

TRANSMITTAL

TO
The Council

DATE

09/01/16

COUNCIL FILE NO.

FROM
The Mayor

COUNCIL DISTRICT

ALL

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.


Eric Garcetti
Mayor

(Ana Guerrero)

CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE



Date: August 16, 2016

To: Eric Garcetti, Mayor

From: Anna Burton, Executive Assistant
Emergency Operations Board

A handwritten signature in black ink, appearing to read "Anna Burton".

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

At its July 19, 2016, meeting, the Emergency Operations Board approved the attached City of Los Angeles 2016 Cyber Security Table Top Exercise After Action Report/Improvement Plan (AAR/IP) and recommended it be forwarded to the Mayor for approval and forwarding to the City Council.

Executive 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.

With your approval this report should be forwarded to the City Council with the attached transmittal for its information and file.

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

cc: Jeff Gorell, Deputy Mayor, Mayor's Office of Public Safety

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

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	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. 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. 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

	and answer panel discussion open to all participants. A summary of those presentations and discussions is included in Appendix D.
Mission Area	Prevention and Response
Core Capabilities	• Cyber Security • Intelligence and Information Sharing • Interdiction and Disruption • Operational Coordination • Planning
Objectives	• 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).
Threat or Hazard	Cyber-Terrorism Attack
Scenarios	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)

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

City of Los Angeles:

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

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

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		
Ratings Definitions: 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.					

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, reimage 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	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	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 ⁱ	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)
Kaurloto	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	• 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	• 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	• 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%)

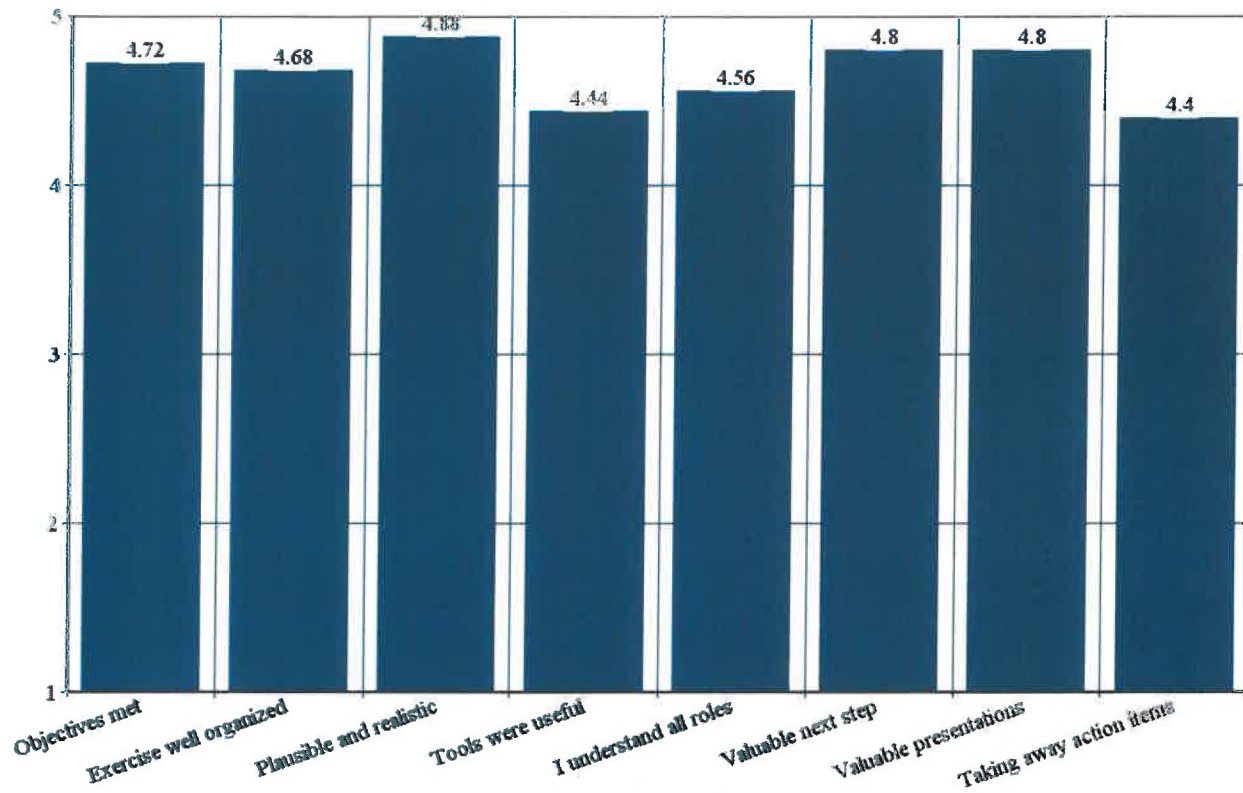
- Emergency plans need to be modified to include cyber elements. (8%)
- Computers are too easily accessible in the city. Login to systems should be done by biometrics or credentials.
- The Information Technology Agency should provide more support for the EOC, more cyber expertise, and have more of a 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 CIRTs 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*

