation and Segregation </div> </div> 

<h3>Mitigations</h3>  <p>Keeping Workforce Educated</p> <ul style="list-style-type: none">Enhance existing cyber training programs to adapt and transform to evolving cyber environment<ul style="list-style-type: none">Build cybersecurity awareness and multiple competencies across skilled workforceStay abreast on the cyber threat and the employee's role in securityPrepare for the future<ul style="list-style-type: none">Participate / sponsor STEM engagements  <p>US-CERT United States Computer Emergency Readiness Team 17</p>	<h3>Mitigations</h3>  <p>General User Accounts are Targets</p> <p>We are seeing common vulnerabilities exploited and actors compromising general user accounts instead of admin accounts.</p> <ul style="list-style-type: none">Threat actors can conduct business on the network as an authorized userMost organizations, all users have access to some sensitive information (fileshares, databases, etc.)  <p>US-CERT United States Computer Emergency Readiness Team 18</p>
<h3>Questions?</h3> <p>Contact US-CERT: info@us-cert.gov 888-282-0870</p> <p>Subscribe to the National Cyber Awareness System: http://www.us-cert.gov/ncas</p> <p>Learn about US-CERT's mailing lists and feeds: http://www.us-cert.gov/ mailing-lists-and-feeds</p> <p>Follow US-CERT on Twitter: @uscert</p> <p>Report incidents, malware, phishing or vulnerabilities: https://www.us-cert.gov/report</p>  <p>US-CERT United States Computer Emergency Readiness Team 19</p>	 <p>Homeland Security</p>

Questions posed to the second presenter:



- 1) Can you speak to any lessons learned regarding the attack on the Ukrainian electric system?
 - The three entities that were targeted had never been in the same room prior to the attack even though they operated similar systems. Had they met before the attack, some of the security breaches that occurred could have been avoided.
- 2) How big is the CERT team?
 - There are roughly a couple hundred members (publications, analysis, digital analytics, indicator sharing, and incident response).

Presenter #3: Michael K. Hamilton
Chief Executive Officer (CEO)
Critical Informatics, Inc.

Michael Hamilton has 25 years of experience in information security as a practitioner, consultant, executive, and entrepreneur. He is currently the CEO of Critical Informatics Inc. Prior to his current role Mr. Hamilton served as a Policy Advisor for the State of Washington, Chief Information Security Officer (CISO) for the City of Seattle, and Managing Consultant for VeriSign Global Security Consulting.

Mr. Hamilton has provided his expertise to hundreds of organizations in nearly every sector; from Fortune 100 businesses to small private colleges. Mr. Hamilton is a subject-matter expert and former Vice-Chair for the U.S. DHS State, Local, Tribal and Territorial Government Coordinating Council. In Washington State, he founded the Public Regional Information Security Event Management (PRISEM) project; a regional monitoring shared service for the public sector. He now leads its successor PISCES, the Public Infrastructure Security Collaboration and Exchange System. His awards include Member of the Year from the Association of City and County Information Systems (ACCIS) and the Collaboration Award from the Center for Digital Government for the PRISEM project.

<p style="text-align: center;">CYBERSECURITY MEETS SLT GOVERNMENT</p>  <p style="text-align: center;">Michael Hamilton Critical Informatics Inc</p>	<p style="text-align: center;">AGENDA FOR THIS TALK</p> <ul style="list-style-type: none"> • The intersection of cybersecurity and emergency response: best practices and remaining issues • Lessons learned in managing cybersecurity for a major U.S. City • Regional monitoring as an option for the public sector
<p style="text-align: center;">GOVERNMENT IT SECURITY</p> <ul style="list-style-type: none"> • Government cuts across critical sectors • Federal – National Security Issue <ul style="list-style-type: none"> – NCCIC, ISACs, US-CERT • State – Economic Issue <ul style="list-style-type: none"> – Primary focus on Executive agency security • Local – Life-Safety issue <p style="text-align: center;"><i>We're all in it together, and need the equivalent of a NATO Article 5</i></p> 	<p style="text-align: center;">LOCAL GOVERNMENT</p> <ul style="list-style-type: none"> • 911: network, call centers and dispatch • Transportation management • Communication for Police/Fire/EMS • Water purification • Waste treatment • Energy delivery • Emergency management  

