WILLIAM T FUJIOKA
Chief Executive Officer

County of Los Angeles
CHIEF EXECUTIVE OFFICE
OPERATIONS CLUSTER

DATE: May 2, 2013
TIME: 1:00 p.m.
LOCATION: Kenneth Hahn Hall of Administration, Room 830

AGENDA

Members of the Public may address the Operations Cluster on any agenda item by submitting a written request prior to the meeting.
Three (3) minutes are allowed for each item.

1. Call to order – Gevork Simdjian

A) **Computer Emergency Response Team (CERT) Discussion**
DA – Jackie Lacey or designee

B) **Board Letter – COUNTYWIDE INTEGRATED RADIO SYSTEM (CWIRS) AGREEMENTS**
ISD – Tom Tindall or designee

C) **Archives Management Proposal**
RR/CC – Dean Logan or designee

D) **IT Projects**
Arts Commission – Laura Zucker or designee

E) **Upcoming IT Items**
CIO – Richard Sanchez or designee

2. Public Comment

3. Adjournment

MEMORANDUM

TO: STEVE COOLEY
District Attorney

THROUGH: JACQUELINE LACEY
Chief Deputy District Attorney

JANICE MAURIZI, Director
Bureau of Fraud and Corruption Prosecutions

FROM: KATHRYN SHOWERS, Head Deputy
High Technology Crime Division

SUBJECT: **CREATION OF CYBER TEAM**

DATE: AUGUST 13, 2012

The Los Angeles County District Attorney's Office High Technology Crime Division proposes the creation of a specialized cyber team composed of a deputy district attorney, a supervising investigator, four senior investigators, and one support staff. We are requesting funding for these new positions. Since December 2011, investigators and prosecutors from the High Technology Crime Division have worked five intrusion cases with the Los Angeles County Chief Information Officer, Robert Pittman, and members of the Internal Services Department Security and Business Recovery Division. We are currently involved in two active investigations.

The goals and objectives of Cyber Team are as follows:

- Assist CISO Pittman, ISD Security Team and the 34 County Department Information Security Officers (DISO) to secure and protect their department networks.
- Conduct basic penetration testing for the most popular attacks or as requested by the DISO to assess vulnerabilities associated with computer network infrastructure.
- Conduct security audits of county buildings which house the critical network infrastructure.
- Provide incident response services to the 34 county departments 24/7.
- Investigate and prosecute individuals responsible for the breach or attempted breach of county networks.

This specialized team will continuously train and utilize the most sophisticated security software tools to protect county infrastructure.

"Cyber Attacks of Los Angeles County Departments"

The High Technology Crime Investigation Section of the Los Angeles District Attorney's (LADA) Office, Bureau of Investigation, formed a Computer Emergency Response Team (CERT) in 2007 to investigate individuals who target the Los Angeles County computer infrastructure as well as those in private industry. The LADA CERT has been working with the Los Angeles County Chief Information Security Officer (CISO), Robert Pittman, since December 2011 on security incidents, as well as establishing security measures for Los Angeles County.

CISO Pittman recently wrote that during the last two years, the County has experienced a 200% increase in sophisticated application-level attacks. This increase in attacks is consistent within the industry of information technology.

The LADA CERT has responded to the following Los Angeles County breaches:

- ✓ On December 7, 2011, members of the Los Angeles District Attorney (LADA) Computer Emergency Response Team (CERT) met with Chief Information Security Officer (CISO) Robert Pittman, and Division Manager Regeanie Becerra, Internal Services Department, Security and Business Recovery, regarding a potential breach of the Los Angeles County Adult Drug Courts and the Sentenced Offender Drug Court (SODC) Program. The Drug Court Management Information System (DCMIS), which stores 17,697 records with client Personal Identifying Information (PII), including names, dates of birth, social security numbers, and driver license numbers was compromised.

  The LADA CERT performed a comprehensive analysis and investigation using computer forensic tools, log analysis, open source tools, and other law enforcement sensitive sources and determined the breach stemmed from an "automated tool (malware)"[1] that affected the whole internet and

[1] **Malware** is software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software.

thousands of Websites; the source Internet Protocol (IP)[2] address originated in Russia. The malware was not specifically targeted at Los Angeles County. The LADA CERT found that the malware used a Structured Query Language (SQL)[3] Attack as well as a Cross-Site Scripting[4] Attack. The LADA CERT investigation found the County Database on the DCMIS server was not compromised of PII information.

- ✓ On January 3, 2012, members of the LADA CERT received information from a law enforcement sensitive source that over 2,500 government usernames and passwords were shared by the infamous hacker group Anonymous. This information was shared by Anonymous using the Peer-to-Peer technology. The LADA CERT received a copy of the information being shared and notified Los Angeles County CISO Robert Pittman as well as Robert Morgester, Senior Assistant Attorney General for the State of California. CISO Pittman reported that none of the government passwords belonged to Los Angeles County employees. However, Morgester reported emails and passwords were compromised as follows: 1,024 were California employees (306 from the California Department of Justice and 49 from the California Department of Motor Vehicles). The investigation was turned over to the State of California.

- ✓ On April 27, 2012, the LADA CERT members were briefed by CISO Pittman and ISD Security Operations Staff Regeanie Becerra of the possibility that computer servers of the Registrar Recorder/County Clerk's Office (RRCC) were breached. One of the servers was for the Electronic Vote by Mail Ballot (EVMB). The LADA CERT performed a comprehensive analysis and investigation using computer forensic tools, log analysis, open source tools, and other law enforcement sensitive sources determined unknown suspect(s) used a network tool called Acunetix[5] to scan two public facing servers of the RRCC. It is well known

---

[2] An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "*A name indicates what we seek. An address indicates where it is. A route indicates how to get there.*"

[3] **SQL** (sometimes referred to as **Structured Query Language**) is a special-purpose programming language designed for managing data in relational database management systems (RDBMS).

[4] **Cross-site scripting** (**XSS**) is a type of computer security vulnerability typically found in Web applications, such as web browsers through breaches of browser security, that enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec as of 2007. Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

[5]**Acunetix** checks for all web vulnerabilities including SQL injection, Cross-site scripting and many others. SQL injection is a hacking technique which modifies SQL queries in order to gain access to data in the database. Cross-site scripting attacks allow a hacker to execute a malicious script on your visitor's browser. Detection of these vulnerabilities requires a sophisticated detection engine. Paramount to web vulnerability scanning is not the number of attacks that a scanner can detect, but the complexity and thoroughness with which the scanner launches SQL injection, Cross-site scripting and other attacks.

that Acunetix is a tool of choice by the Anonymous[6] hacking group. Based on the LADA CERT investigation, it was determined that the suspect(s) used the Acunetix tool to determine if the county servers were vulnerable to a SQL Injection Attack and a Cross-Site Scripting Attack. It was determined that no data from the SQL server was compromised. This case caught the attention of the Board of Supervisors because of the upcoming June 5, 2012 Presidential Primary Election. A source IP address was found to have originated from Saudi Arabia. The United States does not have a Mutual Legal Assistance Treaty (MLAT)[7] with Saudi Arabia. Through law enforcement sensitive sources, it was determined to be an open proxy server that would not yield information for us, even if an MLAT could be sought.