DOJ/FBI	DHS	DoD
- 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 investigation	- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents - Operate domestic cyber threat and vulnerability analysis - Protect critical infrastructure - Secure federal (effort system) - Investigate cyber crimes under DHS jurisdiction	- Defend the nation from attack - Surveil 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

DOJ/FBI LEAD FOR Investigation and Attribution
DHS LEAD FOR Protection, Prevention, Mitigation, and Recovery
DoD LEAD FOR National Defense

INTELLIGENCE COMMUNITY: Cyber Threat Intelligence & Attribution

SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS

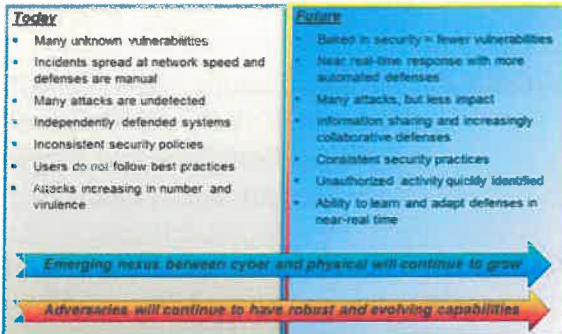
PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER

Coordinate with Public, Private, and International Partners

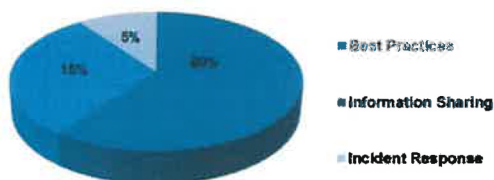
DHS, Cybersecurity and Communications Responsibilities



Cyber and Communications Ecosystem for the Future



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
- ✓ 1,800+ 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

Cybersecurity Tools 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. 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 • 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  Office of Cybersecurity and Communications	Information Sharing • 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. – 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 13536 – 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. 
Conclusion • 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 (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. Successful Risk Management: <i>Consider the "worst circumstance" and put mitigations in place to assure your critical functions will survive them.</i>  Office of Cybersecurity and Communications	  Office of Cybersecurity and Communications

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.

 UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT) INCIDENT RESPONSE TEAM (IRT)	Disclaimer This presentation is intended for informational and discussion purposes only. 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. 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. 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. 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. 
Agenda • US-CERT Overview • Case Study • Incident Response (IR) • Mitigations • Questions 	 US-CERT RESPOND TO MAJOR INCIDENTS, ANALYZE THREATS, EXCHANGE CRITICAL CYBERSECURITY INFORMATION WITH PARTNERS AROUND THE WORLD. The US-CERT, established in 2003, serves as a partnership between DHS and public/private sectors with the responsibility to: • 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.



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.



Case Study: OPM cont....

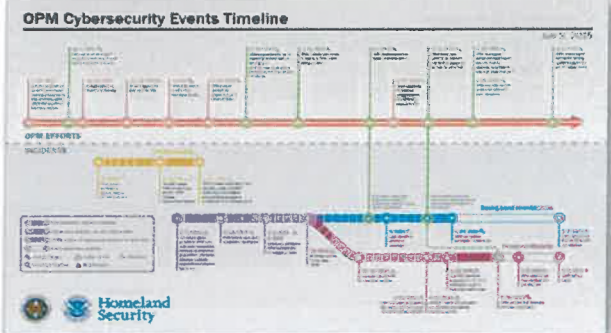


Based on guidance provided by US-CERT during mitigation of an earlier cybersecurity incident, the organization began implementing improved cybersecurity capabilities across its networks.

- 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.



Event Timeline



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



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.



IR Best Practices – During (cont.)

- **Incident Containment**
 - Closely monitor compromised systems
 - Possibly network isolate compromised systems
 - Limit scope and magnitude of intrusion
 - Gain visibility into the adversary's foothold
 - Setup alerts for known malicious network infrastructure
 - Setup alerts for known compromised accounts
 - Setup alerts for known host-level TTPs
 - Create containment & eradication strategy



US-CERT
Cyber Security Operations Center
Department of Homeland Security

IR Best Practices – During (cont.)

- **Incident Eradication**
 - 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



US-CERT
Cyber Security Operations Center
Department of Homeland Security

IR Best Practices – During (cont.)

- **Incident Recovery**
 - Rebuild compromised hosts offline
 - Validate and restore data
 - Continue to monitor compromised systems and accounts



US-CERT
Cyber Security Operations Center
Department of Homeland Security

IR Best Practices – Post

- After the Incident**
- 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



US-CERT
Cyber Security Operations Center
Department of Homeland Security

Mitigations



- Two-Factor Authentication**
- Can minimize attacker moving laterally through network
- Netflow / Full Packet Capture**
- Critical for tracking attack movement
 - Finding other compromised hosts
 - Tells the story
- Server Discipline**
- Not hardened or standardized
 - Unnecessary web access / programs / services running
 - Outdated OS
 - Sys admin or leadership reluctant/afraid to change "what's currently working"



