California Law Enforcement Telecommunications System (CLETS)
Advisory Committee (CAC)
Meeting Minutes (Unapproved)

March 21, 2013
California Highway Patrol Headquarters, Sacramento

Present: Chair: Sam Spiegel (California Peace Officers' Association)

Members: Cuong Nguyen (Department of Justice), Marc Shaw (California Peace Officers' Association), Larry Spikes (California State Association of Counties), Scott Silsbee (California Highway Patrol), Scott Marshall (California State Sheriffs' Association), Karen Wong (Department of General Services/California Technology Agency), Steve Westerman (Department of Motor Vehicles), Cynthia Renaud (California Police Chiefs Association)
Maria Cranston (CLETS Executive Secretary)

Absent: Evert Palmer (League of California Cities)

CALL TO ORDER – Chair Sam Spiegel called the meeting to order at 10:03 a.m.

ROLL CALL – CLETS Executive Secretary Maria Cranston called roll. A quorum was present.

APPROVAL OF MINUTES – A motion was made to approve the minutes from the meeting of November 14, 2012.

Motion:	Larry Spikes
Second:	Scott Marshall
Vote:	Approved unanimously

CHAIR'S REPORT (Sam Spiegel)

a. The chair read a brief biography and introduced new committee member Cynthia Renaud, representing the California Police Chiefs Association.

b. Reconstitution of the Standing Strategic Planning Subcommittee (SSPS)

1. History and Purpose

Maria Cranston provided a brief history of the SSPS, which dates to 1996, when then-CAC Chair Bud Hawkins established the committee because he had concerns with the increasing flow of legislation and rapidly changing technology was creating separate nonintegrated systems, which were all competing for the same dollars and resources. Mr. Hawkins wanted to project the CLETS operation into

2001. In 1996, a think tank was formed and several issues were identified by an ad hoc steering committee, which later became a permanent standing subcommittee, renamed the Standing Strategic Planning Subcommittee, or SSPS.

The SSPS' goal was to evaluate pertinent legislative and technical environments of CLETS and to make timely recommendations, perform planning functions as directed by the CLETS Advisory Committee, as well as to update the CLETS Strategic Plan as needed. In 2008, the CAC voted to adopt and be a part of Vision 2015, a DOJ-hosted project involving the collaboration of criminal justice information and various law enforcement partners. Since then, the SSPS has continued to exist, but was only to meet to provide a forum for discussing specific CLETS policies and issues and to develop recommendations to go before the committee. Three working groups – legislative, technical and administrative – were originally created to provide law enforcement input. The groups were also to convene as needed, but with Vision 2015 there became more of a need to reach out to other forums and participate among other information-sharing networks.

2. Vision and Mission, Moving Forward (Sam Spiegel and Cuong Nguyen)

Chair Spiegel noted he was a charter member of the SSPS, which ensured CLETS met the needs of the community. Over the last several months since Cuong Nguyen became the CJIS director, it was evident the ever-changing technology created the necessity for a working group to bifurcate different issues and make recommendations to the CAC. This way, the Subcommittee would be at the forefront of changing technology, rather than being constantly reactive. At the time Vision 2015 was constituted, it was a laudable program, Chair Spiegel said and with new CAC members, Chair Spiegel believed it was time the SSPS be reinstituted and perhaps assume even a larger role. Sam Spiegel asked CAC members for recommendations to the SSPS, which serves at the will of the chair, without a numerical limit. Director Nguyen also served as a charter SSPS member and said the Subcommittee can be vital to understand future law enforcement needs. SSPS recommendations can formulate decisions that need to be made by the CAC. Despite today's funding constraints, Director Nguyen said it is important SSPS recommendations be prioritized.

EXECUTIVE SECRETARY'S REPORT (Maria Cranston)

a. **Action Items**

1. The CLETS Policies, Practices and Procedures (PPP) should be amended to be compatible with the FBI CJIS Security Policy. *Result: The PPP were amended to conform; both a clean copy and a strikeout version are included in members' folders, and the revised PPP will be voted on later during the meeting.*
2. Scott Marshall to contact the Los Angeles County Sheriff regarding password compliance. *LASD expects to be compliant by July 2013. This issue will be further discussed in client report section.*

3. Scott Marshall to contact the San Francisco County Sheriff regarding an implementation plan that would include Security Awareness for IT and private contractor personnel; advance authentication for the agency's laptops; and encryption that would meet National Institute of Standards and Technology certification in accordance with FIPS 140-2 standards on segments utilizing public, wireless and Internet network segments transmitting criminal justice data. *An Implementation Plan to resolve the outstanding issues has been received. This issue will be further discussed in client report section.*

b. **CLETS System Misuse Statistics**
Possible cases of CLETS misuse worked by the Department of Justice (DOJ) from December 2012 through March 20, 2013.