<h3>THE CISO IN LOCAL GOVERNMENT</h3> <ul style="list-style-type: none"> • Has no real authority, but responsibility and accountability • Budget: \$0; Staff: 1 • Federated system of agencies/departments with different business drivers • Few regulatory requirements, but lots of regulated data • Public disclosure complicates the job 	<h3>SOME FOCUS AREAS</h3> <ul style="list-style-type: none"> • Focus on monitoring: assume you're breached • Federated incident response – departmental ISOs • Use grants: UASI, SHSP, DHS S&T, Port Security • Procurement: RFP and contract language • Policies: local admin, de-minimus use • Training – leverage employee on boarding <p>...AND, nothing focuses the mind like a public hanging!</p> 
<h3>CYBER INCIDENT ANNEX</h3> <ul style="list-style-type: none"> • Two years to complete • Defines “significant” event • Role for the Fusion Center, regional monitoring for S/A • National Guard lead agency for Unified Coordination Group  	<h3>RESPONSE READINESS</h3> <ul style="list-style-type: none"> – Analysts and Forensic examiners – Access to information – Cross-sector • Law Enforcement Members <ul style="list-style-type: none"> – FBI – USSS – State and Local  
<h3>ISSUES TO ADDRESS</h3> <ul style="list-style-type: none"> • Resource typing – lack of which hinders mission-ready resources • Credentialing and PIV-I – who is a qualified responder? • Indemnification of response volunteers – can someone from Expedia have administrative access to your network? • Resource prioritization – who will we let melt, and what is the reasoning? 	<h3>MORE ISSUES TO ADDRESS</h3> <ul style="list-style-type: none"> • Regulatory impacts – continuity versus response • No forensic capabilities – evidence is likely to be destroyed • Coordination – cross-jurisdictional response hindered by proprietary communication tools • ESF2 – incorporates cyber – is that good enough? 

AND MORE...

- Emergency declaration – when do we activate the National Guard?
- Stafford Act applicability – what gets paid for through federal reimbursement?
- Active response – do we hit back, study the attack, or clean up and recover?

To sum up:
POLICY LAGS TECHNOLOGY (by a lot!)

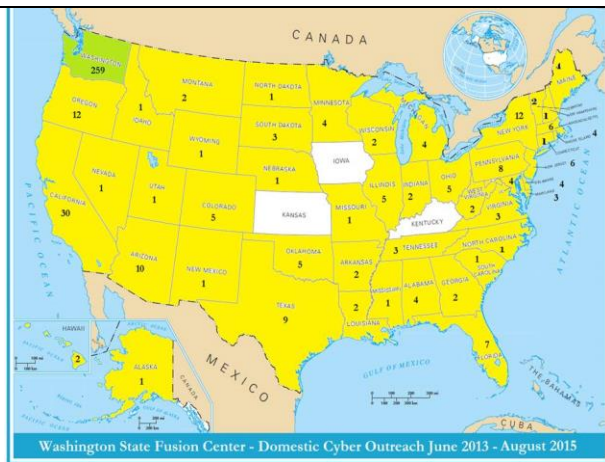


PRISEM REGIONAL MONITORING

Security Dashboard

At-a-glance situational awareness for the Puget Sound metro area and maritime ports

System capable of drilldown to individual event details



EDUCATION

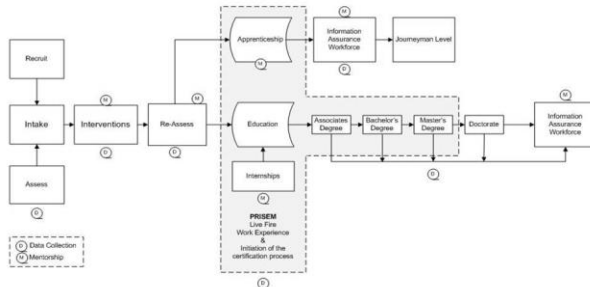
- Provost-level curriculum development
- Regional monitoring as a teaching tool
- UW-Tacoma focal point for returning Veteran training/transition
- USAR has selected UW-T for Army cyber training