- ✓ On May 16, 2012, at approximately 8:30 p.m., the LADA CERT received a telephone call from a law enforcement source that members of Anonymous, the infamous hacking group, had just hacked into the Los Angeles Sheriff's Department servers. At approximately 9:30 p.m., the LADA CERT notified the Los Angeles Sheriff High Tech Crime Unit of the breach. The breach involved the Sheriff's dashboard, which is a Graphical User Interface (GUI)[8] that is interactive and sorts through data. The LADA CERT turned the investigation over to the Sheriff's High Tech Unit upon their request. The LADA CERT has been assisting the Sheriff's High Tech Unit with their investigation due to the LADA CERT expertise in network intrusion investigations. The details of the breach were reported by the LADA CERT to CISO Pittman.

- ✓ On May 30, 2012, the LADA CERT was notified by CISO Pittman of a possible breach to the Registrar Recorder/County Clerk's (RRCC) server. A newly implemented Web Application Firewall (WAF)[9] device was implemented. The log files of the WAF found that there was a SQL Injection Attack of the www.lavote.net server on May 29, 2012. This server tells county voters their polling place. The LADA CERT conducted an analysis of the file logs and found a suspect IP Address in Sacramento, California. The LADA CERT obtained search warrants for Subscriber

---

[6] **Anonymous** is a loosely associated hacktivist group. It originated in 2003 on the imageboard 4chan, representing the concept of many online and offline community users simultaneously existing as an anarchic, digitized global brain. It is also generally considered to be a blanket term for members of certain Internet subcultures, a way to refer to the actions of people in an environment where their actual identities are not known. It strongly opposes Internet censorship and surveillance, and has hacked various government websites. It has also targeted major security corporations.

[7] A **mutual legal assistance treaty** is an agreement between two countries for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws.

[8] A **graphical user interface** (GUI, commonly pronounced gooey) is a type of user interface that allows users to interact with electronic devices using images rather than text commands.

[9] An **application firewall** is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall. The application firewall is typically built to control all network traffic on any OSI layer up to the application layer.

Information to determine the person(s) and location of the suspect IP Address. After receiving the Subscriber Information, a search warrant was served in Sacramento where suspects confessed that they had accessed the Los Angeles County RRCC server. One suspect admitted using the SQL Injection Attack to breach the RRCC's lavote.net server. The LADA CERT is waiting for results from additional search warrants to Amazon for the suspect company's database information and logs. This investigation is still ongoing.

- ✓ In August 2012, the LADA CERT received a telephone call from the Los Angeles County Housing Authority regarding an unauthorized access of one of their servers. This server is a waiting list for those requesting Section 8 housing. The LADA CERT responded and after their analysis and investigation, found a suspect using other people's credentials to log into the server. The suspect has found a "time-out" vulnerability that allows the suspect to manipulate the data in the database. "Time-out" vulnerability allows a user to wait for a period of time before entering data on the Website. After a period of time, the user is able to access the whole database. The suspect is charging citizens of Los Angeles money to move their name up higher on the priority list. The investigation is still on-going and we are waiting for the results from the suspect IP Address for Subscriber Information.

CYBER TEAM PROPOSAL

"Protection of the Los Angeles County Computer Infrastructure"

I. INTRODUCTION

Los Angeles County is the most populous county in the United States. It is also an economic hub for the movie and recording industries, software and videogames development, aerospace and automobile design, pharmaceuticals, fashion and accessories, and finance and is the site of the largest port complex on the Pacific coast. Los Angeles County economy ranks 19th in the world; the United States is ranked number one. Thirty-two (32) county departments serve more than eleven (11) million constituents providing critical infrastructure for residents and businesses. Law enforcement's ability to identify, prioritize, and manage the risks associated with the protection of the county critical assets is a priority.

The Los Angeles County District Attorney's Office proposes the creation of a law enforcement cyber team whose core mission is the protection of county computer networks and the investigation, and prosecution of individuals and crime groups who attack and attempt to seize control of county computer infrastructure.

This highly trained investigative "Cyber Team" will be staffed by a Deputy District Attorney IV, a Supervising District Attorney Investigator, four Senior Investigators, and a typist clerk.

II. BACKGROUND

As the largest prosecutorial office in the United States, the Los Angeles County District Attorneys Office (LADA) is a leader in fighting cyber crime. The High Technology Crime Division (HTCD) is composed of eight prosecutors tasked with the vertical prosecution of technology related crime. Integral to their success is the Bureau of Investigation High Technology Crime Investigation Section (HTCIS) staffed by a lieutenant, two supervisors, and ten senior investigators. HTCD prosecutors and HTCIS investigators are recognized leaders within the cyber community not only within the United States, but also internationally serving as officers, directors and advisors for professional organizations such as the High Technology Crime Investigation Association (HTCIA), the Society for Policing of Cyber Space (POLCYB) and Cyber Watch West. HTCD and HTCIS have been very successful investigating and prosecuting cyber crimes including network intrusions, theft of intellectual property and large-scale identity theft rings. However, HTCIS does not have the financial resources or staff to implement the proactive measures necessary to evaluate risks and harden security procedures related to county computer infrastructure.

Recognizing that technology can facilitate theft and fraud, District Attorney Steve Cooley created the LADA Computer Emergency Response Team known as CERT in 2007. In addition to their other duties, the team responded to eleven (11) cyber incidents using their tech skills to investigate hackers targeting county computer infrastructure as well as private industry. LADA cyber investigators have completed incident response training focusing on computer breaches receiving certification from Carnegie Mellon, the FBI and Secret Service. With these credentials, CERT members have evolved into an elite law enforcement team.

The Bureau's High Technology Crime Investigation Cyber Investigators began working with Robert Pittman, the County Chief Information Security Officer, in 2011 investigating hacking attempts on county networks. Most of the incidents have involved Series Query Language (SQL) injection attacks on county databases and servers. In the last nine months, HTCIS has investigated four (4) breaches and attempted breaches of county computer infrastructure. To our knowledge, none of the hacks were successful in breaching county network security. However, the increase in attempts is a wake up call. It is just a matter of time before the hackers will be successful if the county does not take steps to harden security procedures and increase personnel to investigate and prosecute individuals who attempt to breach the county's computer infrastructure.

Government agencies, private corporations and academic institutions often do not learn their network has been breached for days, months, even years after the intrusion occurred. Intruders can conceal their presence, which allows them time to identify and export personal identifying information, research, intellectual property and proprietary information at their leisure. Professional security managers agree there is no completely secure system. Recently at a conference of industrial control system (ICS) security officials sponsored by the United States Department of Homeland Security, managers from the oil and nuclear industry and water districts all admitted their agencies and corporations often operate using outdated software and that their systems have known vulnerabilities. Historically, industrial control systems have not been designed with robust security features. Updating software and hardware generally is not sufficient to protect critical infrastructure from unauthorized intrusions. In the last year, HB Gary Federal, an internationally recognized firm who provides network security for the federal government was decimated by the infamous hacker group "Anonymous" after bragging about the security features of their corporate network.

