ERIC GARCETTI
MAYOR

EXECUTIVE DIRECTIVE NO. 2

Issue Date: October 30, 2013

Subject: Cybersecurity

Introduction

The health, safety, and welfare of the residents of the City of Los Angeles are paramount among the responsibilities of city government. Increasingly, we rely on local and global computer networks to maintain services for our community. The City's electronic infrastructure is vital to the proper functioning of the City and the ability of the City departments and personnel to serve the residents of Los Angeles. The City must be able to defend against, and quickly recover from, any disturbance, whether it is a natural or human-caused disaster, and whether it be an accidental or intentional incident.

One aspect of the City's strategy for reducing the opportunity for attack is to make our systems more resistant to penetration. Pursuant to this Executive Directive, department heads, including all Board and Commission members, General Managers, Directors and Administrators of departments, offices, bureaus, and agencies shall implement the following instructions. Business partners, contractors, vendors, and consultants shall also be bound by this Directive while conducting business with the City.

Collaboration will be the key to the City's successful strategy. A new level of collaboration is necessary among City departments, between every department and the Information Technology Agency ("ITA"), and between the City and other levels of government. Together we become stronger, and can become more resilient to address this emerging threat.

Background on Cybersecurity Developments

In his February 12, 2013 Executive Order,[1] President Obama declared the cyber threat as one of the most serious economic and national security challenges we face as a nation. America's economic prosperity in the 21st century will depend on cybersecurity. Foreign governments, criminal syndicates, and lone individuals are probing our financial, energy, and public safety systems every day. The President further stated that through an environment of collaboration and partnership we can create a cyber environment that promotes safety and security, while promoting business, innovation, and efficiency.

In March and April of 2013, James Clapper, the Director of National Intelligence, testified before Congress[2] noting that:

1) It is difficult to overemphasize the significance of cyber threats.

2) Increasingly, state and non-state actors are using cyber techniques and capabilities to achieve strategic objectives by gathering sensitive information from public and private-sector entities.

3) Some terrorist organizations are interested in developing offensive cyber capabilities.

4) Some digital technologies are being applied faster than our ability to understand the security implications and mitigate potential risks.

5) Foreign intelligence and security services have penetrated numerous computer networks of the United States Government, business, academic, and private sector entities.

6) Highly networked information technology provides opportunities for foreign intelligence and security services, trusted insiders, hackers, and others to target and collect sensitive United States national security and economic data.

In October 2012, then Secretary of Defense Leon Panetta made the following observations:[3]

---

[1] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (Copy of the President's Executive Order).
[2] http://www.intelligence.senate.gov/130312/clapper.pdf; http://www.dni.gov/index.php/newsroom/testimonies/194-congressional-testimonies-2013/817-remarks-as-delivered-by-dni-james-r-clapper-on-the-2013-worldwide-assessment
[3] http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136

1) The Internet is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens.

2) A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attacks on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.

3) Foreign cyber actors are probing America's critical infrastructure networks; targeting the computer control systems that operate chemical, electricity, and water plants and those that guide transportation throughout this country. Intruders have successfully gained access to these control systems, seeking to create advanced tools to attack and cause panic and destruction, and even the loss of life.

Cybersecurity Collaboration

All City departments, including all proprietary departments, shall participate in a collaborative effort known as the Cyber Intrusion Command Center, which shall consist of all City departments, led by the Office of the Mayor, and shall incorporate assistance from the Federal Bureau of Investigation ("FBI"), the United States Secret Service, and any other federal or state agency that will join in this collaborative effort. The City of Los Angeles is very appreciative of the FBI and Secret Service for their demonstrated commitment to this collaborative project, and for offering assistance to the City in this effort. The cybersecurity goals of this group are to:

- Facilitate the identification and investigation of cyber threats and intrusions against City assets;
- Ensure incidents are quickly, properly, and thoroughly investigated by the appropriate law enforcement agency;
- Facilitate dissemination of cybersecurity alerts and information;
- Provide uniform governance structure accountable to City leadership;
- Coordinate incident response and remediation across the City;
- Serve as an advisory body to City departments;
- Sponsor independent security assessments to reduce security risks; and
- Ensure awareness of best practices.