Cybersecurity Rapid Education And Transition To Employment System

CREATES & PRISEM working together

Rapidly Producing High Quality IA Professionals - Building a Pipeline from the Military To The Information Assurance Workforce



PUTTING IT ALL TOGETHER

- Regional monitoring for infrastructure protection: local government, ports, others
- Veterans' training and transition using "live-fire" operational training to develop resources
- Coordination with state, local and federal law enforcement to reduce crime and disruption
- Research: real-time information sharing and distributed response



<p style="text-align: center;">IF THINGS WENT WELL...</p> <p style="text-align: center;">We have time for questions</p> <p style="text-align: center;">Michael.hamilton@criticalinformatics.com</p>	
--	--

Questions posed to the second presenter:

- 1) Regarding PRISEM’s Regional Monitoring (slide 12), what data are you getting and from where.
 - Information is gathered from all critical infrastructure sectors. Mr. Hamilton worked with the Department of Homeland Security to fund research programs to help transition them into commercial programs. Now, he works more with data analytics.
- 2) Because PRISEM is working with public utilities, how do you bypass NERC regulations?
 - In this case, the Electric Security Perimeter (ESP) does not apply.

Question and Answer Panel Discussion

- 1) Does the NCCIC have anything that interfaces with infrastructure down to the local level across various ISACS?
 - The NCCIC is currently working on merging infrastructure protection and cyber security. There is an ongoing initiative that is focusing on national coordination between tech/IT companies. The NCCIC looks across critical infrastructure and creates maps of the information gathered. This information can be of great use to local government, which is why local government leaders should foster relationships with the NCCIC.
- 2) What is an example of a temporary denial of service attack?
 - A temporary denial of service attack could occur in the form of 100 “fake” phone calls to 9-1-1 per minute. This draws resources away from where they are truly most needed and can have catastrophic effects.
- 3) Do you have any recommendations for list-serves?
 - Mike Echols will send an email upon request of the list-serves he subscribes to. Mike Hamilton curates his own daily news digest, which is available for subscription via his website - <http://www.criticalinformatics.com/news.htm>.
- 4) Is there any intent to process future data that is department-specific?
 - Yes. There is currently a push in this direction because there is a great desire for a common operating picture. This may take a while because there is so much data and it is not always clear how everything is related. This project will probably pick up momentum with the upcoming change of administration, because the next President will already be aware of the high importance that cyber security should be afforded.
- 5) Is the IP Gateway related to critical infrastructure information?
 - No. The information is stored at the IP Gateway but analyzed elsewhere.
- 6) What should the characteristics of the technical expert in the EOC be?
 - This person should know about emergency management, be familiar with critical infrastructure in the city/state, and should be able to “speak government/layman’s terms.”
- 7) What threats should we anticipate moving forward?
 - We can and should expect that the presence of cyber-attacks will not only continue, but rise. Cyber-attacks will continue to be used as a means of unconventional warfare. Oftentimes breaches start within infrastructure (i.e., HR) and then move through the system in search of sensitive information.
- 8) Were there multiple actors involved in the Office of Personnel Management (OPM) hack?
 - While this is not totally clear, it seems as if there were. The second actor seems to have piggy-backed off of the first actor’s hack. The evidence suggests that this was an organized campaign facilitated by multiple actors.
- 9) Elaborate on the topic of machine learning versus artificial intelligence (AI) as it relates to cyber security.
 - Cyber security will never be a self-serving machine. While AI will certainly be a part of our lives in the future, data analytics will be more relevant to the maintenance of cyber

security. There are aspects of cyber security maintenance that must be carried out by an actual person that a machine could never learn to process.

