

California Law Enforcement Telecommunications System (CLETS)
Advisory Committee (CAC)

Standing Strategic Planning Subcommittee (SSPS)
Meeting Minutes

March 25, 2015

Folsom Police Department

Present: Chair: Tom Bruce (California Police Chiefs Association Technology Committee)

Members: Julie Basco (Department of Justice)
Sam Spiegel (California Peace Officers' Association)
Janelle Dickey (Department of Motor Vehicles)
Sherri Rinkel (League of California Cities)
Chris Emery (California Police Chiefs Association)
John Lemmon (Office of Emergency Services)
Ashish Kakkad (California State Sheriffs' Association)
Laurie Porcari (California State Association of Counties)

Absent: Marc Shaw (California Peace Officers' Association)
Rita Lugo (California Highway Patrol)

CALL TO ORDER

Chair Bruce called the meeting to order at 9:02 AM.

ROLL CALL

California Law Enforcement Telecommunications System (CLETS) Administration Section (CAS) analyst Mark Hayward called the roll; a quorum was present.

APPROVAL OF MINUTES

A motion was made to approve the minutes from the meeting of December 2, 2014.

Motion: Julie Basco
Second: Sherri Rinkel
Discussion: Member Spiegel voiced his concern about the lack of detail and specificity contained in the minutes from the December 2, 2014 meeting. He stated the minutes did not fully convey the essence or the evolution of the remaining goals from the 2009 CLETS Strategic Plan. After discussion, it was decided that Member Spiegel's concerns would be addressed during the discussion of agenda item #6, 2009 CLETS Strategic Plan.
Vote: Approved, Member Spiegel opposed

SAN DIEGO - LAW ENFORCEMENT COORDINATION CENTER- LECC

San Diego - Law Enforcement Coordination Center (LECC) Director Leslie Gardner made a presentation to the SSPS explaining the function and structure of the San Diego - LECC. Director Gardner explained that the LECC is one of 79 law enforcement fusion centers in the United States and supports investigation efforts for member law enforcement agencies. She indicated that LECC works closely with the High Intensity Drug Trafficking Areas Program (HITDA), the Western States Information Network (WSIN) as well as with local, state and federal agencies. She further explained that LECC is staffed by local law enforcement personnel from various law enforcement agencies and grant funded employees.

Discussion

Member Basco inquired as to which Originating Agency Identifiers (ORI) were used by the San Diego - LECC when accessing the CLETS. Director Gardner explained that the members working at the center use their agency's ORI while accessing CLETS and that the grant funded employees must be sponsored by a law enforcement agency and use the sponsoring agency's ORI. Member Basco asked if the current grant funded employees access CLETS behind the San Diego Sheriff Department's (SDSO) message switching computer and if the SDSO takes responsibility for the grant funded employees. Director Gardner indicated that the grant funded employees use the SDSO ORI and are under the authority and supervision of the SDSO.

Director Gardner went on to explain that of the 79 fusion centers in the United States, six of them are in California. Chair Bruce then asked Director Gardner to describe the structure of her fusion center. Director Gardner explained that the San Diego - LECC has a staff of 75 persons and further explained that the San Diego - LECC staff represented a variety of organizations and included, federal, state, local and grant funded sources. The agencies providing staff are local police departments, sheriff offices, the Department of Homeland Security, HITDA, the Federal Bureau of Investigation and the Drug Enforcement Agency. Director Gardner then went on to explain that the fusion center was formed following 911 and was created to facilitate the sharing of information between law enforcement agencies.

CLETS STRATEGIC PLAN

Chairman Bruce initiated a discussion of the 2009 CLETS Strategic Plan.

Goal 3

To enable biometric capture of misdemeanor and infraction information for the transmission to the appropriate agency's repository and will work with current technology.

Discussion

Subcommittee members engaged in a discussion of Goal 3 which was read to the Subcommittee by Member Spiegel. Member Spiegel explained that the primary purpose of Goal 3 is to provide a automated cite and release system to replace the current method of either using an ink pad and placing the thumbprint on the ticket or taking the person to the station for a complete booking in the case of an infraction. Member Spiegel further stated that an automated system would reduce the need to take people to the station and would be valuable in expediting the current cite and release process and asked the Subcommittee whether they thought a preamble might be of value in clarifying the intent of Goal 3.