- Journal search requests 54
- Searches conducted 169
- Searches for possible misuse within own agency 111
- Searches for possible misuse for another agency 10
- Searches for other purposes 48

c. **CLETS Traffic Statistics (October through December 2012)**

	Inbound	Outbound
• Total messages	230,527,150	231,493,728
• Monthly average	76,842,383	77,164,576
• Peak day	3,161,725	3,077,258
• Peak hour	239,365	219,205

CLETS Inbound Traffic Statistics (October through December 2012)

- CLETS 100 percent
- CJIS 46 percent
- DMV 13 percent
- NCIC 6 percent
- Nlets 3 percent
- Miscellaneous 32 percent

d. **Legislative Report (Mark LeForestier)** – Marc LeForestier, Director of Legislative Affairs for the Attorney General's (AG) office, discussed the following bills that are significant elements of the AG's 2013 legislative package. They included firearms, electronic privacy, behavioral tracking, funding for the Controlled Substance Utilization Review and Evaluation System (CURES) and debt buyers regulation. These bills are summarized below.

Firearms

AG Kamala D. Harris' focus has been on the Armed Prohibitive Persons System, which emerged about 10 years ago when former AG Bill Lockyer wanted to take advantage of the state's robust criminal history system by cross-referencing firearms registry and mental health information databases. That process began in 2003, and information was circulated to local law enforcement agencies in the hope it would result in the retrieval of weapons from those already prohibited by

law from possessing weapons. Funding restraints for local law enforcement agencies did not allow that cross-referencing to materialize; thus, an inventory was created and the list of people prohibited from owning weapons began to grow. Former AG Jerry Brown created an enforcement team to start processing the inventory, but the amount continued to increase. When AG Harris took office, she made that issue a priority and now there are 33 agents dedicated to processing this inventory. Still, the amount continued to rise by approximately a dozen per month. Thus, the legislature has seen this issue as a focal point and two of the key state firearms bills are listed below:

1. SB 140 (Leno) – Firearms. This legislation, one of 45 pending firearms bills currently before the legislature, would provide an additional $24 million to the DOJ's Bureau of Firearms (BOF) for enforcement of California laws prohibiting people who have felony and violent misdemeanor convictions, domestic violence restraining orders and serious mental illnesses from possessing firearms. AG Harris also is supporting federal legislation by California Representative Mike Thompson, which through funding mechanisms of the U.S. Department of Justice encourages states to adopt systems to retrieve weapons from prohibited persons. The idea is to encourage other states to reinforce the prohibitions.

2. Bill No. To Be Determined. Under current law, the BOF has 10 days to conduct a background check, required in California, when someone attempts to purchase a weapon. The time frame is seen as a cooling-off period for someone who might purchase a weapon in anger, but also provides time for the state to do a background check. In many instances, however, the 10-day background period is not enough because there often is a disconnection between the potential buyer's arrests and dispositions. The DOJ has taken the position that if the background check is not completed in 10 days, no firearms permit will be issued. That is causing some dismay, and this legislation would extend the time allowed to the BOF to conduct background checks on applicants for firearms permits.

Electronic privacy

Currently there is nothing in existing law that would require an Internet provider to inform a reader that a password has been breached. Enforcement mechanisms have not been worked out, although they probably would reside with the AG's office.

- SB 46 (Corbett) – Privacy/Identity Theft. This legislation will require online service providers to notify users of any breach of a user's online password.

Behavioral tracking

- AB 370 (Muratsuchi) – Consumers: Online tracking. When using private browsing settings on a computer, a signal is sent to the Internet site indicating that preference. There is no legal requirement for such disclosure to be acknowledged. This legislation would require online service providers to inform users of the extent to which their online behavior is being tracked, how this information will be used, to whom they are selling and for what purposes.