10) Regarding the organization “CIRCAS,” how are actors like Amazon allowed into the process?

- The Pacific Northwest is extremely collaborative; there are a large number of public/private sector relationships across the board. Mike Hamilton will inquire as to whether he is allowed to share the Washington State Significant Incident Annex with the team.

This page is intentionally blank.

APPENDIX E: ACRONYMS

Acronym	Term
AAR	After-Action Report
BOC	Business or Bureau Operations Center
BOS	Bureau of Sanitation
CAD	Computer Aided Dispatch
CICC	Cyber Intrusion Command Center
CIRT	Cyber Incident Response Team
CISO	City/Chief Information Security Officer
ConOps	Concept of Operations
COOP	Continuity of Operations
DHS	Department of Homeland Security
DOC	Department Operations Center
DOT	Department of Transportation
DWP	Department of Water and Power
EI	Essential Elements of Information
EMD	Emergency Management Department
EndEx	End of Exercise
EOC	Emergency Operations Center
EPT	Exercise Planning Team
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FMS	Financial Management System
GIS	Geographic Information Systems
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Incident Command System
IP	Improvement Plan
IR	Incident Response
ISAC	Information Sharing and Analysis Center
ISIM	Information Security Incident Manager
ISOC	Integrated Security Operations Center
ITA	Information Technology Agency
JRIC	Joint Regional Intelligence Center
LAFD	Los Angeles Fire Department
LAPD	Los Angeles Police Department
LAWA	Los Angeles World Airports
MAC	Multi-Agency Coordination
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
NGO	Non-Governmental Organization
NIST	National Institutes for Standards and Technology
PIO	Public Information Officer
POLA	Port of Los Angeles
RACR	Real-Time Analysis and Critical Response
SEMS	Standardized Emergency Management System
SitMan	Situation Manual
StartEx	Start of Exercise

Acronym	Term
TTX	Tabletop Exercise
USSS	United States Secret Service
VOIP	Voice-Over-Internet-Protocol

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: July 12, 2016

To: Charlie Beck, Chair
Emergency Operations Board

Emergency Operations Board Members

From: Anna Burton, Executive Assistant
Emergency Operations Board

A handwritten signature in black ink, appearing to read 'Anna Burton', written over the printed name in the 'From' field.

Subject: **UCLA BOELTER HALL ACTIVE SHOOTER EMERGENCY
OPERATIONS CENTER ACTIVATION AFTER ACTION
REPORT/CORRECTIVE ACTION PLAN**

Recommendation

That the Emergency Operations Board, as recommended by the Emergency Management Committee (EMC), approve the attached UCLA Boelter Hall Active Shooter Emergency Operations Center (EOC) Activation After Action Report/Corrective Action Plan (AAR/CAP) and forward to the Mayor for transmittal to the City Council.

Summary

The EOC was activated June 1, 2016, to provide effective citywide coordination of information and to support the Los Angeles Police Department (LAPD) and the Los Angeles Fire Department (LAFD) response to the UCLA Boelter Hall Active Shooter incident.

EMD consulted with the LAPD, the LAFD and the Office of the Mayor to determine that at a minimum, this event warranted an EOC Level I activation. The EOC was activated to provide support to field response agencies and to ensure effective Citywide coordination of resources and information.

The attached AAR/CAP provides a summary of the activation, identifies involved departments and agencies, and details the recommendations for future activations of the EOC. This report was approved by the EMC at its July 6, 2016, meeting. With approval by the EOB, EMD will forward to the Mayor for approval and transmittal to the City Council.

EMD will track areas recommended for improvement and, as appropriate, report back through the Emergency Operations Organization.

Attachment

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: June 28, 2016

To: Anna Burton, Chair
Emergency Management Committee
Emergency Management Committee Members

From: Carol Parks, Special Projects Division Chief
Emergency Management Department

Subject: **UCLA BOELTER HALL ACTIVE SHOOTER EMERGENCY
OPERATIONS CENTER ACTIVATION AFTER ACTION
REPORT/CORRECTIVE ACTION PLAN**

Recommendation

That the Emergency Management Committee (EMC) approve the attached UCLA Boelter Hall Active Shooter Emergency Operations Center (EOC) Activation After Action Report/Corrective Action Plan (AAR/CAP) and forward to the Emergency Operations Board (EOB) for approval.

