THIS PAGE INTENTIONALLY LEFT BLANK

REQUEST FOR RESPONSE

California Penal Code Sections[1] §933(c) and §933.05 requires a written response to all Recommendations contained in this Report which shall be made no later than ninety (90) days after the Civil Grand Jury publishes its Report (filed with the Clerk of the Court).

Respond to:

Presiding Judge
Los Angeles County Superior Court
Clara Shortridge Foltz Criminal Justice Center
210 West Temple Street,
Eleventh Floor, Room 11-506
Los Angeles, CA 90012

All responses for the 2010 - 2011 CGJ Report's Recommendations must be submitted to the above address on or before the end of business **September 30, 2011.**

Responses are required from:

Recommendation Number(s)	Responding Agency
1, 2, 3 and 4	City of Long Beach

[1] Reference California Penal Code Sections §933(c) and §933.05 at the beginning of this 2010-2011 Civil Grand Jury Report

THIS PAGE INTENTIONALLY LEFT BLANK

E-SUBPOENA
ONE WAY TO END THE PAPER CHASE

Committee Members

Chairperson: Joseph H. Safier
John A. Rangel
Susan Stetson

E-SUBPOENA
ONE WAY TO END THE PAPER CHASE

SUMMARY

Annually, Los Angeles County prosecutorial and defense agencies serve hundreds of thousands of subpoenas on law enforcement agency personnel. The e-Subpoena system automates this process including tracking of receipt, thereby saving time, money and resources. This Report describes the system, summarizes its implementation to date and makes recommendations to advance the program.

PURPOSE

The 2010-2011 Civil Grand Jury (CGJ) examined the electronic subpoena distribution process (e-Subpoena) for law enforcement agencies (LEAs). The objective was to understand the process, the current state of implementation and the costs and benefits for the Los Angeles District Attorney's Office (DA) and related LEAs.

BACKGROUND

During calendar year 2010, the DA issued 358,900 subpoenas to law enforcement personnel to appear in court. Approximately 35% were served on Los Angeles Police officers and 26% on Los Angeles Sheriff's deputies. Personnel in one hundred sixty-five (165) different agencies received subpoenas. The volume of paper and associated tracking involved time consuming manual effort, both for the DA as well as the agencies receiving the subpoenas.

When an arrest is made, prosecutors have a limited time to charge, arraign and conduct a preliminary hearing. Generally, arraignments must be held within forty-eight (48) hours of arrest with the preliminary hearing conducted within ten (10) days of arraignment. The arresting and investigating law enforcement officers must testify at the preliminary hearing. Subpoenas are the legal document requiring an officer to appear in court. In the event an officer does not appear in court, the defendant must be released unless the prosecuting agency files a new set of charges. Most of the problems with subpoenas deal with preliminary hearings where the time window for reaching an officer is limited. In addition, civilians and some law enforcement personnel are served with paper subpoenas.

One of the law enforcement agency complaints is that many officers are being subpoenaed. When paper subpoenas are delivered and hand distributed, the DA has no timely confirmation of who is served. For example, if six (6) officers investigate a crime, unless the prosecutor knows the lead officer receives their subpoena, the DA often sends to all six (6) officers involved. E-Subpoena increases accountability by ensuring the specific officer is served, thereby obviating the need for the other five (5) officers to appear in court. This new system also permits law enforcement management to track offending officers with a history of missed hearings or who intentionally run up court appearance overtime. Previously, such officers could not be disciplined, as the agency had no knowledge of officers who were abusing the system. In addition, e-Subpoena eliminates delays and missed deliveries if an officer moves between departments or offices within an agency.

METHODS AND PROCEDURES

The CGJ reviewed DA prepared e-Subpoena presentation materials, an overview of the County's Information Systems Advisory Board (ISAB), Proactive Information Exchange (PIX) system, and several LEA e-Subpoena Policy/Procedure statements. The CGJ analyzed statistics of subpoenas issued by the DA during 2010 and prepared a Report of LEAs in descending order of number of subpoenas received. In addition, CGJ members met or spoke with representatives of the DA, ISAB and the following LEAs and City Attorneys to discuss the system:

1. Los Angeles Sheriffs Department (LASD)
2. Los Angeles Police Department (LAPD)
3. City of Alhambra Police Department
4. City of Bell Police Department
5. City of Bell Gardens Police Department
6. City of Beverly Hills Police Department
7. City of Burbank Police Department
8. City of Covina Police Department
9. City of Culver City Police Department
10. City of Gardena Police Department
11. City of Glendale Police Department
12. City of Glendora Police Department
13. City of Huntington Park Police Department
14. City of Inglewood Police Department
15. City of Inglewood City Attorney
16. City of Long Beach Police Department
17. City of Los Angeles Fire Department
18. City of Los Angeles Unified School District School Police
19. City of Manhattan Beach Police Department
20. City of Monrovia Police Department
21. City of Monterey Park Police Department
22. City of Pasadena Police Department
23. City of Redondo Beach Police Department
24. City of San Fernando Police Department
25. City of San Gabriel Police Department
26. City of South Pasadena Police Department
27. City of Torrance Police Department
28. City of West Covina Police Department
29. City of Whittier Police Department

FINDINGS

1. The e-Subpoena system provides prosecutorial and defense agencies with an automated means to serve law enforcement officers. Currently, the following agencies use the system:

    a. District Attorney's Office

    b. Alternate Public Defender (APD)[1]

    The Los Angeles Public Defender is developing this capability.

2. The Los Angeles City Attorney and Long Beach City Prosecutor also electronically subpoena officers, but their requests are sent internally with their respective cities' systems. To the CGJ's knowledge, most other City Attorneys/City Prosecutors are using paper based subpoenas.

3. E-Subpoena is a means of delivering subpoenas to law enforcement personnel throughout the County electronically and receiving "proof of service" automatically. Prior to development of e-Subpoena, subpoenas were either mailed, hand carried or sent to the Justice Data Interface Controller (JDIC) printer at the law enforcement agency. This method was slow and did not provide the DA with proof that the officer/deputy was served.

4. The e-Subpoena process begins when a Deputy DA or APD inputs in their respective Case Management System (CMS) when an officer is needed in court on a specific date and time. CMS generates an electronic message to the officer. Although more complicated, this is essentially an e-mail. The message is sent to PIX, which then routes the message to the law enforcement agency. Depending upon the technology used by the law enforcement agency when delivering the message to the officer, a "proof of service" is returned via PIX to the originator when:

    a. The officer opens their e-mail

    b. The officer positively responds that they received it

    PIX provides the secure system for sending and receiving messages among agencies.

    The system is also used to notify an officer when they are no longer needed to appear and/or for rescheduling.

    JDIC-received and paper subpoenas are manually logged and tracked by the law enforcement agency, and no automated "proof of service" is returned to the originator.

    An overview provided by the DA describes the system benefits:

    a. More reliable than paper and regular e-mail

    b. Complete logging of delivery and receipt

[1] The Alternate Public Defender is Court-appointed counsel for indigent defendants who cannot be represented by the Public Defender because of a conflict of interest.

c. Improved control using case management systems versus ad hoc e-mail

d. PIX ensures reliable delivery/return receipt and a standard interface to different law enforcement agency systems

All DA, Public Defender, APD, and City Attorneys/City Prosecutors in the future can use the same message formats and delivery mechanisms.

5. E-Subpoena was started approximately five (5) years ago with LAPD.

6. Electronic notice of delivery and receipt occurs between PIX and the following agencies:

   a. LASD

   b. LAPD

   c. Long Beach Police Department

   d. Inglewood Police Department

   e. Culver City Police Department

   f. Montebello Police Department

   The last three (3) agencies on the preceding list use a third-party vendor that supply and maintain the technology for LEA delivery and receipt. At least one LEA reported that the implementation took one (1) month followed by a two (2) month period of running the systems in parallel. The biggest implementation problem encountered was officer resistance to change.

7. Additional benefits are:

   a. Electronic service reduces officer overtime from having to subpoena more officers than actually needed (blanket subpoenas) since the DA can now verify which officer(s) were served.

   b. With planned court closures, travel time as well as court overtime are reduced.

   c. Because the officer is positively served and will appear, the DA, Public Defender, and APD reduce their case continuance costs.

   d. Accuracy is improved through officer validation; the sender ensures that the correct officer is served.

   e. The law enforcement agency's subpoena control personnel can review and manage multiple requests more efficiently.

   f. Risk of loss of JDIC-printed or paper subpoenas is reduced.

   g. Follow-up phone calls are minimized.

   h. Formal audit trail of service is provided.

i. Management follow-up and auditing statistics are available.