All departments must contribute personnel, resources, and data to the Cyber Intrusion Command Center in order for it to succeed. The nature and extent of each department's involvement will depend on the nature and extent of their cyber assets, with those deemed to have the most critical assets being more heavily involved in this collaborative effort. It is not acceptable for any City department to withhold information from the Cyber Intrusion Command Center regarding cybersecurity issues. In addition, every department will:

- Establish and maintain permanent liaisons with the Cyber Intrusion Command Center;
- Report information about significant cyber-related events occurring in its department;
- Identify personnel who require notification about distributed threat information;
- Provide resources for cooperative actions as situations may require.

Appropriate members of the Cyber Intrusion Command Center will report to the Mayor and Council, as directed by those offices, regarding the issues being addressed by the group. The existence of this collaborative effort does not eliminate the need for departments to perform their required reporting to federal or state agencies, as required by law and/or regulation. Further, this order is not intended to supersede, replace, or interfere with the applicability of all relevant federal, state, and local laws relating to privacy and the confidentiality of personal information.

Within 10 days of the date of this Executive Directive, the Office of the Mayor will organize a working group of key City departments that will propose a more detailed organizational structure for the Cyber Intrusion Command Center. The working group will present the proposed structure to the Office of the Mayor for approval within 30 days of this directive.

City Department Responsibilities

In addition to participating in the Cyber Intrusion Command Center, each department must enhance its own cybersecurity. Each department in the City of Los Angeles plays a unique role in securing its departmental information, personal data of its users, and residential information. Each department is responsible for the City network usage by its employees and contractors. All City departments should review and comply with the related citywide policies established by the ITA and the Information Technology Policy Committee (ITPC). The policies may be found on the City intranet at: http://ita.ci.la.ca.us/ITManagers/ITPC/CitywideITPolicies?index.html. Departments are responsible for keeping up-to-date with all City cybersecurity policies. Furthermore, departments are encouraged to present their recommendations for new cyber policies to the General Manager of ITA, to the ITPC, and to the Cyber Intrusion Command Center.

All departments must adhere to the following minimum standards:

Prevent Unauthorized Access: Limiting data and network access to authorized individuals is a primary means for securing the City's information technology assets. This includes:

- Physical, wireless, and virtual access to City workstations, systems, networks, and e-mail must be limited to authorized City employees or contractors.
- Departments must deactivate all passwords and network access for employees who have left City service. Departments must deactivate all access for employees who have not accessed their network within 60 days, unless on a pre-approved medical leave or other authorized leave approved by the General Manager.
- Implement physical security measures for City computers, servers, and network ports to physically separate them from unauthorized users. This could include moving them behind locked doors and into restricted areas. Computers dedicated for public usage should include security restrictions to ensure they are logically separated from City networks and data.
- Responsible Wi-Fi Network Access: City departments choosing to use Wi-Fi services must abide by the ITA Wireless Network Access Policy.

Promote and Enforce Password Security: All systems, networks, e-mail, and screensavers must be password protected. This includes all departmental applications and network drives that contain sensitive, personal, or confidential information. In addition,

- Password protected screensavers shall be set to activate after 15 minutes of workstation inactivity.
- Passwords must meet the City's minimum password requirements and shall be changed every 90 days.
- Passwords shall contain a combination of upper and lower case letters, with numbers and symbols, so that they are considered to be "strong" passwords.
- Passwords must be used on all devices that are used for City business, including hand held devices such as smart phones, tablets, etc.

Maintain Anti-Virus Software: Servers, laptops, desktops, and other appropriate devices must have anti-virus software installed and updated at all times. Departments must ensure that anti-virus software is installed at every workstation and virus definitions are updated periodically.