Summary

The EOC was activated June 1, 2016, to provide effective citywide coordination of information and to support the Los Angeles Police Department (LAPD) and the Los Angeles Fire Department (LAFD) response to the UCLA Boelter Hall Active Shooter incident.

EMD consulted with the LAPD, the LAFD and the Office of the Mayor to determine that at a minimum, this event warranted an EOC Level I activation. The EOC was activated to provide support to field response agencies and to ensure effective Citywide coordination of resources and information.

The attached AAR/CAP provides a summary of the activation, identifies involved departments and agencies, and details the recommendations for future activations of the EOC.

Attachment



After Action Report/Corrective Action Plan
2016 UCLA BOELTER HALL ACTIVE SHOOTER
EOC Activation

June 28, 2016



TABLE OF CONTENTS

I.	Executive Summary	2
A.	Statement of Purpose.....	2
B.	Event Name	2
C.	Event Date	2
D.	Event Location	2
E.	EOC Activation Duration	2
F.	EOC Activation Lead Agency	2
G.	EOC Activation Level	2
H.	EOC Activation Participating Agency	2
I.	EOC Activation Chronology.....	3
II.	Synopsis.....	4
A.	Major Developments	4
B.	Core Capabilities	5
C.	EOC Objectives.....	5
III.	Findings	5
A.	Practices to Sustain.....	5
B.	Area Requiring Improvement	6
IV.	Conclusion	7
V.	Improvement Plan Matrix.....	7

I. Executive Summary

A. Statement of Purpose

The Emergency Management Department (EMD) is responsible for preparing a formal After Action Report/Corrective Action Plan (AAR/CAP) following all activations of the City's Emergency Operations Center (EOC). AAR/CAPs are intended to assist the City of Los Angeles analyze its EOC activation, staffing and management processes in order to document the following:

- Procedures and protocols to sustain and build upon,
- EOC operational elements and processes to improve, and
- Improvement plan with recommended corrective actions, responsibilities and timelines.

The AAR/CAP should be viewed as providing suggestions for improving the effectiveness of future EOC activations. Recommended corrective actions identify steps to be taken and assign specific City agencies with responsibility for their coordination and implementation. Timetables are also established for implementation and are considered against the benefits in determining resource allocation. In some cases, agencies may determine the benefits of implementation are insufficient to outweigh the costs. In other cases, agencies may identify alternative solutions that are more effective. Each agency should review the recommendations and determine the most appropriate action and time needed for implementation.

B. Event Name

UCLA Boelter Hall Active Shooter

C. Event Date

Wednesday, June 1, 2016

D. Event Location

580 Portola Plaza, Los Angeles, CA 90095

E. EOC Activation Duration

1100 – 1430 hours

F. EOC Activation Lead Agency

EMD

G. EOC Activation Level

Level I (EMD Lead)

H. EOC Activation Participating Agency

EMD

I. EOC Activation Chronology

The EOC was activated to monitor the situation, gather information and intelligence from appropriate resources, and to support the Unified Command Post operations. Based on discussions with the Los Angeles Police Department (LAPD), the Los Angeles Fire Department (LAFD) and the Office of the Mayor, it was determined that the EOC should be activated at Level I. In making this decision, the following factors were considered:

- An active threat was reported at UCLA
- UCLA's emergency notification system pushed out a lock-down/shelter-in-place message
- LAPD activated its Department Operations Center
- LAPD declared a city-wide tactical alert

The activation of the EOC occurred at 1100 hours on June 1, 2016. The EOC was activated at Level I. The EOC was deactivated for this event at 1430 hours on June 1, 2016. Staffing for this activation included the EMD Duty Officer and Duty Team. EMD's Duty Team staffed the following EOC positions:

- EOC Director
- Planning and Intelligence Section Coordinator
- Situation Status Unit Leader
- Public Information Officer

Initial Briefing and Coordination Meetings

The Duty Officer briefed the EOC responders on the EOC Coordination Plan and the anticipated schedule of events.