8. E-Subpoena results in fewer continuances/dismissals, swifter justice for crime victims, decreased criminal case backlog, and potentially reduces incarceration time and costs.

9. Different internet standards are used by various agencies and a third-party vendor. For example, messaging protocol and identification standards exist but are not used consistently by all departments. Currently, PIX must convert e-subpoenas into at least four (4) different technologies in order to send them to different law enforcement agencies.

10. Although the CGJ could not locate the source of the information, it noted from public statements that e-Subpoena resulted in significant savings to LAPD in court overtime. LAPD representatives explained that due to the different components of court overtime (number of cases filed, number of officers subpoenaed, etc.), these savings could not be calculated precisely.

11. Several departments reported that court affairs/subpoena control personnel time spent performing subpoena control was reduced by 50%, freeing personnel to work on other critical department functions. In addition, the volume of paper and postage was reduced 50-65%.

12. Less manpower is needed to generate mail and manually track each subpoena. In larger departments, less time is spent locating officers who have been transferred.

13. Less time is spent attempting to determine if an officer was served.

14. In this time of municipal budget constraints, whatever can be done to streamline the process and reduce court overtime is desirable.

15. Ten (10) cities within the County use the City Attorney/City Prosecutor to prosecute misdemeanors[2]. In cities where e-Subpoena is installed, some City Attorneys/City Prosecutors are still issuing paper subpoenas.

16. Several departments that have implemented e-Subpoena encourage their officers to check e-mail on their days off, although requiring that may violate Fair Labor Standards Act de minimus rules.

17. One LEA that has not implemented e-Subpoena was concerned about the actual direct and indirect costs of the system.

18. A concern raised was the situation where an officer is subpoenaed at the last minute. In these cases, the subpoena control officer would be required to contact the subpoena recipient regardless of whether the department was using paper copies or e-Subpoena.

19. At least one LEA was concerned that their city was behind the technology curve and may not have the infrastructure to handle e-Subpoena.

[2] The District Attorney prosecutes misdemeanors, as well as felonies, for the remaining 78 cities as well as the unincorporated areas of the County.

20. The following is a Table of law enforcement agencies receiving at least one hundred fifty (150) subpoenas from the DA during the period October through December 2010 and their e-Subpoena implementation status:

LOS ANGELES DISTRICT ATTORNEY-ISSUED LAW ENFORCEMENT SUBPOENAS AGENCIES RECEIVING AT LEAST 150 SUBPOENAS FOR THE PERIOD OCTOBER THRU DECEMBER, 2010		
Agency	**No. Issued**	**e-Subpoena Status**
CALIFORNIA HIGHWAY PATROL	2,128	Interested
PASADENA POLICE DEPARTMENT	988	
GLENDALE POLICE DEPARTMENT	903	
HUNTINGTON PARK POLICE DEPARTMENT	685	
BURBANK POLICE DEPARTMENT	612	
HAWTHORNE POLICE DEPARTMENT	604	Interested
WHITTIER POLICE DEPARTMENT	593	
SANTA MONICA POLICE DEPARTMENT	537	In process
LASD - VARIOUS	515	Implemented
GARDENA POLICE DEPARTMENT	501	
DOWNEY POLICE DEPARTMENT	490	Interested
EL MONTE POLICE DEPARTMENT	474	Interested
POMONA POLICE DEPARTMENT	456	Interested
ALHAMBRA POLICE DEPARTMENT	433	
L. A. CITY FIRE DEPARTMENT	422	
SOUTH GATE POLICE DEPARTMENT	421	Interested
TORRANCE POLICE DEPARTMENT	403	
MONTEREY PARK POLICE DEPARTMENT	366	
WEST COVINA POLICE DEPARTMENT	364	
L. A. UNIFIED SCHOOL DISTRICT PD	318	
L. A. COUNTY CORONER	300	Interested
EL SEGUNDO POLICE DEPARTMENT	274	Interested
MONTEBELLO POLICE DEPARTMENT	271	In process
L. A. COUNTY PROBATION	255	Interested
SAN FERNANDO POLICE DEPARTMENT	216	
MANHATTAN BEACH POLICE DEPARTMENT	189	
BEVERLY HILLS POLICE DEPARTMENT	182	
COVINA POLICE DEPARTMENT	176	
MONROVIA POLICE DEPARTMENT	168	
GLENDORA POLICE DEPARTMENT	163	
SAN GABRIEL POLICE DEPARTMENT	163	
BELL GARDENS POLICE DEPARTMENT	159	
REDONDO BEACH POLICE DEPARTMENT	159	
BELL POLICE DEPARTMENT	157	
LAPD – VARIOUS	155	Implemented
SOUTH PASADENA POLICE DEPARTMENT	154	