Chair Bruce further added that under the current field process, a thumbprint is applied to paper using an ink pad in cases where the identity of a person is in question. As such, the intent of Goal 3 is to move to a digital system that would replace the ink pad process with a digital process. Chair Bruce stated that a digital system could aid in providing the identity of a person in the field and asked if the Subcommittee members believed that Goal #3 should be reworded to better explain its purpose; however, there was no determination or further discussion.

Result:

No motion made or changes requested to Goal 3.

Goal 4

Transmit "Failure to Appear" (FTA) bench warrants to DOJ and the FBI and have a fingerprint associated with the warrant for positive identification.

New Goal 1

Explore the capture and sharing of historical and real time Global Positioning System (GPS) based geospatial data on offenders statewide.

Discussion

Chair Bruce started the discussion of Goal 4 and New Goal 1 by recommending that the two goals be separated from under Task ID 3. Chair Bruce stated that the primary purpose of New Goal 1 is intended to apply to convicted offenders who are under house arrest and is an attempt to consolidate disparate systems under a unified system and thus provide statewide tracking under circumstances, which have already been court sanctioned and do not violate an individual's 4th Amendment rights.

Chair Bruce then provided an example of a situation in Orange County in which the use of GPS allowed law enforcement personnel to apprehend a suspect in a sexual assault case. Member Basco added that pending legislation, Assembly Bill 1213, would require the Department of Justice to begin tracking GPS data if chaptered and therefore, Chair Bruce stated that this is another example of the importance keeping up with technology.

Result:

No motion made and no changes requested to Goal 4 or New Goal 1.

Goal 8

Representatives from the California Police Chiefs' Association, the California State Sheriffs' Association, the California Peace Officers' Association and the DOJ CAC or SSPS representatives will meet with the Department of Motor Vehicles (DMV) Director to discuss:

1. Electronic, interstate exchange of driver license and identification photos for law enforcement purposes; and,
2. Facial recognition technology.

Discussion:

Chair Bruce began by announcing that Goal 8 would be addressed in the afternoon CAC meeting, then read Goal 8 to the Subcommittee and asked if there was any discussion, which there was none.

Action:

No motion made and no changes requested to Goal 8.

MEMBERS' REPORTS

Member Kakkad thanked the SSPS for inviting the San Diego - LECC to speak to the Subcommittee.

Chair Bruce thanked the DOJ for its update to the California Law Enforcement Website (CLEW) and expressed his appreciation for its new updated appearance and improved utility. Chair Bruce indicated that he used the website frequently and especially liked the Missing and Unidentified Persons (MUPS) update, which he believed is an excellent tool for law enforcement. Chair Bruce asked if the MUPS portion of CLEW could be automated to create a periodic distribution to law enforcement statewide. Member Basco indicated she would need to explore whether this could be done. Chair Bruce expressed his pleasure with the recent DOJ MUPS training he attended and indicated that he would be interested in hosting a MUPS training sometime in the future.

SSPS DISCUSSION/OPEN FORUM/PUBLIC COMMENT

Chair Bruce referred the Subcommittee to the EFF letter included in each Member's packet, which was submitted as public comment and will be entered into the public record for the SSPS meeting.

David Maass, an investigative researcher with the Electronic Frontier Foundation (EFF) asked to address the SSPS. Mr. Maass inquired whether the meeting between the law enforcement association representatives and the DMV Director had taken place. Member Basco responded that the proposed Goal 8 meeting with the DMV Director did not occur due to potential open meeting concerns. A complete transcript of Mr. Maass' subsequent statement is attached.

Brian Barnes, the Executive Director of the California CLETS Users Group, CCUG, asked to address the Subcommittee. A complete transcript of Mr. Barnes comments is attached.

NEXT SSPS MEETING

The meeting was adjourned at 10:11 a.m. The next SSPS meeting is scheduled for July 22, 2015.