Planning Meetings

The Planning and Intelligence Section Coordinator provided an updated situation report and implemented the pre-established, advanced event EOC management and coordination objectives that were approved by the EOC Director (See Section C – Objectives on page 5).

Coordination Meetings

The Planning and Intelligence Section Coordinator provided an updated situation report and confirmed status of the established objectives. The EOC coordinated with the LAPD DOC to monitor intelligence.

Final Coordination and EOC Demobilization Meeting

The Planning and Intelligence Section Coordinator provided a final update on event status. No specific requests were directed to the EOC by the UCP.

No significant incidents or unusual occurrences were reported. Final EOC 909 report was approved and released on June 1, 2016, at 1430 with demobilization of the EOC at 1445 hours.

II. Synopsis

The EOC was activated on Wednesday, June 1, 2016, at 1100 hours and was deactivated at 1430 hours, to provide effective citywide coordination of information and to support the LAPD and LAFD response to the UCLA Boelter Hall Active Shooter.

EMD consulted with the LAPD, the LAFD and the Office of the Mayor to determine that at a minimum, this event would warrant an EOC Level I activation.

The EOC was activated to gain and maintain situational awareness, to provide support to field response agencies and to ensure effective Citywide coordination and response in the active shooter incident occurring on the campus of UCLA. The shooting incident occurred at approximately 1000 hours when classes were in session and at a time of day when the campus was actively in use by students, faculty, staff and visitors. The details and extent of this incident were not initially known, which prompted the LAPD to issue a citywide tactical alert.

This Level I activation was staffed by EMD personnel. Level I activation level requires (at minimum) staffing of the EOC Director, Planning and Intelligence Section Coordinator, Situations Status Unit Leader, and Public Information Officer positions. EMD personnel maintained regular communications with LAPD's DOC.

The EOC monitored the news and social media sites for any increase of incident related activities. The monitoring actions included watching the various local and national news channels as well as obtaining reports from LAPD's DOC. The EOC was not tasked to provide any significant resources or services.

A. Major Developments

The EOC Director and Planning and Intelligence Section Coordinator provided overall leadership of the EOC organization and the process of management by objectives. EMD developed advanced EOC coordination objectives as described in Section II above. These objectives were consistent with and supported field level advanced event plan objectives developed by the Unified Command.

The Planning & Intelligence Section collected, analyzed and disseminated information from field, DOC, EOC and media and social media sources. The Section maintained situational awareness, coordinating the assembling of section situation reports, setting meeting agendas and facilitating all meetings conducted in the EOC Management Room.

During the EOC activation, the Planning and Intelligence Section focused specifically on the safety of the UCLA Students, the safety of the first responders, the City's traffic situation, and monitoring the overall City footprint for any threats, disruptions, or impacts to City services.

EOC deactivation occurred and the EOC transitioned its operations to the EMD Duty Officer.

B. Core Capabilities

This event provided an opportunity to assess the following EOC core capabilities:

- Intelligence and Information Gathering and Sharing
- Recognition of Indicators and Warnings
- EOC Management and Coordination Planning Processes including development of advanced event EOC coordination objectives
- Staffing a Liaison Officer position at the UCP

C. EOC Objectives

The EOC developed the following advanced event plan objectives based on the Unified Command's Advanced Event Plan.

Management Objectives

- Ensure information sharing is established and maintained between the EOC, any activated DOCs and the Los Angeles County EOC.
- Provide support to the UCP in the event citywide emergency services are required.
- Gather information and intelligence from appropriate resources.
- Monitor the event and be ready to advise City leadership if the EOC activation level needs to be increased.