RECOMMENDATIONS

1. Implement e-Subpoena as a cost saving and operational efficiency measure for local law enforcement agencies receiving at least one hundred fifty (150) DA subpoenas quarterly.
2. Encourage the City Attorney/City Prosecutor to use the system in cities where the Police Department is using e-Subpoena.
3. LASD and LAPD evaluate electronically transmitting other documents such as police reports and probable cause determinations[3] among law enforcement agencies, prosecutors and the Court.
4. LASD to expand implementation of filing Pitchess motions electronically. A Pitchess motion defines those portions of a deputy's personnel file which may be made available to defense counsel.
5. The DA staff is encouraged to conduct an e-Subpoena training class for court liaison/subpoena control officers and encourage departments still receiving paper subpoenas to implement e-Subpoena.

REQUEST FOR RESPONSE

California Penal Code Sections[4] §933(c) and §933.05 requires a written response to all Recommendations contained in this Report which shall be made no later than ninety (90) days after the Civil Grand Jury publishes its Report (filed with the Clerk of the Court).

Respond to:

Presiding Judge
Los Angeles County Superior Court
Clara Shortridge Foltz Criminal Justice Center
210 West Temple Street,
Eleventh Floor, Room 11-506
Los Angeles, CA 90012

All responses for the 2010 - 2011 CGJ Report's Recommendations must be submitted to the above address on or before the end of business **September 30, 2011.**

Responses are required from:

Recommendation Number(s)	Responding Agency
1	City of Alhambra (Police Department)
	City of Bell (Police Department)
	City of Bell Gardens (Police Department)
	City of Beverly Hills (Police Department)
	City of Burbank (Police Department)

[3] Probable Cause determination is a LEA prepared, Court approved document which permits an agency to detain a suspect.
[4] Reference California Penal Code Sections §933(c) and §933.05 at the beginning of this 2010-2011 Civil Grand Jury Report

City of Covina (Police Department)
City of Gardena (Police Department)
City of Glendale (Police Department)
City of Glendora (Police Department)
City of Huntington Park (Police Department)
City of Los Angeles Fire Department
City of Los Angeles Unified School District (School Police)
City of Manhattan Beach (Police Department)
City of Monrovia (Police Department)
City of Monterey Park (Police Department)
City of Pasadena (Police Department)
City of Redondo Beach (Police Department)
City of San Fernando (Police Department)
City of San Gabriel (Police Department)
City of South Pasadena (Police Department)
City of Torrance (Police Department)
City of West Covina (Police Department)
City of Whittier (Police Department)

2 City of Inglewood (City Attorney)

3 City of Los Angeles (Police Department)
County of Los Angeles (Sheriffs Department)

4 County of Los Angeles (Sheriffs Department)

5 County of Los Angeles (District Attorney)

Acronyms

APD	Alternate Public Defender
CGJ	Los Angeles County Civil Grand Jury
CMS	Case Management System
DA	Los Angeles District Attorney's Office
ISAB	Los Angeles County Information Systems Advisory Board
JDIC	Justice Data Interface Controller
LAPD	Los Angeles Police Department
LASD	Los Angeles Sheriffs Department
LEA	Law enforcement Agency
PIX	Proactive Information Exchange

THIS PAGE INTENTIONALLY LEFT BLANK

HIGH TECH FORENSICS AND CYBER SECURITY CRIME FIGHTING IN THE DIGITAL AGE

"We have to do better at what we do.
Our public deserves it."

Committee Members

Chairperson - Meg George
Grace Hernandez
Beverly T. Kishimoto
Max E. Van Doren

HIGH TECH FORENSICS AND CYBER SECURITY
CRIME FIGHTING IN THE DIGITAL AGE

"We have to do better at what we do.
Our public deserves it."[1]

SUMMARY

The use of digital evidence to successfully prosecute crimes is becoming critically important. In part, this is due to the proliferation in the use of digital devices. Specific training in the collection and processing of digital evidence is needed, as is the acquisition of the hardware and software required to analyze the evidence.