CURES funding

- SB 809 (DeSaulnier) – Controlled substances: reporting. Since the 1940s, the U.S. DOJ has tracked prescriptions for controlled substances, originally in triplicate paper form and electronically for the last decade or so, through CURES. CURES information is obtained via the DOJ's Prescription Drug Monitoring Program (PDMP); however, budget cuts in 2011 eliminated funding for the PDMP, though it continued to exist. There is considerable support for this bill, and the DOJ is optimistic long-term, stable funding will be secured to maintain the CURES/PDMP for medical providers, pharmacists, the California Medical Board and law enforcement.

Debt Buyer Regulation

- SB 233 (Leno/Correa) – Debt buying. A version of this bill nearly passed last year, and there is considerable optimism for passage in 2013. This industry purchases large amounts of consumer debt, typically by the thousands from credit cards, and tries to negotiate with consumers for pennies on the dollar. Typically, information procured from the upstream seller is a spreadsheet with some digits that are physically undecipherable to anybody else and may not contain any real evidence. It seems for some of the large debt buyers, their model is to hope consumers do not actually respond to the collection efforts. Should that debt buyer tactic occur, there could be lawsuits filed against the consumer, the consumer will not show up in court and then there could be collection efforts on default judgments. This business practice is seen as unfair and there is attention on this nationally, including from the Federal Trade Commission. This bill would require that in addition to the debt being down-streamed, evidence of the debt also would need to be in the stream of commerce, with that debt. Subsequent debt buyers would need actual evidence of the debt before suing and being awarded judgments. The Judicial Council is in favor of establishing these standards, and the entire collection industry supports this bill.

Other bills of interest to the DOJ and its constituents include California Environmental Quality Act reform, underground economy legislation that is focused on information sharing across state agencies and dark money that showed up just before the November 2012 election.

UPDATE: ASSEMBLY BILL 391 (Adrian Farley, Chief Information Officer, CJIS) – AB 391 was geared toward connecting various systems that exist across municipalities and then consolidating them in a statewide manner relating to the information of pawned items. The bill's objective was to automate pawned information. Currently, pawn shops and secondhand dealers are required to keep information about pawned items for five years, costing them $14,000 to $100,000 a month, according to the industry. The second goal was to establish a statewide repository of pawned information, which would further enable law enforcement agencies to perform advanced investigative capabilities. The project will be approved by the Department of Finance and the California Technology Agency in April 2013. In May, business requirements will be finalized. Procurement will be completed and a contract will be awarded after the budget is passed and signed by the governor, anticipated to be in July. The solution development process will continue from July through September. Testing of the solution and training will begin in October and in December, the solution will be implemented. So far, more than $700,000 has

been collected; at the end of 2012, less than 2,500 pawnbrokers and secondhand dealers had made their payments. Just above 50 percent of the dealers has complied so far. Chair Spiegel, noting DOJ had provided an updated compliance list, said it was the responsibility of law enforcement agencies, not the DOJ, to oversee compliance.

UPDATE: ASSEMBLY BILL 109 (Adrian Farley) – As a result of the Criminal Justice Realignment Act, or AB 109, which chaptered in 2011, a statewide data-sharing initiative was developed to focus on providing, collecting and enhancing data relating to the population released from the state's correctional facilities.

After receiving information from law enforcement and other interested stakeholders across the state, in January 2013 the AG convened a meeting to determine how to better share data about the realigned population. Specifically, the goal was to determine where the released population is, what the conditions of their release are and how the existing data are reconciled. The effects of AB 109 illustrate the opportunity for statewide data systems to coexist with local law enforcement agency's systems, rather than existing as silos as is presently the case, especially when disconnections have public safety repercussions. AB 109 offers an attempt to achieve a broader platform for information sharing.

The DOJ wants to leverage its current investments and assets, rather than discarding what it has, and will work with a vendor to build, through tunneling, to connect all the systems. The top priority, according to law enforcement, should be training rather than creating another system. In terms of core capabilities, the DOJ will focus on integrating state, regional and local data, and will provide web portal access for those agencies that do not have it and will provide analytic and investigative capabilities. Ultimately, this will serve as a data informational exchange with a portal to access the information that connects state, regional and local systems, with an initial focus on those who were realigned or are on some type of post release community supervision (PRCS). The first phase of the project, scheduled to be finished this summer, is focused on data enhancement and how accuracy, completeness and timeliness are assured. The second phase has two components, the first of which focuses on the realigned population, and relates to data access and integration, and the second component is the statewide sharing solution.