Coordination Objectives

- Maintain situational awareness regarding the active threat and any impacts to the City.
- Monitor media reports and coordinate public information related to the active threat.
- Facilitate policy direction as needed.
- Coordinate/share information with the UCP, activated DOCs and other applicable jurisdiction EOCs.
- Provide resource support to the UCP, if requested.
- Keep City executives and elected officials informed of any significant event related incidents.

III. Findings

A. Practices to Sustain

The following EOC practices were reported as effective by responders and are recommended to be sustained:

1. Level I EOC Activation Policies and Procedures

EMD has developed a set of policies and procedures for EOC Level I activations. During Level I activations, the EOC is staffed by an EMD Duty Officer and Duty Team members. A system of primary and back-up Duty Officers and Duty Teams ensures sufficient depth of coverage for key positions such as EOC Director, Planning and Intelligence Section Coordinator and Situation Status Unit Leader as well as support positions such as Documentation Unit Leader,

Management Staff Support and Public Information Officer. Typical Level I staffing requires that these six (6) positions are filled.

This model relies on liaison with representatives from other operating departments and effective communication with activated DOCs for situational awareness and resource coordination. Should the event or incident escalate, the activation level can be increased to II or III which requires staffing of various positions by other departments. Most of the recent EOC activations have been at Level I using this model which has proven to be efficient and cost effective. It is recommended that these policies and procedures be sustained.

2. Advanced Event EOC Coordination Planning Process

EMD plays an active role in advanced event planning with LAPD, LAFD, DOT and other field response agencies. An EMD planning liaison is assigned to work with advanced event planning teams to ensure that inter-agency coordination issues are managed proactively from a Citywide perspective. Their role includes recommending appropriate EOC activation levels, assignment of an EMD Liaison Officer to UCPs or Incident Command Posts, and development of an advanced event EOC Coordination Plan that is based on objectives of the field level Advanced Event Plan.

3. EMD Staffing of UCP Liaison Officer Position

EMD has a standing practice of staffing the UCP Liaison Officer position for major planned events. This position ensures effective interagency coordination and cooperation, especially between the established Unified Command agencies and City support agencies such as the Department of General Services, the DOT, etc. This practice is especially valuable for Level I EOC activations where the Liaison Officer also provides the EOC with regular informational briefings to ensure good situational awareness and a “common operating picture” with the Unified Command staff.

B. Area Requiring Improvement

The following area was reported as requiring improvement.

Further Development of the EOC 909 Situation Report Process

A key component of the established, successful Level I EOC Activation Process and Procedures has been the enhancements to the MCR Management Room and use of the EOC 909 form for standardized Situation Status Reporting. The Management Room is currently equipped with a manual that can assist EMD staff during the EOC activation. While this process has become standard for Level I events, it is recommended that the EMD EOC Task Force continue to refine and further develop this process for information gathering and reporting and refining the recipient list to ensure all appropriate department representatives are informed and updated.

The EOC 909 was provided electronically to key City agencies and decision makers. EMD should evaluate expanding the scope of distribution as well as exploring the use of WebEOC for a Level 1 activation and areas for overall improvement.

IV. Conclusion

EMD continues to improve on the staff efficient and cost effective set of processes and procedures for Level I activations of the City’s EOC. The improvement over past practices will proceed with Level I staffing of EOC activations with trained emergency managers from EMD. These staff provide core EOC position capabilities and maintain situational awareness and coordinate available resources by communicating with personnel from other response and support agencies at the DOC and UCP/ICP level.

EMD staffs the physical EOC; other departments are brought to bear in a “virtual” EOC environment through effective communication and use of technology. Physical staffing of EOC positions by these agencies is generally required for Level II and III activations.

V. UCLA Boelter Hall Active Shooter EOC Activation Corrective Action Plan (Improvement Plan Matrix)

The following matrix identifies specific recommended corrective action.

Required Improvement	Corrective Action	Lead Agency	Timeframe	Resources Required
Continue enhancement of the EOC 909 Situation Reporting Process	Continue to refine and further develop this process to ensure effective information flow, management and distribution.	EMD	On-going	EMD staff resources, EOC Task Force, and public safety department representatives, as needed