Standing Strategic Planning Subcommittee Tasks

✓ In Process
⊘ Removed



ID	Task Title/Description	Assigned To	Due Date	Priority	Status
2	Recommend rewording 2009 CLETS Strategic Plan Goal 3 to any future CLETS Strategic Plan as incorporating fingerprints into the traffic citation process so when a booking and release citation is issued, there is an associated fingerprint, which can be utilized for positive identification and for inclusion on the individual's rapsheet. (Goal 3) <i>Presented and approved by the CAC to read: To enable biometric capture of misdemeanor and infraction information for transmission to the appropriate agency's repository and will work with current technology.</i>	SSPS			✓
3	Further exploration by committee members of addressing 2009 CLETS Strategic Plan Goal 4 with SmartJustice and a fusion between the CJIS databases and the Automated Criminal History System to determine recommendation options to the CAC. (Goal 4) <i>Presented and approved by the CAC to read: Transmit "Failure to Appear" (FTA) bench warrants to the DOJ with a fingerprint or thumbprint."</i> Also, Goal 4 renumbered to Goal 3.1.	SSPS			✓
5	Determine if California DMV photos can be shared nationally for investigative purposes. (Goal 8) Reworded Goal 8 presented and approved by the CAC. Task: Further discussion on LEA associations meeting with DMV mangagement. CAC Chair Spiegel to send a letter to the law enforcement association presidents stating: <i>1. What the CAC is attempting to accomplish with Goal 8, and;</i> <i>2. Asking them to appoint a representative to attend the meeting with the DMV Director.</i> <i>Member Dickey to provide pertinent Government codes and statutes to Member;</i> <i>DOJ to prepare a mock-up of the current/proposed Nlets response.</i>	SSPS			✓

Standing Strategic Planning Subcommittee Tasks

✓ In Process
 ⊘ Removed



ID	Task Title/Description	Assigned To	Due Date	Priority	Status
6	<p>Determine availability of using facial recognition with Cal-Photo and California DMV photos. (Goal 8) Reworded Goal 8 presented and approved by the CAC. Task: Further discussion on LEA associations meeting with DMV mangagement. CAC Chair Spiegel to send a letter to the law enforcement association presidents stating:</p> <p>1. What the CAC is attempting to accomplish with Goal 8, and;</p> <p>2. Asking them to appoint a representative to attend the meeting with the DMV Director.</p> <p>Member Dickey to provide pertinent Government codes and statutes to Member;</p> <p>DOJ to prepare a mock-up of the current/proposed Nlets response.</p>	SSPS			✓
7	<p>Look at the architecture of the SRF to determine if a data field can be added that includes GPS data and a hyperlink which provides the ability to ping the location of the SRF registrant. <i>A field can be added to SRF, which would allow GPS data to be entered; however, hyperlink capability would not be available. An alternate solution would be for the individual to cut and paste the GPS data into another application or browser.</i> Task: To keep New Goal 1 in any future CLETS Strategic Plan. Accordingly, presented and approved by the CAC to read: Explore the capture and sharing of historical and real-time Global Positioning System (GPS) based geospatial data on offenders statewide.</p>	SSPS			✓

2009 CLETS Strategic Plan

1) ID 2

Goal #3

To enable biometric capture of misdemeanor and infraction information for transmission to the appropriate agency's repository and will work with current technology.

2) ID 3

Goal #4

Transmit "Failure to Appear" (FTA) bench warrants to the DOJ with a fingerprint or thumbprint."

New Goal One

Explore the capture and sharing of historical and real time Global Positioning System (GPS) based geospatial data on offenders statewide.

3) ID 5

Goal #8

a. Representatives from the California Police Chiefs Association, the California State Sheriffs' Association, the California Police Officers' Association and the Department of Justice CLETS Advisory Committee or SSPS representatives will meet with the Department of Motor Vehicles Director to discuss:

- 1. Electronic, interstate exchange of driver license and identification photos for law enforcement purposes; and,*
- 2. Facial recognition technology.*

b. Department of Motor Vehicles Code Citation Response

c. NLETS DMV Inquiry



Department of Motor Vehicles Code Citation Response to the CLETS (Draft) Strategic Plan 2014; Goal #8

Goal #8 Representatives from the California Police Chiefs' Association, the California State Sheriffs' Association, The California Peace Officers' Association, the DOJ and the CAC or SSPS representatives will meet with the DMV Director to discuss:

- 1. Electronic, interstate exchange of drivers' license and identification photos for law enforcement purposes; and*
- 2. Facial recognition technology*

DMV Code Citations Response to the CLETS Standing Strategic Planning Subcommittee (SSPS) request on 12/2/14

State and federal statutes and regulations address the confidentiality and release of personal information in the form of Driver License (DL) and Identification (ID) photos contained in the Department of Motor Vehicles (DMV) database.