Computers, cell phones and other digital devices are increasingly intertwined with the commission of crimes, raising the importance of the resources and priority that must be given to cyber security, cyber investigations and high tech forensic[2] examinations to provide public safety. These cyber and forensic services are provided within Los Angeles County (LAC) and its cities by regional high tech crimes task forces (RTFs) (RTFs cover more than one county.), local high tech crimes task forces, police department high tech forensic labs or through private companies. In addition seventeen (17) municipal police agencies have some in-house high tech forensic crime capability. LAC is home to critical infrastructure, businesses and industries that are vulnerable to cyber attack. It must be in a position to provide response support to such attacks, so that such business and industry will identify Los Angeles as a safe and welcoming place to locate.

Those who harm us (be it crooks, cyber terrorists, or nation-states) are highly motivated and continuously improving. To counter this assault effectively we must be highly motivated and continuously improving to be effective in the efforts to: provide public safety, catch the perpetrators and successfully prosecute them. This requires vision, commitment, equipment, training and resources.

Technology is evolving at a rapid pace requiring frequent upgrades to equipment, software and training. Funding of high tech forensics, cyber investigation and cyber security in LAC has largely been through government transfers (grants from State and Federal programs). This source of funding has been decreasing and continues to be under pressure due to continuing cuts and constraints.

Borrowing the endowment concept from the University system, a possible new source of funding might be the establishment within law enforcement of a High Tech Forensics Examination – Cyber Investigations – Cyber Badge Endowment Program (Endowed Badge). The Endowed Badge (EB) would be awarded on a rotating basis. Funding of each EB would be through a public private partnership, and the EB could be named by the benefactor; e.g., Port of Los Angeles EB, Apple EB, Harry Potter EB, Warner Brothers EB, Wells Fargo EB, Exxon EB, DWP EB, etc. Business and industry has a vested interest in a safe City/County in which to do business; hence, there may be interest from many sectors to participate in funding an EB and

[1] Graham, Gordon "Affairs in Government 2010. Some Thoughts on Risk Management," December 3, 2010
[2] In the Report, High Tech Forensics concerns digital information; it does not include DNA or fingerprint analysis

naming one of the EBs. Eight (8) initial Endowed Badges are visualized. The eight (8) are comprised of five (5) EBs where each LAC Board of Supervisors District sets up and oversees the public-private partnership funding; plus three (3) EBs, where each of the City of Los Angeles Proprietary Departments (Department Of Water and Power, Port of Los Angeles, Los Angeles International Airport (LAWA)) sets up and oversees the public-private partnership funding for a total of eight (8) EBs.

The EB concept is to use a combination of government and private funds to pay for training of sworn officers in the arena of high tech forensics-cyber investigations and cyber security. There are legal issues to explore and logistical issues to analyze. The example of the partnership between Los Angeles and Microsoft in the area of fighting piracy may provide insight of a process to be followed.

PURPOSE

The Civil Grand Jury (CGJ) investigated the level of engagement and commitment of government entities within LAC in the prevention and prosecution of high tech crimes, as well as in the use of digital evidence in crime fighting efforts. Computers, cell phones and other digital devices are increasingly intertwined with the commission of crimes, raising the importance of resources and priority that must be given to cyber security, cyber investigations and high tech forensic examinations to provide public safety. In view of the shrinking budgets at all government levels, this Report recommends how to sustain the current level of cyber security, cyber investigations and high tech forensic examinations in the County and cities, while further developing the capability and staying ahead of the curve.

BACKGROUND

The amount of data storage available on a thumb drive, cell phone, iPad, laptop computer or desk top computer, is huge and growing. Cell phones alone can store upwards of eight (8) gigabytes of data; hard drives have moved into the realm of terabytes (Appendix A). Text, accountings, data, photographs, video, GPS (global positioning system), contacts and more information may be stored on these devices. Additionally, there are mainframes and clouds.

Task Forces and Forensic Laboratories

In 1998 the State of California established five (5) RTFs to address the growing threat of high tech crime. California is home to many industries which are vulnerable to theft of trade secrets, copyrights, patent infringements, and pirating (think bank accounts, credit cards, medical history, software, music, film, auto engineering, energy, defense, fashion, etc.). Statistics indicate that California is also home to many perpetrators of cyber crime including, but not limited to, child pornography, cyber stalking, cyber bullying, cyber preying on children, consumer fraud, cyber intrusion, pirating, and identity theft. Commonly, digital evidence is available for collection and use in cyber crimes and “old school” crimes as well. Murderers, arsonists, rapists, burglars, robbers and drunk drivers, to name a few, regularly own and use cell phones and computers. Criminals use the same digital devices in both their daily routines and illegal enterprises.