A pilot should be available by the fall, and the solution should be available by December.

GUIDELINES FOR MOBILE DEVICES (Adrian Farley) – Relating to smart phones, this global trend is referred to as the consumerization of information technology. Given the questions DOJ receives from law enforcement agencies about proceeding securely, the DOJ has defined a security framework for accessing criminal justice information for mobile devices.

The Federal Bureau of Investigation (FBI) CJIS Security Policy is used as a foundation, but the process is an interlocked chain that begins with mobile device management, continues on to advanced authentication, requires data encryption (both in transit and at rest) and finally requires secured connectivity. Mobile device management is a way to control network traffic to and from a device, detect and eradicate malware on the mobile device and to enforce policy settings as well as implement incident response reporting to deactivation protocol should the device be lost or stolen. The policy and its specifics are on the CLEW website and the DOJ is working closely with several criminal justice agencies, including the San Francisco Police Department and San Diego Sheriff, on how to implement mobile device management.

Agencies having questions about how they might proceed with something new (new technology) should begin by contacting the CLETS Administration Section, prior to submitting the application. The DOJ will convene a group of experts to aid the inquiring agency in the process, since there are several security issues not regulated by the FBI or DOJ security policies. This will assist the agency while they are completing the application. *A handout has been included in each member's folder.*

CLETS POLICIES, PRACTICES AND PROCEDURES (PPP) REVISIONS – CLETS Executive Secretary Maria Cranston spoke briefly about the intent of the revisions, which included removing technical security requirements and instead referring to the FBI CJIS Security Policy. A motion was made to accept the PPP revisions as a whole.

Motion:	Larry Spikes
Second:	Scott Silsbee
Vote:	Approved unanimously

MHZ BROADBAND SPECTRUM NETWORK – (Karen Wong, Public Safety Communications Office) – The Middle Class Tax Relief and Job Creation Act of 2012, signed by the President in February of that year, reallocated the 10-MegaHertz (MHz) portion of the 700-MHz radio spectrum, known as the D-Block, to public safety. The D-Block refers to the portion of the electromagnetic spectrum between the frequencies from 758 MHz to 763 and from 788 MHz to 793. Seven billion dollars is designated from auction proceeds for the build out of the network, funding will be come from future Federal Communications Commission auctions of other radio frequency spectrums. However, that amount is not enough for a nationwide public safety broadband network, so other funding sources will be needed to determine how the network will be funded.

Planning for the build out of the network has begun, the State and Local Implementation Grant Program Application process identified California qualified for $5.8 million, California qualified for the second-highest allocation in the nation (Texas' allocation is $6 million). The grant request was submitted and the outcome should be announced in the early summer. In addition, it is too early to determine if the state should participate through the First Responder Network Authority (FirstNet) or try to deploy its own interoperable network after seeking a waiver. Ideally, the program would be complete enough so that when first responders arrive on scene, they would have a patient's medical information at their immediate disposal. *For more details, see the attached power point presentation.*

UPGRADE APPLICATIONS APPROVED BY THE DOJ

Upgrade Service – Chair Spiegel referred the Committee to the seven upgrade applications. These applications were not voted on, as they were approved by DOJ management, and are being presented for informational purposes only.

a. Los Gatos/Monte Sereno Police Department (Santa Clara County)
b. Oakland Police Department (Alameda County)
c. National Parks Service, Sequoia/Kings Canyon National Parks (Tulare County)
d. San Diego County Sheriff's Department (San Diego County)
e. San Joaquin County Sheriff's Department (San Joaquin County)
f. Sunnyvale Department of Public Safety (Santa Clara County)
g. Ventura County Sheriff's Department (Ventura County)

NEW SERVICE APPLICATIONS CALENDAR – Chair Spiegel referred the Committee to the three new service applications. Each application was voted on individually.

a. **CN-01 – Saddleback College PD (Orange County)** – CAS analyst Michelle Mitchell said the department is the primary uniformed law enforcement agency for the college campus. The agency has statutory law enforcement authority, which includes full arrest powers, authority to carry concealed weapons, authority to execute search warrants and conduct criminal investigations. Staff recommends for approval pending DOJ technical review. A motion was made to accept the application.