Perhaps the most important information gleaned from our recent investigations of attempted hacks of the county's networks is that a penetration test of county departmental systems would have easily detected many of the vulnerabilities found within the county's computer system. Carnegie Mellon's SANS Institute defines penetration testing as the process of attempting to gain access to resources without knowledge of user-names, passwords or other normal means of access. In the case of computer network resources, examples of a successful penetration would be accessing or subverting confidential documents, pricelists, databases or other protected

information. Permission is the characteristic that distinguishes a penetration tester from a hacker. The penetration tester has permission from the owner of the computing resources to access the network and its resources and is responsible for identifying and reporting system vulnerabilities. The goal of a penetration test is to provide recommendations to increase the security of the computing resources being tested. According to CISO Pittman, penetration testing has not been conducted on the county's networks in many years. Penetration testing by private security companies can be quite expensive.

CISO Robert Pittman is in support of the creation of a Cyber Team and wrote the following:

> The Countywide Information Security Program (CISP) was established and adopted by the Board of Supervisors (Board) on July 13, 2004. The CISP is supported by Board-level information technology (IT) security policies in order to assure appropriate and authorized access, usage, and the integrity of County information and information technology assets. There are numerous elements within the CISP; however, the Countywide Computer Emergency Response Team (CCERT) must be highlighted. The CCERT is comprised of employees from each department to respond to various computer security emergencies. These emergencies could be a computer incident associated to a website being hacked exploiting a known vulnerability, potential compromise of the county's confidential and/or sensitive information, etc.

The County of Los Angeles 2010-2011 Civil Grand Jury Final Report (see attached investigative report as it pertains to Hi-Tech Forensics) stated recommendations specific to "High Technology Forensics and Cyber Security Crime Fighting in the Digital Age." The Chief Information Office (CIO) Memorandum of August 19, 2011, accepted their recommendations for improvements in this area as agreed by the County's Chief Information Security Officer (CISO). The CISO engaged and collaborated with the District Attorney's High Technology Crimes Investigation Unit (DA) to address the Grand Jury's recommendations:

3. *LAC Chief Information Office and Internal Services Department should conduct internal reviews concerning cyber security and infrastructure protection from Cyber attacks and terrorism:*

    a. *LAC must have protocols, policies and procedures facilitating timely, efficient rapid response by the most able cyber security resources available and ancillary emergency response by other agencies, if warranted, in the event of a cyber intrusion, fire wall breach or other cyber attack.*

b. *These should include coordination with key third party vendors. Many basic services within the LAC are provided by third party vendors. The Metropolitan Water District and California Edison are two (2) examples.*

This collaboration will establish an incident response team that provides a level of expertise that does not currently exist throughout the County.

The DA and CISO partnership permits the CCERT to create an Incident Response discipline while intensifying our capability and knowledge specific to personnel involved in responding to a computer security incident. During the last two (2) years, the County has experienced a 200% increase in sophisticated application-level attacks that is consistent with the industry. This warrants a workforce increase and promotes the establishment of a Cyber Team. This expansion supports Board IT Security Policies:

✓ **#6.103 - Countywide Computer Security Threat Responses:**

The purpose of this policy is to define the County's responsibility in responding to countywide computer security threats affecting the confidentiality, availability and/or integrity of County computerized data, and/or information processing resources.

✓ **#6.109 - Security Incident Reporting:**

The intent of this policy is to ensure that County departments report information technology (IT) security incidents in a consistent manner to responsible County management to assist their decision and coordination process.

III. LADA RESOURCES

The LADA HTCD and HTCIS already have the infrastructure in place to investigate and prosecute unauthorized intrusions. HTCD prosecutors have specialized training in forensic technology, how network intrusions are initiated and malware deployed within systems, and how to utilize digital and electronic evidence to convict intruders. HTCIS cyber investigators have extensive training from the United States Secret Service Electronic Crimes Task Force, United States Department of Defense, Carnegie Mellon's Software Engineering Institute, and SANS Institute. Many of the cyber investigators are certified by the SANS Institute on incident response and network intrusions. The background and training of LADA cyber investigators equals that of cyber investigators employed by the Federal Bureau of Investigation.

As part of the county family, securing the county computer infrastructure is a top priority for the Los Angeles County District Attorney's Office. As a founding member of the United States Secret Service Electronic Crimes Task Force and task force member of the FBI's Intellectual Property Loss Mitigation Working Group, and Southern California High Tech Task Force, HTCIS has collaborated and cooperated with federal, state and local partners on issues related to network security. HTCD prosecutors routinely work with the United States Attorney's Office for Central District on cyber cases and the extradition of suspects from foreign countries.

IV. BENEFITS FOR THE COUNTY

There are volumes of confidential, personal information on the approximately eleven (11) million residents of Los Angeles County within the various County of Los Angeles department databases. The county's stated mission is, "To enrich lives through effective and caring service." The county must do everything possible to protect that information. The creation of a Cyber Team will:

- ✓ help protect constituents from cyber incidents that damage critical infrastructure and disrupt delivery of essential services;
- ✓ investigate and resolve computer security incidents occurring within the county, including threats to critical infrastructure from insiders and outliers; and
- ✓ integrate computer forensics and cyber crime analysis tasks to provide real-time response capability that will potentially mitigate damage to networks and loss of data from these incidents, decrease incident response time, and facilitate the apprehension and prosecution of perpetrators responsible for these breaches.

The Cyber Team will collaborate with the County Chief Information Security Officer, Robert Pittman, and the Internal Services Division Security Team on issues related to the prevention, investigation, and prosecution of the cyber criminals who attack the county's computer infrastructure.

Funding a Cyber Team will provide the County of Los Angeles with the opportunity to assume a leadership role in the development of prevention and incident response for local governments. These best practices will be a model for other government agencies throughout the country.

IV. RECOMMENDATIONS

I. Cyber Team

A. Personnel Requirements:

$986,000

1. One Deputy District Attorney IV
2. One Supervising District Attorney Investigator
3. Four Senior Investigators
4. One Support Staff

B. Goals and Objectives:

1. Assist CISO Pittman, ISD Security Team, and 34 Department Information Security Officers to secure and protect their department networks;
2. Conduct penetration testing as requested to assess vulnerabilities associated with computer network infrastructure;
3. Conduct security audits of county buildings housing critical network infrastructure;
4. Provide incident response services to county departments 24/7; and
5. Investigate and prosecute individuals responsible for the breach or attempted breach of county computer networks.

C. Training:

1. Cyber investigations
2. SANS Institute
   a. Incident response
   b. Computer network breaches
3. Penetration testing
4. Network forensics

II. **Utilize Private Security Resources**

A. Contract with private intelligence companies for real-time intelligence on hacker activities and websites:

   1. Team Cymru.
   2. Tiversa Funding for Team Cymru and Tiversa (real-time information about hackers that are trying to hack into the County's infrastructure).