The California Information Practices Act (IPA) (Civil Code (CC) §1798, et. seq.) imposes restrictions on the release of photos. CC §1798.1(c), states that in order to protect the privacy of individuals it is necessary that the maintenance and dissemination of personal information be subject to strict limits. CC §1798.3(a), defines personal information as any information that is maintained by an agency that identifies or describes an individual including, but not limited to his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. The IPA imposes a general prohibition against release of personal information; however, there are exceptions such as release to a government entity when required by state or federal law, or to a law enforcement or regulatory agency when required for an investigation of unlawful activity unless the disclosure is otherwise prohibited by law.

Vehicle Code (VC) §1810.5, authorizes law enforcement and specified government entities to access DMV records, including photos. The methods of accessing the department's records are limited by regulation.

Title 13, California Code of Regulations (CCR), Article 5, §350.10, specifies that in order to obtain information from DMV about a licensee; a government requester must provide sufficient identifying points of information including the driver's full name and date of birth or the driver's license number only (the same requirements apply to identification cards).



Department of Motor Vehicles Code Citation Response to the CLETS (Draft) Strategic Plan 2014; Goal #8

VC §1808.5, establishes all records of the department relating to the physical condition of any person are confidential and not open to public inspection. This is considered applicable to a photo since it provides information relating to the physical condition of the DL/ID holder.

VC §§12800.5 and 13005.5, explicitly restrict the release of DL/ID photos. The department is prohibited, unless requested by the subject of the photo, from distributing, selling the picture or photo, or any information pertaining to the physical characteristics of the subject to any private individual or any firm, co-partnership, association or corporation. The statutes referenced in this paragraph do not directly apply to NLETS; however, provide examples of existing restrictions regarding the release of DL/ID photos.

The Federal Driver's Privacy Protection Act (DPPA) [United States Code, Title 18, §§2721-2725], prohibits generally, the disclosure of highly restricted personal information (includes photos) to any person or entity, however, there are exceptions. Photos are subject to mandatory disclosure in connection with certain federal laws pertaining to motor vehicles. In addition, the DPPA authorizes photo release in four discretionary categories.

An opinion from the California Attorney General in 1996 stated the discretionary release categories of the DPPA allow a state to authorize disclosure, however, access to the information is prohibited if the Legislature does not "affirmatively authorize" disclosure in the specified circumstances. No affirmative authorization is found in existing state statutes that would require or allow the transmission and wholesale sharing of DL/ID photos between Cal-Photo and NLETS.

All government agencies, including law enforcement requesting DMV record information must complete and submit a Government Requester Account Application (INF 1130). Each government requester is required to follow security and other requirements. In the General Security Requirements section of the form, the government requester agrees to not sell, retain, distribute, provide or transfer any record information or portion of a record acquired under the government requester account agreement, except as authorized by the department.

CCR, Title 13, Article 5, §350.42, states any use of DMV information for a purpose other than stated in the approved INF 1130 application is prohibited. Section C-9 of the INF 1130 states the agency shall not sell, retain, distribute, provide or transfer any record information or portion of the record information except as authorized by the department.

DMV executed an Inter-Agency Agreement (IAA) with DOJ to allow for access to photos in DMV files. The agreement requires DOJ to not transfer, distribute, enter into any third party agreement or otherwise provide images to any unauthorized entity or use images for any unauthorized purposes. In addition, DOJ shall not retain images for the purposes of creating a database unless specifically authorized in writing by DMV's Information Services Branch Chief.



Department of Motor Vehicles Code Citation Response to the CLETS (Draft) Strategic Plan 2014; Goal #8

Currently, NLETS is authorized to obtain DL/ID photos from CLETS/Cal-Photo on a “one-in/one-out” basis for law enforcement and other government agencies authorized by statute and approved by DOJ and DMV. Authorized law enforcement and government agencies making a request for DL/ID photos through DMV, CLETS, or NLETS are required to provide identifying points of information to ensure the correct photo is provided to the requester and for tracking the release and receipt of the photo.

DMV and DOJ are required to maintain an accurate accounting of the date, nature, and purpose of each disclosure of personal information pursuant to CC §1798.25. The accounting is required to include the name, title, and business address of the person or agency to which the disclosure was made. Routine disclosures of information pertaining to crimes, offenders, and suspected offenders to law enforcement or regulatory agencies of federal, state, and local government are considered disclosures pursuant to CC §1798.24(e) for the purpose of meeting these requirements.

Accordingly, DMV in meeting its obligations to maintain an accurate accounting of each disclosure of personal information has the authority to audit DOJ for the purpose of determining compliance with statute, regulations, and other requirements contained in the IAA.