Motion:	Marc Shaw
Second:	Cuong Nguyen
Vote:	Approved unanimously

b. **CN-02 – Central Marin Police Authority (Marin County)** – CAS analyst Dave Sutherland said the agency provides first response to emergencies and other threats to public safety, protection to public facilities and maintains public order. Staff recommends approval, pending DOJ technical review. A motion was made to accept the application.

Motion:	Scott Marshall
Second:	Karen Wong
Vote:	Approved unanimously

c. **CN-03 – Sacramento City Attorney (Sacramento County)** – As the City Attorney for the City of Sacramento, the office serves as the legal advisor to the city of Sacramento and as the prosecuting city attorney charged with prosecuting all Sacramento city code violations, including criminal misdemeanors and infractions. Staff recommendation was changed to approval as DOJ technical review completed its review and had no concerns.

Motion:	Scott Marshall
Second:	Marc Shaw
Vote:	Approved unanimously

UPGRADE APPLICATIONS (NEW TECHNOLOGY)

a. **CU-01 – San Gabriel Police Department (Los Angeles County)** – CAS analyst Teresa Mora reported the agency was seeking expansion of mobile access to include the use of a handheld devices outside of the mobile unit and to upgrade the encryption module for mobile access to use Netmotion VPN over the Internet. This application proposes to use technology that has not previously been approved by the CAC and thereby requires the application be brought forward to the CAC for approval. The new technology proposed is the use of an Android-based tablet. The solution meets the FBI CJIS Security Policy including required Advanced Authentication. The DOJ Network Information Security Unit has reviewed this upgrade application and has no concerns to report. Staff recommends approval. A motion was made to approve the application.

Motion:	Scott Silsbee
Second:	Scott Marshall
Vote:	Approved unanimously

b. **CU-02 – San Diego County Sheriff's Department, Automated Regional Justice Information Systems (ARJIS)** – CAS analyst Michelle Mitchell said the agency is sponsoring ARJIS, which is requesting to add Android OS Galaxy tablets to the ARJIS mobile environment using CLETS. The agency will communicate via the Sprint DataLink, using a Juniper VPN, and is equipped with personal firewalls, antivirus software and a two-factor authentication (Deepnet Security) where an additional password obtained via a personally assigned token is required. The DOJ Network Information Security Unit has reviewed this application and has no concerns. Staff recommends approval. A motion was made to approve the application.

Motion:	Cuong Nguyen
Second:	Marc Shaw
Vote:	Approved unanimously

CLIENT REPORTS (CLETS Administration Section) – Previously, the Committee voted to allow client reports to be provided via letter. The CLETS Administration Section (CAS) staff provided a brief background statement for each client. The client was called upon to give an update in person, only if previously requested by the Committee or if the client was requesting an extension.

a. **Berkeley Police Department** – CAS analyst Dave Sutherland reported that a 2011 FBI audit revealed the agency was not compliant in seven areas. Six have been resolved. The one remaining area is the 128-bit NIST-certified encryption on the line connecting the public safety network to the city public network. Agency representative Brenda Velasquez said the agency anticipates full compliance by May 1, 2013. *A client update was e-mailed to Committee members. A motion was made to grant an extension to May 1.*

Motion:	Larry Spikes
Second:	Mark Shaw
Vote:	Approved unanimously

b. **Marin County Sheriff's Department** – CAS analyst Dave Sutherland reported that a 2013 FBI audit revealed the agency was not compliant in two areas, password requirements and logging of all failed log-in attempts/ability to disable user accounts after five failed attempts. Given the age of its current CAD system, the client is asking for a two-year extension to implement a new CAD system to mitigate these issues. Barring that possibility, the client is asking the committee to allow at least 90 days to work with its current vendor on technically and financially feasible solutions for the current system. Agency representative Rich Brothers said the agency was prepared to spend $20,000 for a temporary patch that would take an undetermined amount of time. A motion was made to grant a 90-day extension, and the client is to report progress at the next CAC meeting. *A client update was e-mailed to Committee members.*