Use of digital devices[3] in the perpetration of crime facilitates the commission of crimes across jurisdictional boundaries. The RTF model embraces this aspect by creating a structure in which local detectives (sheriff, police) work in a structure that includes State law enforcement (Highway Patrol, California Department of Justice) and Federal law enforcement (U. S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS)[4] including the Secret Service, Federal Bureau of Investigation (FBI)). Prosecutors from the local, State and Federal level are also a part of the mix. In addition, a partnership with industry through regular forums facilitates the flow of information. This RTF structure facilitates mutual aid, learning, and the leveraging of limited resources to maximum advantages.

The joint task force model provides a framework for a collaborative crime fighting environment. In this way, the resources of the participants are combined to effectively and efficiently make a significant impact on electronic crimes. Digital evidence is used to fight high tech crime and solve "old school" crime. These pockets of expertise also place an emphasis on prevention and education, in addition to traditional law enforcement measures. This blend of law enforcement agencies brings additional criminal enforcement jurisdiction and resources to the task force while representatives from private industry bring a wealth of technical expertise.

Cyber Security, Cyber Investigations and High Tech Forensic Examinations

An FBI official has said that disruption of the internet was the greatest active risk to the U.S. "other than a weapon of mass destruction or a bomb in one of our major cities." According to a Los Angeles (LA) Times,[5] article, "US officials say China already has laced the US power grid and other systems with hidden malware that could be activated to devastating effect."

In the LA Times article, it was reported that a large Southern California water system hired a Los Angeles based hacker to probe the vulnerability of its computer network. The "hacker" and his team "seized control of the equipment that added chemical treatments to the drinking water - in one day." The "door" they used to get into the system was there because employees had been logging on to the water system computers from their home computers. This simple convenience left a "gaping security hole." This commandeered system is the same or similar to systems controlling electrical grids, pipelines, chemical plants and other infrastructure. This type of threat can be viewed as having the potential for a "virtual" war.

Attacks via the internet on infrastructure to compromise secure information, or to "crash" a site and cause "denial of service" are the realm of cyber security.[6] (See Appendix B for a brief description of "WEB or Internet How it Works.") Being proactive and preventing the intrusion is the goal. Reacting, limiting and fixing the damage is also a reality. Besides trying to identify, catch and prosecute such intrusion perpetrators (hackers or cyber terrorists) responses usually entail detection of the intrusion, stopping the progress of the intruder, mitigating damage done, and improving defenses to prevent a similar breach. Attacks via the internet pose a tricky

[3] Cell phones, computers, pads, gps, etc.

[4] Departments, funding and training formally part of DOJ may have moved to DHS

[5] Los Angeles Times, *It's Warfare at the Click of a Mouse*, page A1, March 28, 2011, Ken Dilanian

[6] When WikiLeaks released classified U.S. Government documents in December 2010 it sparked several rounds of online conflict. WikiLeaks became the target of denial of service attack, lost the support of its posting and payment providers. This in turn inspired sympathizers to counterattack, briefly bringing down the sites of MasterCard and a few other companies. Sites related to the hackers were then attacked. Mirror sites sprang up claiming to host copies of the wikileaks documents--some were said to carry viruses ready to take over the machines of those who downloaded copies. (Scientific American, March 2011, J. Zittrain).

problem in that it is often impossible to trace an attack back to its instigator. This instigator may be in the building, down the street, in another county, state, or country.
Cell phones differ. With cell phones, the telecom operator can tell which phone placed a call and to whom the phone is registered. Even with "throw away" cell phones some information is available. Establishing the same level of identity on the internet is a far harder charge.

Whether in high tech crimes or "old school" crimes, digital evidence is relevant. Collection, chain of custody, targeted analysis and expert witness testimony all require specialized training. Analysis requires special equipment and software which must be regularly updated. Digital evidence, like a smoking gun or DNA, should be collected and used in fighting crime, not left unused.