B. Monitor hacker chat and threats related to targets located in Los Angeles County.

County of Los Angeles
INTERNAL SERVICES DEPARTMENT
1100 North Eastern Avenue
Los Angeles, California 90063

TOM TINDALL
Director

Telephone: (323) 267-2101
FAX: (323) 264-7135

"To enrich lives through effective and caring service"

May 14, 2013

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Dear Supervisors:

REQUEST FOR APPROVAL OF AGREEMENTS WITH SPRINT NEXTEL CORPORATION AND HARRIS CORPORATION TO RE-BAND AND UPGRADE THE COUNTYWIDE INTEGRATED RADIO SYSTEM (CWIRS) (ALL DISTRICTS – 3 VOTES)

SUBJECT

Approval of agreements with Sprint Nextel Corporation (Sprint) and Harris Corporation (Harris) to upgrade and re-band the Countywide Integrated Radio System (CWIRS) per the Federal Communication Commission's (FCC) nationwide mandatory re-banding program for 800 megahertz (MHz) radio channels. This $20 million settlement agreement, fully funded through Sprint, will allow the Internal Services Department (ISD) to comply with the FCC mandates, as well as to upgrade CWIRS to meet the national Project 25 (P25) land mobile radio standard, at no cost to the County.

IT IS RECOMMENDED THAT YOUR BOARD:

1. Approve and instruct the Chairman to sign the Frequency Reconfiguration Agreement (Attachment I) with Sprint, which provides $20 million and certain radio equipment and infrastructure hardware to replace and upgrade CWIRS as part of the FCC's frequency re-banding mandate.

2. Approve and instruct the Chairman to sign the 800 MHz System Rebanding Agreement (Attachment II) with Harris, under which Harris will provide radio reconfiguration services to move CWIRS to new radio frequencies using the nationwide P25 radio standard at no cost to the County.

3. Authorize the Director of ISD or his designee to exercise change orders if needed with Harris, not to exceed an aggregate maximum of $250,000, and to add and delete facilities, approve necessary changes to scope of services, and execute applicable contract amendments should the original contracting entity merge, be acquired, or otherwise have a change of entity.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

CWIRS is a County radio system used for mobile communications by a number of departments, including Health Services, Public Works, Probation, Animal Care & Control and ISD. In addition to serving the day-to-day operations of its user departments, CWIRS is the County's primary disaster recovery mobile communications system in a major emergency incident.

About fifteen years ago, public agencies like the County using the 800 MHz radio band frequency started to experience radio interference caused by adjacent frequency use by Nextel Communications, Inc. (now Sprint). To eliminate this interference and allocate frequencies for more efficient use, the FCC issued orders in 2004 requiring all 800 MHz licensees, including the County, to move to new frequencies. The FCC also ordered Sprint to provide funding to all licensees for such reconfiguration.

Reconfiguration involves re-tuning (re-banding) system hardware (e.g., consoles, base stations, mobile and portable radios) and system software to use new frequencies, but does not require civil engineering or construction.

Under FCC jurisdiction, reconfiguration is a two phase project. Phase 1 is planning and design. Phase 2 is implementation. Each phase requires (1) a funding agreement with Sprint to commit funds as mandated by the FCC, and (2) a services agreement with our existing CWIRS equipment vendor, Harris (formerly M/A-COM). On January 11, 2007, we notified your Board of ISD's intent to enter sole source negotiations with M/A-COM/Harris for agreements related to both the planning and implementation of this project.

Your Board approved Phase I agreements on February 20, 2007, with delegated authority to the ISD director. As previously reported to your Board, Phase 1 was completed in October 2008, when Harris delivered an implementation plan and proposal to ISD.

The start of work on Phase 2 was delayed until June 2012, pending the conclusion of a treaty with Mexico for radio frequency allocations. Since then, ISD has provided periodic status reports to your Board, most recently on April 9, 2013, describing the status of negotiations with Sprint and Harris, including the "opt-out" settlement with Sprint.

The Opt-Out Upgrade

Sprint has offered an "opt-out" settlement, whereby a three-way accord is established among the County, Sprint, and the FCC, and all parties agree to settlement payments. This settlement provides the County with flexibility to upgrade CWIRS to meet the national P25 land mobile radio standard. P25 will enhance system compatibility and interoperability with other and future state-of-the-art public safety/service communication systems, including the planned Los Angeles Regional Interoperable Communications System (LA-RICS).

The Sprint offer includes a $20 million settlement funding to re-band and simultaneously upgrade CWIRS. Additionally, Sprint offered to provide 6,247 new P25-ready radios, and Harris, our current CWIRS contractor, will upgrade 1,494 existing radios to the P-25 standard at no cost to the County.

Sprint's offer requires County acceptance by June 1, 2013. This time frame will provide Sprint with access to County-relinquished radio frequencies within 28 months after contract execution, pursuant to a mutually agreed upon schedule.

Implementation of Strategic Plan Goals

The recommended contracts support County Strategic Plan Goals Number 1 for Operational Effectiveness, by providing timely delivery of customer oriented and efficient public services, and Goal Number 2 for Fiscal Sustainability, as the County will be able to upgrade its aged CWIRS radio system to current P25 standards without contributing general fund monies.

FISCAL IMPACT/FINANCING

Under the Frequency Reconfiguration Agreement (Attachment I), Sprint will provide $20 million to replace and upgrade CWIRS as part of the FCC's frequency re-banding mandate, including the following cost estimates:

System upgrade cost to be paid to Harris	$17.3 million
System upgrade cost to be paid to the County	$2.5 million
Legal services to be paid to the County's outside counsel	$0.2 million
Total	$20 million

ISD implementation costs totaling $2.5 million will be fully reimbursed by Sprint, requiring no net County cost. ISD will request additional appropriation required to support this project during the Final Changes phase of the Fiscal Year 2013-14 budget process, and in future fiscal years. For project contingencies, ISD seeks authority to execute change orders up to a maximum of $250,000 over the project term. Such change orders, if any, will be funded from the $2.5 million identified for County costs.

Under the agreement, the County will receive cost reimbursement in two parts: the first $1.25 million after the agreement is executed, and the remaining $1.25 million after the County relinquishes its 800 MHz radio frequencies to Sprint.

The payment schedule to Harris is described in the 800 MHz System Rebanding Agreement (Attachment II). Payments are linked to Harris' successful completion of tasks described in the Statement of Work. The payment schedule for Harris retains $2.5 million pending final system acceptance by the County.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The 800 MHz System Rebanding Agreement with Harris includes a Statement of Work as Attachment B to that Agreement. The Statement of Work describes the project technical details, including: radio system coverage overview; planned migration and cutover; current and proposed radio frequencies; equipment description for each site/area; the project team and responsibilities; reporting requirements and project schedule; site power and cooling requirements; antenna system designs and equipment installation; user equipment description including portable radios; acceptance testing details; training for maintenance and operation of

systems and radios, equipment removal description; etc. The project timeline is expected to be approximately 28 months.