Conversely, the transmission and wholesale sharing of DL/ID photos between Cal-Photo and NLETS raises significant concerns. DMV has a statutory and regulatory obligation to protect all information, including photos that are maintained in the department’s database. There is no viable method for DMV to account for each disclosure of California DL/ID photos via NLETS under this proposal. The proposed expansion of photo-sharing between CLETS/Cal-Photo and NLETS may open the door to random accessing of photos without providing identifying points of information. The inability to account for each California DL/ID photo disclosure via NLETS would make it difficult, if not impossible to track the source of a security breach involving the NLETS network.

At this time, DMV cannot support Goal #8 to the extent it depends on the use of any California DMV information, specifically DL/ID photos. Existing statute and regulations require a vast array of security measures to protect DMV record information for the reasons stated.

References

California Vehicle Code, §§1808.5, 1810.5, 12800.5, and 13005.5

<http://www.dmv.ca.gov/portal/dmv/detail/pubs/vctop/vc/d2/c1/a3/1808.5>

<http://www.dmv.ca.gov/portal/dmv/detail/pubs/vctop/vc/d2/c1/a3/1810.5>

<http://www.dmv.ca.gov/portal/dmv/detail/pubs/vctop/vc/d6/c1/a3/12800.5>

<http://www.dmv.ca.gov/portal/dmv/detail/pubs/vctop/vc/d6/c1/a5/13005.5>



**Department of Motor Vehicles Code Citation Response
to the CLETS (Draft) Strategic Plan 2014; Goal #8**

References, *continued*

Information Practices Act (California Civil Code) §§1798, 1798.1(c), 1798.3(a), 1798.24, and 1798.25

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.1.

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.3.

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.24.

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.25.

California Code of Regulations, Title 13, Article 5, §§350.10, and 350.42

Section 350.10

[https://govt.westlaw.com/calregs/Document/I9DF7BEC0D46811DE8879F88E8B0DAAAE?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=\(sc.Default\)](https://govt.westlaw.com/calregs/Document/I9DF7BEC0D46811DE8879F88E8B0DAAAE?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default))

Section 350.42

[https://govt.westlaw.com/calregs/Document/IA1BD7950D46811DE8879F88E8B0DAAAE?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=\(sc.Default\)](https://govt.westlaw.com/calregs/Document/IA1BD7950D46811DE8879F88E8B0DAAAE?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default))

Federal Driver's Privacy Protection Act, U.S. Code, Title 18, §§2721-2725

[http://uscode.house.gov/view.xhtml?req=\(title:18 section:2721 edition:prelim\) OR \(granuleid:USC-prelim-title18-section2721\)&f=treesort&edition=prelim&num=0&jumpTo=true](http://uscode.house.gov/view.xhtml?req=(title:18 section:2721 edition:prelim) OR (granuleid:USC-prelim-title18-section2721)&f=treesort&edition=prelim&num=0&jumpTo=true)

Attorney General Opinion: 79 Ops.Cal.Atty.Gen. 76 (June 10, 1996)

<http://oag.ca.gov/system/files/opinions/pdfs/95-805.pdf?>

NLETS Driver's License Inquiry

NORTH CAROLINA



DR.NCDCI0000
15:00 12/04/2014 12517
15:00 12/04/2014 49723 CA0349400
*CMFK005925
TXT
Query data:
OLN/1.IMQ/N.
NAME: ELTON ROY PEELE
RESIDENCE ADDRESS: BX30562TH DORM LN; DURHAM,NC
277080001
COUNTRY: UNITED STATES
DATE OF BIRTH: 1912-11-20
HEIGHT: 510
EYE COLOR: BLUE
HAIR COLOR: GREY
GENDER: Male
RACE: White
*** DRIVER LICENSE DETAILS ***
DRIVER AUTHORIZATION ID: 000000000001
JURISDICTION AUTHORITY CODE: NC
DRIVER LICENSE PERMIT QUANTITY: 0
LICENSED COMMERCIAL DRIVER: NO
LICENSED NON-COMMERCIAL DRIVER: YES
DRIVER LICENSE NON-COMMERCIAL STATUS: CDL B EXPIRED