What has the CGJ to offer with its limited jurisdiction of government entities within the County boundaries? Indeed! All crime has a victim, and that victim(s) is located somewhere. LAC and its cities, businesses and industry rely on and provide critical infrastructure, from the basics of water and power to banking, ports, refiners, healthcare, and justice. When the cyber breach or crime occurs in LAC, first responders may well be local law enforcement agencies.

When a crime is committed in LAC, it is likely that local patrol officers and detectives investigating the scene collect both physical and digital evidence for further evaluation. If this first step leaves the digital evidence uncollected, it is then unavailable to help solve the crime, get the perpetrator(s) off the street before they commit additional crimes and provide justice to the victim(s). If evidence is collected, but not analyzed in a timely manner which maintains a chain of custody and preserves the evidence integrity for use in court, again the use and benefit of the evidence is lost. In order for punishment, and therefore deterrence, to be even possible digital data must be collected, processed, analyzed, and used.

If there is a cyber security breach, are the protocols, policies and procedures in place for rapid response by the most able cyber security resources available? Is it sufficient in some places, better in others and mediocre to poor everywhere else? This type of information, by its nature, is highly classified and is not available to the CGJ for investigation. This is as it should be. However, cyber attacks have the potential to "blow up city blocks, erase bank data, crash planes and cut power to large areas of the country."[7] Hence the question: Is there a plan? Does LAC 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? Are there regular reviews, updates, and modifications in this fast moving area? Is there a clear blueprint as to who is accountable for what?

Complacency in this arena is dangerous. According to a 2011 article in the Federal Times[8] the 2002 Federal Information Security Management Act (FISMA) is in need of updating. The article opines that agencies that rely on "old" law compliance as a measure of sufficient preparedness are embracing a false sense of security. In 2002 most "cyber attackers were teenagers looking for amusement or notoriety"[5] ... In 2011 most cyber "attackers are criminal organizations and nation states that work hard to evolve their methods."[5]

For example, in October 2010, the Nasdaq[9] computers were breached. This breach was not disclosed to the public until February 2011. Then, in March 2011 it was announced that NSA was joining the FBI and Secret Service in the investigation. See Appendix C for more on this

[7] ibid., LA Times
[8] Federal Times, p. 23, *Outdated FISMA Threatens Cyber security*, March 7, 2011
[9] Nasdaq, formally known as "**N**ational **A**ssociation of **S**ecurities **D**ealers **A**utomated **Q**uotations" (NASDAQ)

cyber intrusion. Cyber threats have evolved since 2002 and so too must our planning and defenses.
There are six (6) traditional funding sources for government:

1. Sales tax
2. Property tax
3. Fees
4. Government transfers (grants)
5. Reserves
6. Bonding

Most of these funding sources are shrinking as of the writing of this report. Some of the existing fees and taxes, such as land line phone taxes and fees, cell phones or internet access fees or taxes might be better purposed in the twenty-first century to high tech forensics cyber security and forensic examination program support. Grant funds to support this ever growing need must be given high priority.

High Tech Crimes Task Forces and Labs

Los Angeles County and its cities host three (3) regional high tech crime task forces (RTFs). (RTFs cover more than one county.) In addition LAC based law enforcement agencies can avail themselves of high tech forensics support from the FBI Regional Computer Forensics Laboratory in Orange County. Regional task forces are comprised of officers from multiple jurisdictions, frequently including officers from Federal, State and local agencies. In addition, the LAC District Attorney has a High Tech Crime lab and seventeen (17) municipal police agencies have in-house high tech forensic crime investigation capability.

Regional High Tech Crimes Task Forces

1. The Southern California High Tech Task Force (SCHTTF):
    a. SCHTTF is one of five (5) RTFs established by The California State legislature. These RTFs are located throughout the State of California:
        i. California High Technology Crimes Task Force strategy was created through Senate Bill 1734 in 1998. Five (5) task forces were created and located strategically throughout the state, they are:
            - Northern California Computer Crimes Task Force (NC[3] TF) Lead Agency: Marin County District Attorney's Office
            - Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF) Lead Agency: Sacramento Sheriff's Department
            - Rapid Enforcement Allied Computer Team (REACT), Lead Agency: Santa Clara District Attorney's Office
            - Southern California High Tech Task Force (SCHTTF), Lead Agency: Los Angeles Sheriff's Department
            - Computer and Technology Crime High-Tech Response Team (CATCH), Lead Agency: San Diego District Attorney's Office