The FCC has created a Transition Administrator (TA) to administer the 800 MHz re-banding process and review re-banding expenditures for compliance with FCC rules. The TA works directly with all frequency licensees affected by radio band reconfiguration. Upon reviewing and approving the Frequency Reconfiguration Agreement between the County and Sprint, the TA will issue a "Letter of Authorization" to Sprint to proceed with the agreement.

The County retained the law firm of Schulman, Rogers, Gandal, Pordy & Ecker, P.A. as outside telecommunications counsel to assist in negotiating and memorializing the recommended contracts. A confidential opinion memo from Alan S. Tilles, the Chairman of the Firm's Telecommunications Department, is submitted to the Board contemporaneously with this filing. The recommended contracts have been approved as to form by County Counsel.

CONTRACTING PROCESS

In accordance with your Board's policy, on January 11, 2007, ISD notified the Board of ISD's intent to enter into sole source negotiations with M/A-COM (now Harris) for this project.

CWIRS was acquired in 1993 as a result of a County competitive bid process, resulting in the implementation of a radio system designed and manufactured by Ericsson GE, a predecessor to M/A-COM and ultimately Harris. CWIRS uses components, including software, that are proprietary to Harris. Equipment replacement and component or software upgrades must match or inter-member with the existing system. They cannot be substituted without replacing the entire system, which would result in significant cost to the County.

The agreements are exempt from Proposition A, as the services are of an extraordinary professional, technical and/or temporary nature (County Code 2.121.250(B)(3)), and therefore are not subject to the Living Wage Program (County Code 2.201).

The agreements are also based upon standard agreement forms developed by Sprint and Harris, which are approved by the FCC and unique to the re-banding program. Accordingly, standard County program clauses are not applicable.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

The Harris re-banding approach will maintain existing CWIRS radio functionality during the implementation period until users are migrated to the P25 infrastructure. All activity will be coordinated with departments to ensure that there is minimal or no impact on operations. There is no employee impact as a result of these agreements.

CONCLUSION

Approval of the contracts will allow the County to upgrade and re-band its CWIRS radio system to current P25 nationwide standards with no net County cost. This project will ensure the continued viability of CWIRS for countywide radio communications in future years, and will provide system compatibility and interoperability with other state-of-the-art public safety/service communication systems, including the planned LA-RICS.

Respectfully submitted,

TOM TINDALL
DIRECTOR, ISD

TT:JJ:JLG:RK
Attachments (X)

c: Chief Executive Officer (Fujioka, Simdjian)
County Counsel
Chief Information Officer

DEAN C. LOGAN
Los Angeles County
Registrar-Recorder/County Clerk
12400 Imperial Highway
Norwalk, CA 90650

Archives & Records Management Program & Organizational Proposal

REGISTRAR-RECORDER/COUNTY CLERK

OPERATIONS CLUSTER – MAY 2, 2013

Revised April 19, 2013

Objectives

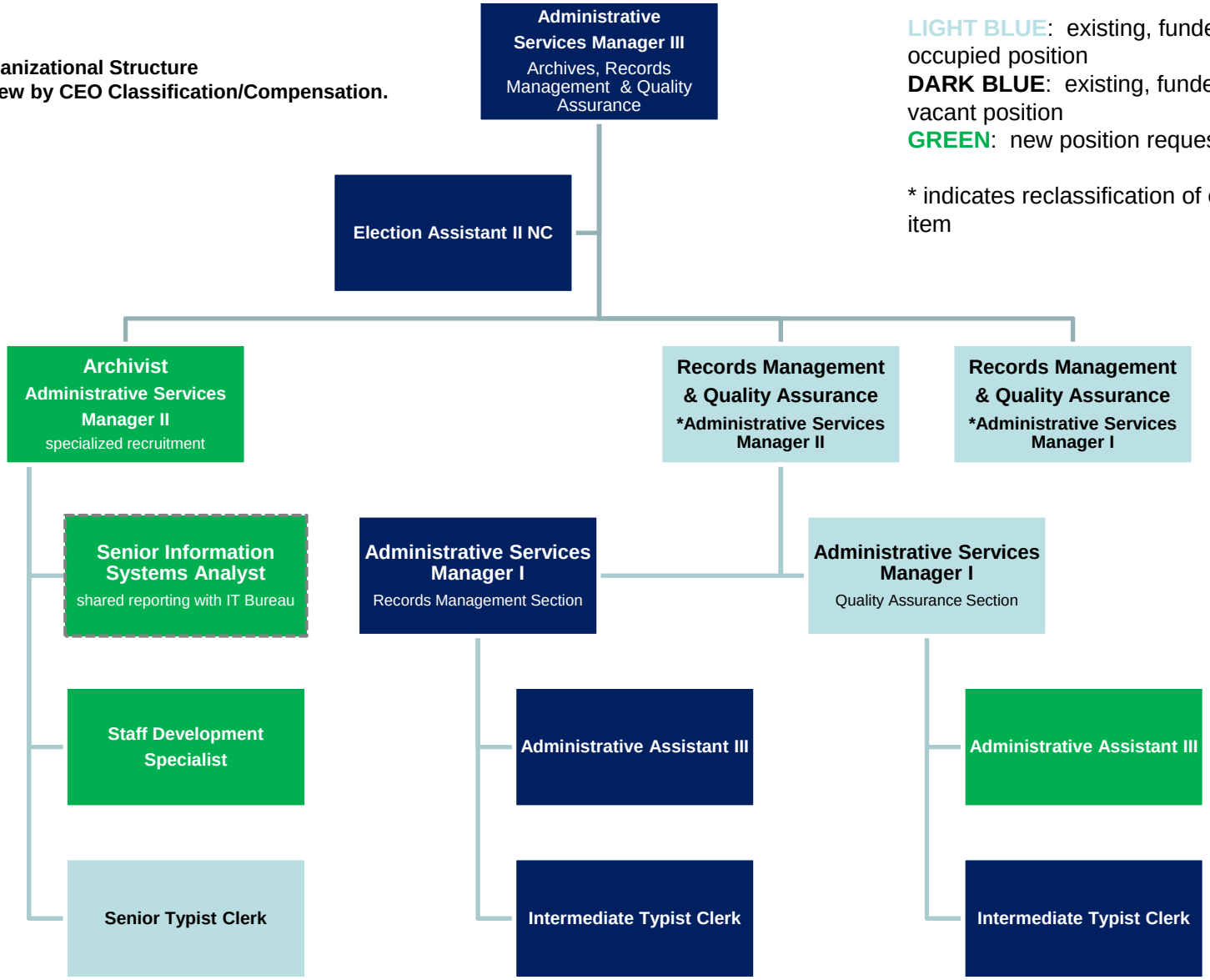
- Establish Countywide records management policies, standards and procedures
- Assess and develop a process for indexing and maintaining County records and items of historical archival or research value – including digital records
- Incorporate above into an organizational structure that can support the objectives and model the policies, standards and procedures once established
- Utilize existing Departmental infrastructure, knowledge and staffing resources to the extent practical
- Adopt an organizational structure that is scalable based on the evolution of the program