Promote a Culture of Cybersecurity Awareness: Departments must periodically remind their employees and contractors of City cybersecurity policies and best practices. Furthermore, cybersecurity considerations shall be incorporated into all new department systems or projects when applicable.

Plan for Business Continuity and Disaster Recovery: Departments must assess their mission critical systems and plan for both continuity of operations and disaster recovery in the event of a successful cyber attack. This includes an annual update of the department's Continuity of Operations Plan (COOP), which should include a listing of mission critical systems and planned responses in the event of a cyber attack. Additionally, each department shall establish a data backup process for mission critical systems to allow system restoration with the loss of significant data.

City Employee and Contractor Responsibilities

City employees are our first line of defense in ensuring that City systems are protected from intruders. Employees are in the best position to protect the systems, and are in the best position to report problems at an early stage before the issue impacts the City more broadly. All City employees are encouraged to promote a culture of cybersecurity within their departments and to report issues that they identify. It is also incumbent upon City employees to act ethically and with integrity when using and accessing the City's computer systems. Additionally, employees have a responsibility to protect these systems from disruption, intrusion, or attack. With these principles in mind, employees should engage in the following practices:

Prevent Unauthorized Access: Limiting data and network access to authorized individuals is a primary means for securing the City's IT assets. City employees are in the best position to ensure that all City IT assets are protected and that only authorized individuals have access to these important City assets.

Promote Password Security: Every employee's user ID and password provides critical protection from unauthorized cyber attacks. Employees shall not share this information with anyone else, including other City employees. Employees should:

- Set their computers to automatically require password protected screensavers after 15 minutes of workstation inactivity.
- Change their passwords every 90 days.
- Use passwords that contain a combination of upper and lower case letters, with numbers and symbols, so that they are considered to be "strong" passwords (please refer to the Information Technology Policy Committee, Password For City's Network and Internet Accessibility for further details on the minimum password requirements that must be followed).
- Use passwords on all devices that are used for City business, including hand held devices such as smart phones, tablets, etc.

"Smart" Usage of Internet and E-mail Attachments: Internet usage and e-mail are primary methods used to install malicious software onto computers and networks. Employees and contractors must practice vigilance in the usage of the Internet and e-mail (please see the ITA Internet Acceptable Usage Policy). Practices that should be employed include:

- Never entering personal or sensitive City information into untrusted websites;
- Deleting e-mails and e-mail attachments from unrecognized sources;
- Never downloading material from untrusted sources; and
- Maintaining Internet browser security settings of medium or higher.

Prevent Usage of Unauthorized Devices: Cyber attackers are looking for "points of entry" into the City network or a department's systems. Employees should not connect personal or unauthorized devices into their work computer. Such devices include flash/thumb drives, external drives, music devices, smart phones, untrusted CDs or DVDs, or other similar devices.

Use Systems Only For City Business Activities: Employees shall not use computers for non-business related access to audio and/or video Internet sites to listen to music or watch video clips. The network traffic created by accessing these audio and video sites places an enormous burden on the City's networks, negatively affecting the ability of other employees to access the Internet for legitimate business activities.

Responsibilities of ITA

The City's Information Technology Agency, as the unifying technology department throughout the City, will be key to ensuring the success of our City's technology security strategy. ITA is responsible for all firewalls, intrusion detection systems, application control engines, annual security audits and penetration tests, and validating to the Cyber Intrusion Command Center that departments are diligent in their security practices. As such, ITA shall ensure that:

- All cyber technology policies are up-to-date, and they are easily accessible to all City employees for use and reference.
- All City departments have proper technology to ensure that they can comply with this directive. This shall include, but not be limited to:
    - Developing mechanisms to determine whether dormant e-mail accounts have been deactivated.

  - Providing all departments with the technology or software needed to automatically prompt employees to change and update passwords every 90 days.
- All City employees receive annual training on cybersecurity.
- All software is maintained, including updates and patches, as recommended by the manufacturer.

Executed this 30th day of OCTOBER, 2013

ERIC GARCETTI
Mayor