Motion:	Marc Shaw
Second:	Cynthia Renaud
Vote:	Approved unanimously

c. **Oakland Police Department** – CAS analyst Dave Sutherland said a review of the client's application determined the agency did not meet encryption requirements when transporting CLETS data over microwave and fiber links. The client is in the process of replacing the current public safety system with a planned deployment date of mid-2015. The new system will provide end-to-end encryption. Agency representative Ahsan Baig said the department is using a shared infrastructure. The agency currently is working with a vendor on a temporary patch and eventually will replace its old CAD system, with a target date of 2015. *A client update was e-mailed to the Committee members. A motion was made to deny mid-2015 date, and the client is to report on a temporary patch at the next CAC meeting.*

Motion:	Larry Spikes
Second:	Scott Marshall
Vote:	Approved unanimously

d. **Los Angeles County Sheriff's Department –** CAS analyst Teresa Mora said a review of the client's application determined the agency did not meet encryption requirements in three areas. One issue has been resolved, but issues remain regarding microwave segments and wireless access for its mobile terminals (MDTs). Additionally, a 2011 FBI audit found the agency also did not meet the requirements in an additional three areas: Password, personal firewalls and virus protection software on its wireless access devices. The MDTs will be replaced with mobile digital computers (MDCs), which will resolve the encryption for the microwave and wireless segments and the personal firewall and virus protection software. Funding has been approved for LASD's Justice Data Interface Controller (JDIC) vendor to make modifications to meet the password compliance. The client's projected compliance date for all issues is July 2013. *A client update was e-mailed to Committee members. No vote was necessary, since the agency had moved forward its compliance date.*

e. **South Bay Regional Public Communications Authority** – CAS analyst Teresa Mora said a review of the client's application determined the agency does not employ antivirus software or firewalls on its mobile computers. At the last meeting, the CAC approved the client's request to extend the compliance date to February 2013. The client now reports that a catastrophic failure occurred to the agency's core switching hardware, which is key to the antivirus and firewall project. Funding for the hardware replacement has been secured. The agency has also secured additional support from the information technology department of the city of Hawthorne to assist in implementing this project. The client is requesting an extension to September 30, 2013. *A client update was e-mailed to Committee members. The agency contact person indicated the agency was unable to send a representative to request the extension. A motion was made to deny the extension request and the agency will be required to attend the next CAC meeting in person.*

Motion:	Sam Spiegel
Second:	Cynthia Renaud
Vote:	Approved unanimously

f. **Humboldt County Sheriff's Department** – CAS analyst Michelle Mitchell said a 2012 DOJ audit revealed the agency was noncompliant with the FBI's CJIS Security policy on passwords, Section 5.6.2.1. The issue was to be resolved with the implementation of its new CAD system and compliance was originally expected by early January 2014; however, the client revised the proposed compliance date to September 30, 2013. *A client update was e-mailed to Committee members and a revised version was placed in members' folders.*

g. **Carlsbad Police Department** – CAS analyst Michelle Mitchell reported a 2011 FBI audit revealed the agency was not compliant with the password requirements. The issue was to be resolved with the implementation of its new CAD system and compliance was expected by March 31, 2013. The vendor was unable to complete the project by that date and the agency is currently negotiating a new projected completion date. The department expects to be compliant by the end of December 2013 and is therefore requesting an extension until that date. No agency representative attended. *A client update was e-mailed to*

Committee members. Since a vendor has yet to be chosen, a motion was made to deny the extension. Chief Renaud will call the Carlsbad Police Chief to get an update.

Motion:	Marc Shaw
Second:	Steve Westerman
Vote:	Approved unanimously

h. **Cathedral City Police Department** – CAS analyst Michelle Mitchell said the agency was previously not compliant with the advanced authentication on its wireless CLETS devices. The agency submitted an implementation plan to provide the advance authentication. The applicant's solution has been implemented and the agency is now compliant. The client will be removed from future agendas. *A client update was e-mailed to Committee members and a revised version was placed in members' folders.*

i. **Orange County Sheriff's Office** – CAS analyst Michelle Mitchell said a review of a CLETS New Service Application determined the agency was not compliant with password policies for its downstream agencies. The application included a letter from the Sheriff's Department notifying DOJ of noncompliance with the password policies based on an audit given to the agency. The agency is in the process of implementing a solution that will be deployed internally and externally by December 13, 2013. *A client update was placed in members' folders.*