Los Angeles County Registrar-Recorder/County Clerk

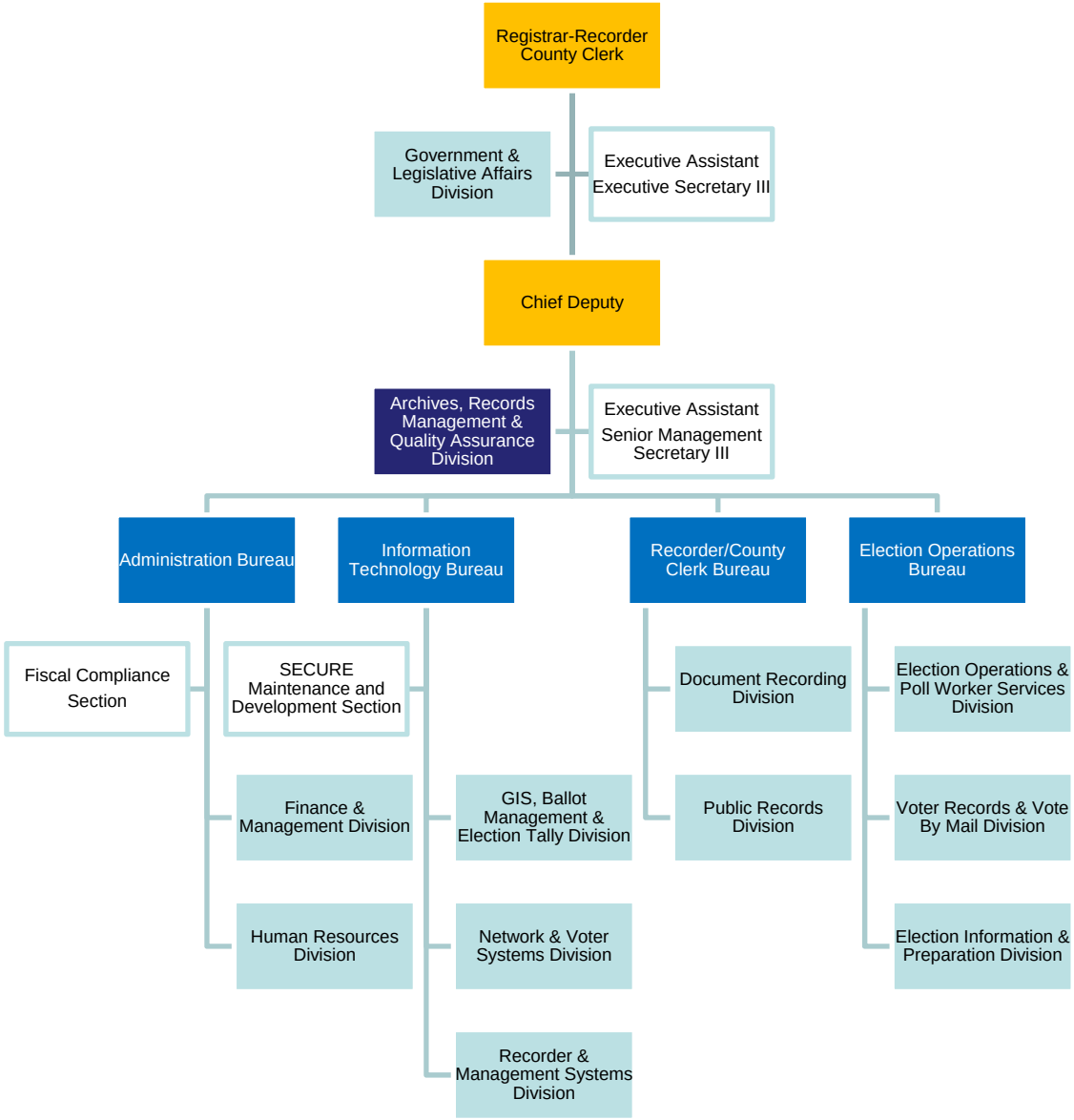
Proposed Organizational Structure
Based on review by CEO Classification/Compensation.

LIGHT BLUE: existing, funded and occupied position
DARK BLUE: existing, funded, vacant position
GREEN: new position request

* indicates reclassification of existing item



Los Angeles County Registrar-Recorder/County Clerk



www.lavote.net

Programmatic Overview

Archives

- Identification of records and items of permanent historical and research value
- Develop digital archives policies and procedures for non-paper based records
- Develop policy for assessing historical and research value of County records
- Provide guidance and assistance with historical research related to the County

Quality Assurance

- Train and facilitate the adoption and implementation of lean six sigma quality assurance principles in Departmental operations
- Consult on all Departmental quality assurance matters
- Conduct quality assurance assessments and assist in special projects with Department wide impact

Records Management

- Maintain County General Records Retention Schedules
- Assist County departments in the development, implementation and maintenance of Departmental records retention programs
- Develop policies and training programs on prudent records management and retention procedures
- Consult on all County records management matters

Comparative Programs & Resources

- King County, Washington
  - Department of Executive Services; Records, Animal & Licensing Services Division (RALS); Records Management & Archives Program
- Riverside County, California
  - Assessor-County Clerk-Recorder; Records Management and Archives Program
- City of Los Angeles, California
  - Office of the City Clerk; Records Management and Historical Archives Division

Budget/Fiscal Considerations

One Time

- Facility Build-out
  - Minimal construction
  - Work station configuration
- Consulting Services
  - Completion of EMC2 records management consulting engagement
  - Potential for Archives consulting engagement
  - Completion of extension on Lean Six Sigma consulting engagement
- Recruitment & Selection
  - Class Comp evaluation of new positions and organizational structure
  - Filling newly established positions
- Employee Training
- Start-up Supplies & Equipment

Ongoing

- Salaries and Employee Benefits
- Operational Budget
  - Travel and training
  - Supplies and equipment

Enriching Lives

Los Angeles County Arts Commission

Arts Commission IT Requests

Presentation to the
Operations Cluster
May 2, 2013

Overview

County Shared Portal Infrastructure upgrade ($570,000)

Ford Theatres ticketing, donor relations and marketing management software
An upgraded system will inform and more accurately track the effectiveness of donor campaigns and outreach strategies and provide advanced ticketing functionality for the Ford Theatres. Implementation of this system will create internal efficiencies and improve the quality of service for all programs.

Arts Commission Web site
The commission Web site was launched in 1993. This site has not changed dramatically since that time. In an effort to Improve constituent services and modernize the site, earlier this year we began meeting with the CIO's office to determine the feasibility of upgrading both the back end and the user interface of the site.