US-CERT
Cyber Security Operations Center
Department of Homeland Security

Mitigations



- Basic Cyber Hygiene**
- Basic cyber hygiene would address or mitigate a vast majority of the security breaches security practitioners deal with today.
- Minimizing Administrative Privileges
 - Application Directory White listing
 - Application Patching
 - System Patching
 - Proper Network Segmentation and Segregation



US-CERT
Cyber Security Operations Center
Department of Homeland Security

Mitigations Keeping Workforce Educated - Enhance existing cyber training programs to adapt and transform to evolving cyber environment - Build cybersecurity awareness and multiple competencies across skilled workforce - Stay abreast on the cyber threat and the employee's role in security - Prepare for the future - Participate / sponsor STEM engagements	Mitigations General User Accounts are Targets We are seeing common vulnerabilities exploited and actors compromising general user accounts instead of admin accounts. - Threat actors can conduct business on the network as an authorized user - Most organizations, all users have access to some sensitive information (files, shares, databases, etc.)
Questions? Contact US-CERT: info@us-cert.gov 888-282-0870 Subscribe to the National Cyber Awareness System: https://www.us-cert.gov/ncas Learn about US-CERT's mailing lists and feeds: https://www.us-cert.gov/ncas/subscribe Follow US-CERT on Twitter: @uscertgov Report incidents, malware, phishing or vulnerabilities: https://www.us-cert.gov/ncas/alerts	Homeland Security

Questions posed to the second presenter:

- 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.
- 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.

CYBERSECURITY MEETS SLT GOVERNMENT  Michael Hamilton Critical Informatics Inc	AGENDA FOR THIS TALK • 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
GOVERNMENT IT SECURITY • Government cuts across critical sectors • Federal – National Security Issue – NCCIC, ISACs, US-CERT • State – Economic Issue – Primary focus on Executive agency security • Local – Life-Safety issue <i>We're all in it together, and need the equivalent of a NATO Article 5</i> 	LOCAL GOVERNMENT • 911: network, call centers and dispatch • Transportation management • Communication for Police/Fire/EMS • Water purification • Waste treatment • Energy delivery • Emergency management  

THE CISO IN LOCAL GOVERNMENT

- 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



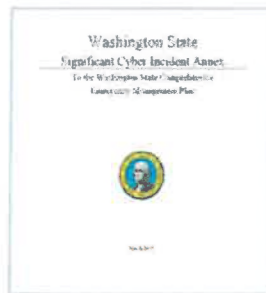
SOME FOCUS AREAS

- 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
- ...AND, nothing focuses the mind like a public hanging!



CYBER INCIDENT ANNEX

- 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



RESPONSE READINESS



- Analysts and Forensic examiners
- Access to information
- Cross-sector



• Law Enforcement Members

- FBI
- USSS
- State and Local



ISSUES TO ADDRESS

- **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?



MORE ISSUES TO ADDRESS

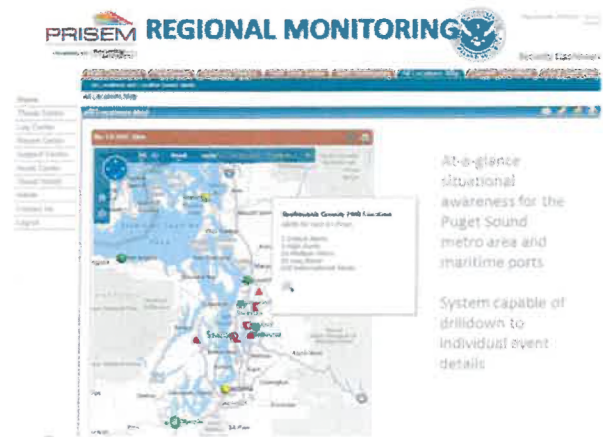
- **Regulatory impacts** – continuity versus response
- **No forensic capabilities** – evidence is likely to be destroyed
- **Coordination** – cross-jurisdictional response hindered by proprietary communication tools
- **ESF2** – incorporates cyber – is that good enough?



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!)



EDUCATION

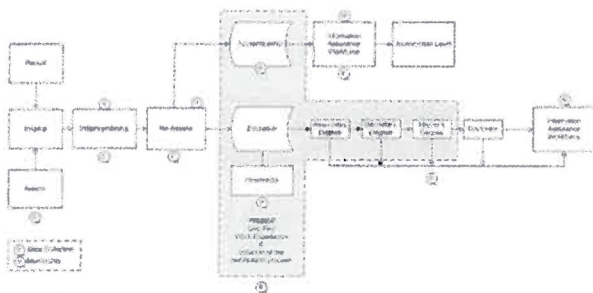
- Provost-level curriculum development
- Regional monitoring as a teaching tool
- UW-Tacoma focal point for returning Veteran training/transition
- USAR has selected UW-T for Army cyber training



Cybersecurity Rapid Education And Transition To Employment System

CREATES 2 PRISM 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



IF THINGS WENT WELL... We have time for questions Michael.hamilton@criticalinformatics.com	
--	--

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
EEI	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