j. **Palm Springs Police Department** – CAS analyst Michelle Mitchell reported a review of the client's application determined the agency did not meet compliance in four areas. Two of the issues have been resolved; however, the remaining noncompliance issues include: The agency does not have an established incident handling plan and the agency does not ensure security awareness training is provided to local agency personnel, city/county IT staff and private contractor staff. *A client update was e-mailed to Committee members.*

k. **San Diego Police Department** – CAS analyst Michelle Mitchell reported a review of the client's application determined the agency did not meet encryption requirements. This issue has since been resolved. Additionally, a 2011 FBI audit revealed the client did not meet requirements associated with passwords and user authentication for its laptops. The original anticipated date for full compliance was December 2012, however, the Committee granted an extension until March 2013. The agency was granted another extension to July 2013 at the last meeting and is on track to have full implementation by then. *A client update was e-mailed to Committee members.*

l. **San Francisco Police Department** – CAS analyst Michelle Mitchell said a review of the client's application determined the agency did not meet advanced authentication requirements and background checks on Department of Technology staff working on the agency's MDCs. The background issue has since been resolved. The original anticipated compliance date for the advanced authentication was September 30, 2013, but the client has advanced the date to April 26, 2013. *A client update was e-mailed to Committee members.*

m. **San Francisco County Sheriff's Office** – CAS analyst Michelle Mitchell reported a 2011 FBI audit revealed the agency was not compliant in three areas: Security awareness training for the city of San Francisco information technology personnel who have access to the agency's CLETS system or data, advanced authentication and encryption requirements. The original projected compliance date for security awareness training and advanced authentication was in 2012; however, after multiple unsuccessful attempts to obtain an implementation plan from the Agency CLETS Coordinator that was signed by the sheriff, a letter was sent to the sheriff requesting a formal implementation plan with projected dates. A revised implementation plan addressing all three issues was received: 1) Security awareness training: The Sheriff's Department implemented a training program that will be completed by March 31, 2013; 2) Advance authentication: The city's IT department is still reviewing vendor options and expects to be awarded a contract this quarter; 3) Encryption requirements: The agency believed its encryption solution met the FIPS 140-2 requirements and requested the issue be re-evaluated. The DOJ re-evaluated the issue, contacted the vendor and the vendor advised the devices were not compliant. The city's IT department is planning upgrades to include devices that are FIPS 140-2 compliant, and the project should be completed by October 2013. *A client update was e-mailed to Committee members.*

n. **Westminster Police Department** – CAS analyst Michelle Mitchell said a review of the agency's request for additional MDTs revealed the agency was not compliant with advanced authentication requirements. The agency submitted an implementation plan stating multifactor software has been purchased and plans to be completed with the project before April 30, 2013. *A client update was e-mailed to Committee members.*

MEMBERS' REPORTS – Chair Spiegel asked members individually for a report regarding their agency and/or representation on the Committee.

- Larry Spikes said counties should stay tuned for the allocation of AB 109 funds. He is also working on the SB 1022 steering committee, which will develop the allocation of funds for the next round of jail construction throughout the state.

- Cuong Nguyen said the DOJ had completed the web-based portal to the Sex and Arson Registration program in March. At the next CAC meeting, he said the DOJ will report on the Supervised Release File.

- Scott Marshall said the sheriffs are challenged by the 90-day password authentication requirement. He also emphasized that agencies must have crosscut shredders to avoid noncompliance.

- Scott Silsbee wished agencies, such as Oakland, good luck in its CAD pursuits.

- Sam Spiegel voiced RMS concerns and how important it was for contracts to be set up correctly with vendors.

CAC DISCUSSION/OPEN FORUM/PUBLIC COMMENT (Committee members/ audience) – Client Services Program Manager Robin Robles indicated the CLETS auditors found many communication centers with the responsibility of providing hit confirmation for records entered by its agency have not been verifying hit confirmations with master case files, but instead verifying the records is in the database via CLETS. When responding to hit confirmations, agencies need to validate the record against the master case file, not by querying CLETS.

NEXT CAC MEETING/ADJOURN – The meeting was adjourned at 1 p.m. The next two CAC meetings were tentatively scheduled for July 2013 and November 2013. Following the SSPS meeting, it was decided the next SSPS meeting would precede the CAC meeting.

Action Items

1. Cynthia Renaud to contact the Carlsbad police chief about choosing a vendor that will lead to the agency meeting password requirements.