FORD THEATRES

Ticketing, Donor Relations and Marketing Software Needs

Desired Capability	Current Ticketing System Capability
24/7 customer service, especially during shows at the Ford.	Software support M-F until 6pm PST, unless “business critical.”
Create-your-own subscriptions (e.g. 20% off 3 or more shows) and the ability to track these subscribers’ lifetime activity.	Subscription packages can only be created if a venue uses the exact same seating layout for each show. As the Ford seating plan varies by producer, we cannot currently create any subscriptions.
A mobile-optimized ticket sales format (API).	No API provided and non-optimized appearance on mobile devices.
Email marketing functionality that can pull data directly from the patron/donor database, with the ability to track open rate, click through rate, and other statistics.	Patron lists can be pulled, but must be imported and maintained separately in Constant Contact.
Social media integration with Facebook and other technologies that allows patrons to purchase directly from their profile & share purchases, and allows us to track sales driven by social media.	Not available.
Flexible day-of-show patron reminder emails with HTML/graphic format.	Very basic text only reminder emails.
Integrated web donations platform that can receive customizable dollar amounts via the web and tracks these transactions in a separate module within the system.	Ability to build donations with fixed giving levels as “performances,” which show online as gifts. Funds from each donation must be manually transferred from Ticketing to the Foundation on the back end.
The ability to track donations from multiple fundraising entities (Arts for All and the Ford Theatres Foundation) while having access to all data at a master level, if desired.	Not available.
Provide customizable reports that can be uploaded seamlessly into our Venue Management System Software.	Basic Daily reports must be manually altered on the back end.
Provide a high level of web design control without having to consult customer support (including but not limited to seat map design, show and series building, making coupon codes and special offers)	Must contact customer support whenever we desire to make any changes.
Automated dynamic pricing options (e.g. capacity triggers)	None; all done manually.

Arts Commission Web Sites

Web Site History

Website Design

- Developed in 1993
- Award Winning
- No update to look and feel in 17 years
- Noncompliant to current Web standards

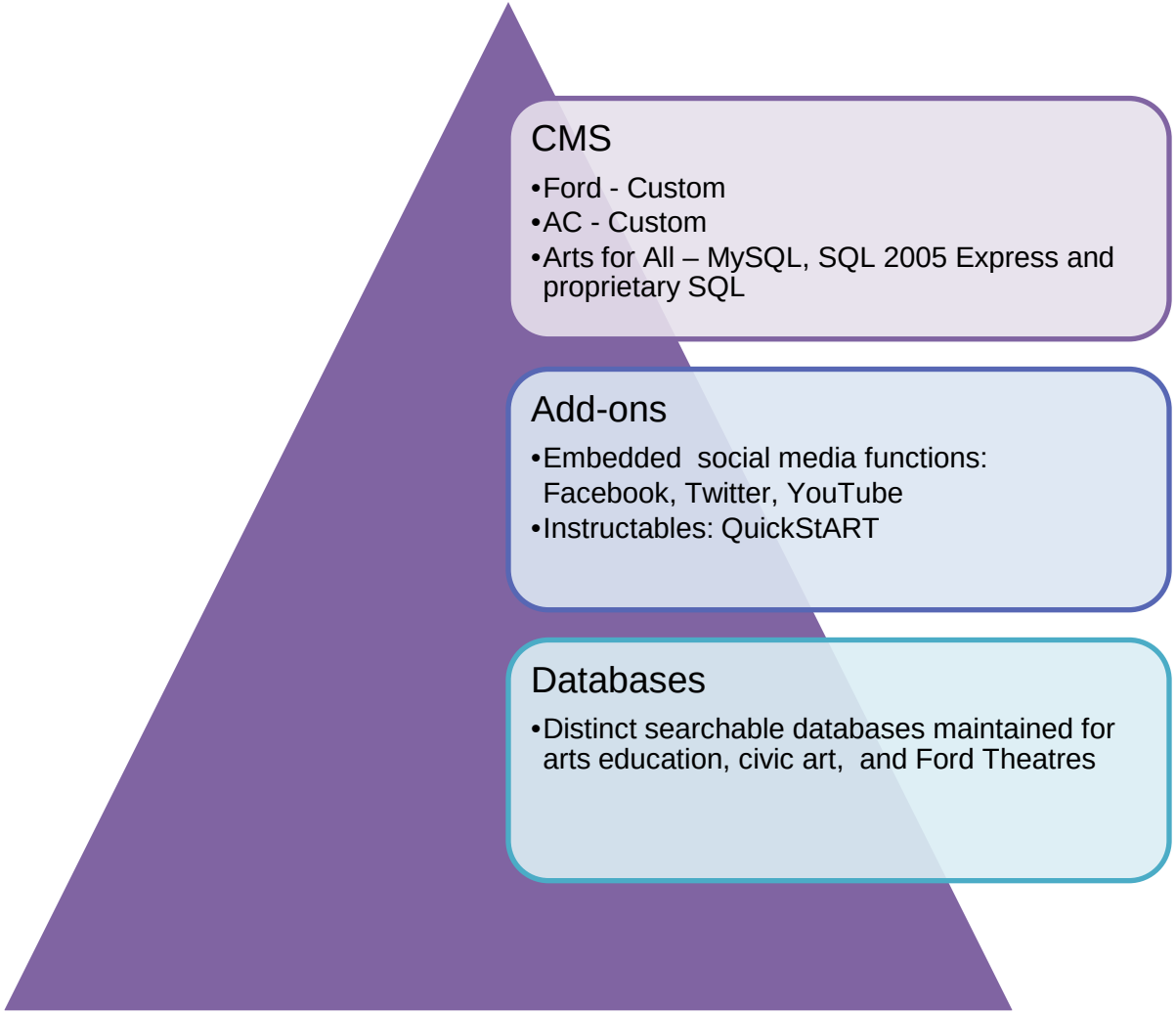
Website Content

- 1993-present ongoing html edits, image replacement, basic upgrades and maintenance
- 2002 separate Ford site launched including CMS
- 2009 CMS Installed in AC site
- 2011 separate Arts for All site launched including CMS

Website Hosting

- Ford/AC: Rackspace
- Arts for All: ISO Media

Current State of Web Site



Web Site Needs

Single CMS

- Arts Commission main site
- Arts for All site
- Ford site

Integrated technology

- Ticketing*
- Event RSVP
- Mapping of services
- Webinars
- Online Classrooms
- Site wide search*
- Social interaction*
- Reliable web analytics across all sites
- Photo and video gallery

Flexibility

- Ability to change the structural elements as the commission evolves

Maintenance

- Dedicated budget for upkeep
- Ability to upgrade software overtime
- Reliable hosting package

*Items indicate existing services which need to be upgraded. All others are new.

Board IT Agenda Items

Department	Board IT Agenda Item	Description	Amount	CEO Cluster	New Term	Planned Hearing Date
A-C	Execute Work Order Under County's Master Services Agreement with EMC for Contract Management System	Authorize execution of a Work Order with EMC Corporation, Inc for the software development and implementation services for the Contract Library System (CLS) component of the Contract Management System (CMS) application. **Funding Source: A-C FY 2012-13 Integrated Applications Budget** **Existing Agreement: EMC MSA 77036**	$650,000	Operations	N/A	5/14/2013
ISD	Authorization to Purchase Mainframe Hardware and Network Equpment	This is to purchase one mainframe computer server to meet the demand for Countywide Web Portal services, and network equipment for DPSS and Public Library. **Funding Source: ISD FY 2012-13 Operating Budget (Appropriation Adjustment from S&S to Capital Assets)** **Existing Agreement: N/A**	$1,004,000	Operations	One-time	5/21/2013
CDC	Acquisition of Microsoft Enterprise Agreement from Insight Public Sector	Agreement to provide Microsoft software for CDC, who currently uses various versions of Microsoft operating systems and Office products. The Agreement will entitle the CDC to access all upgrades in order to standardize all Microsoft products on the most current software versions throughout the organization. **Funding Source: CDC FY 2012-13 Operating Budget** **Existing Agreement: N/A**	$397,656	Community & Municipal Services	3 Years	5/21/2013
DPH	Sole Source Agreement with Computer Therapy for CHOI	Sole Source Agreement with Computer Therapy, LLC for the provision of database technical assistance and training services to support DPH's Children's Health Outreach Initiatives (CHOI) internet based CHOI data collection system for CHOEUR contracted agencies. **Funding Source: First 5 LA Funds and MAA Reimursements** **Existing Agreement: N/A**	$240,000	Health & Mental Health Services	2 years	5/21/2013
DHS	Agreement for Web-based eConsult System and related services between County and SafetyNetConnect	Agreement for development of eConsult software for DHS ACN and SafetyNetConnect. **Funding Source: DHS FY 2012-13 Operating Budget** **Existing Agreement: N/A**	TBD	Children & Families Well-being, Health & Mental Health Services	TBD	6/18/2013

Department	Board IT Agenda Item	Description	Amount	CEO Cluster	New Term	Planned Hearing Date
CIO	Use of ITF for Enterprise IT Security and Privacy Awareness Training Software	Use of ITF to acquire and implement the enterprise IT Security and Privacy Awareness training content for use in the County's Learning Net. **Funding Source: ITF** **Existing Agreement: N/A**	$240,000	Operations	N/A	6/18/2013
DHS	Approval of Amendment to Equipment Maintenance and Repair Services Agreement with Parata Systems	Approval of Amendment to Equipment Maintenance and Repair Services Agreement with Parata Systems, LLC to extend the term. **Funding Source: DHS FY 2013-14 Operating Budget Existing Agreement: H702976**	TBD	Health & Mental Health Services	TBD	7/30/2013
CIO	Los Angeles Region Imagery Acquisition Consortium (LAR-IAC) 4 Agreement	Agreement to acquire digital aerial data for County and participating agencies. **Funding Sources: County Dept Operating Budgets and Participating Cities & Agencies** **Existing Agreement: LAR-IAC 3**	$4M (Est.)	Operations	3 years, with 9 optional years	7/30/2013
DPW	Contract for Alamitos Barrier Project and Dominguez Gap Barrier Project Telemetry System Maintenance Services	Contract for Alamitos Barrier Project & Dominguez Gap Barrier Project Telemetry System Maintenance Services. • Background: The Dominguez Gap and Alamitos Barriers are seawater barriers that are designed to inject freshwater into underground aquifers to create protective pressure ridges and prevent seawater from contaminating groundwater supplies. Portions of the Dominguez Gap and Alamitos Barriers are outfitted with Supervisory Control and Data Acquisition (SCADA) systems that enable operators to remotely monitor conditions and control equipment through COTS user interfaces. Other portions of the barrier systems are manually operated. • Scope: Inspection, maintenance, as-needed repairs, including software configuration and re-programming, and the integration of the manual segments into the automated systems. Note: the Dominguez Gap and Alamitos Barrier systems will remain separate. **Funding Source: Flood Fund (No County General funds)** **Existing Agreement: N/A**	$600,000 per year for up to 5 years	Community & Municipal Services	1 year, with four 1-year option extensions	7/30/2013

Department	Board IT Agenda Item	Description	Amount	CEO Cluster	New Term	Planned Hearing Date
CIO/CEO/DHS/ DMH & DCFS	Countywide Master Data Management (CWMDM)	Implement a Master Data Management solution for the entire County, to include: 1. Development and maintenance of a catalog of enterprise data objects (Data entities, Authoritative sources, Attributes, Values, Access control and policies) 2. Development and maintenance of a catalog of existing system interfaces 3. Development of policies for enterprise information management 4. Building of an Enabling Infrastructure (shared service) for enterprise information management, including: a. Master Data Management b. Enterprise messaging and service bus c. Data analytics **Funding Source: TBD** **Existing Agreement: N/A**	TBD	Operations	TBD	9/17/2013
CIO/LASD/FIRE/ OEM	Extension of AlertLA Agreement with 21st Century Communications	1. Request one-year extention for AlertLA Mass Notification System with 21st Century Communications System. 2. Develop new RFP **Funding Source: ITF** **Existing Agreement: 76945**	N/A	Operations, Public Safety	1 year	
LASD	Multimodal Biometric Identification System (MBIS)	Development of an automated biometric identification system to replace current Cogent system. **Approx. Board Date: TBD** **Funding Source: RAND Board** **Existing Agreement: N/A**	TBD	Public Safety	TBD	
FIRE	Execute Work Order Under the County's IBM Master Services Agreement No. 75869 for Fire Facility Management System	Work Order for services and software licenses will implement Maximo Facilities Management System. **Approx. Board Date: TBD** **Funding Source: Fire FY 2012-13 Operating Budget** **Existing Agreement: 75869**	$407,450	Public Safety	TBD	

Department	Board IT Agenda Item	Description	Amount	CEO Cluster	New Term	Planned Hearing Date
DPW	Agreement For Radio Frequency Identification Project (Note: not official BL title)	Agreement to implement Motorola Radio Frequency Identification (RFID) solution at DPW to automate business processes. The scope of this project includes hardware, software, installation, and training, and two years of maintenance and support. Statement from DPW: "We are going to aim for the 12/18 Board hearing. Meeting this target is dependent on a quick turn around from Motorola's legal staff. Motorola wanted DPW to sign their software and services agreements. Since various Motorola terms and conditions conflicted with the County's, we sent a redlined version back to them for review. We are waiting to hear back from them. " Update from DPW on 2/25/13: "...we are down to a few insurance provisions that we are trying to come to agreement on...hopefully in the next week or so we can begin the BL process." **Approx. Board Date: TBD** **Funding Source: $35,000 loan from County Quality and Productivity Commission (repayment within 3 years), balance from Public Works' Flood Control District General Fund and Public Works' Internal Service Fund** **Existing Agreement: N/A**	$125,000 ($113,690 +10% contingency)	Community & Municipal Services	Implementation, with 2-year maintenance	