DR.NCDCI0000
15:00 12/04/2014 12517
15:00 12/04/2014 49723 CA0349400
*CMFK005925
TXT
Query data:
OLN/1.IMQ/N.
NAME: ELTON ROY PEELE
RESIDENCE ADDRESS: BX30562TH DORM LN; DURHAM,NC
277080001
COUNTRY: UNITED STATES
DATE OF BIRTH: 1912-11-20
HEIGHT: 510
EYE COLOR: BLUE
HAIR COLOR: GREY
GENDER: Male
RACE: White
*** DRIVER LICENSE DETAILS ***
DRIVER AUTHORIZATION ID: 000000000001
JURISDICTION AUTHORITY CODE: NC
DRIVER LICENSE PERMIT QUANTITY: 0
LICENSED COMMERCIAL DRIVER: NO
LICENSED NON-COMMERCIAL DRIVER: YES
DRIVER LICENSE NON-COMMERCIAL STATUS: CDL B EXPIRED

NLETS Driver History Inquiry

NORTH CAROLINA

DRIVER HISTORY INQUIRY INCLUDES:

NAME
RESIDENCE ADDRESS
COUNTRY
DATE OF BIRTH
HEIGHT
EYE COLOR
HAIR COLOR
GENDER
RACE

PLUS THE FOLLOWING:



ACCIDENTS NOTED ON THIS DOCUMENT SHALL NOT BE
CONSIDERED DETERMINATIVE OF FAULT OR NEGLIGENCE
ON THE PART OF THE INDIVIDUAL

**

CERTIFIED A TRUE COPY OF THE D/L RECORD OF THE
PERSON NAMED HEREIN AS APPEARS
ON THE AUTOMATED SYSTEM OF DMV. G.S.20-26(B):

*** DRIVER LICENSE DETAILS ***

DRIVER AUTHORIZATION ID: 0000000000001
JURISDICTION AUTHORITY CODE: NC
ISSUE DATE: 2002-03-06
EXPIRATION DATE: 2008-04-13
DRIVING RESTRICTION CODE: NOT ELIG FOR SCHOOL BUS
DRIVER CERTIFICATION
DRIVING RESTRICTION CODE: 1
DRIVER LICENSE PERMIT QUANTITY: 0
DRIVER LICENSE COMMERCIAL CLASS CODE: B
LICENSED COMMERCIAL DRIVER: YES
DRIVER LICENSE COMMERCIAL STATUS: EXPIRED

*** DRIVER CONVICTION ***

CONVICTION DATE: 2008-11-03
CITATION DATE: 2008-11-03
DRIVER CONVICTION TEXT: CONV: (313)SPEEDING (84 MPH
IN A 70)

*** DRIVING INCIDENT ***

DATE: 2014-08-29
DRIVER ACCIDENT SEVERITY: ACDNT: JOHNSTON COUNTY,
NC PERS INJ

*** ADDITIONAL INFORMATION ***

FIELD NAME: MedicalCertificationStatus
FIELD VALUE: MED CERTIFICATION STATUS :
UNDETERMINED

ACCIDENTS NOTED ON THIS DOCUMENT SHALL NOT BE
CONSIDERED DETERMINATIVE OF FAULT OR NEGLIGENCE
ON THE PART OF THE INDIVIDUAL

**

CERTIFIED A TRUE COPY OF THE D/L RECORD OF THE
PERSON NAMED HEREIN AS APPEARS
ON THE AUTOMATED SYSTEM OF DMV. G.S.20-26(B):

*** DRIVER LICENSE DETAILS ***

DRIVER AUTHORIZATION ID: 0000000000001
JURISDICTION AUTHORITY CODE: NC
ISSUE DATE: 2002-03-06
EXPIRATION DATE: 2008-04-13
DRIVING RESTRICTION CODE: NOT ELIG FOR SCHOOL BUS
DRIVER CERTIFICATION
DRIVING RESTRICTION CODE: 1
DRIVER LICENSE PERMIT QUANTITY: 0
DRIVER LICENSE COMMERCIAL CLASS CODE: B
LICENSED COMMERCIAL DRIVER: YES
DRIVER LICENSE COMMERCIAL STATUS: EXPIRED

*** DRIVER CONVICTION ***

CONVICTION DATE: 2008-11-03
CITATION DATE: 2008-11-03
DRIVER CONVICTION TEXT: CONV: (313)SPEEDING (84 MPH
IN A 70)

*** DRIVING INCIDENT ***

DATE: 2014-08-29
DRIVER ACCIDENT SEVERITY: ACDNT: JOHNSTON COUNTY,
NC PERS INJ

*** ADDITIONAL INFORMATION ***

FIELD NAME: MedicalCertificationStatus
FIELD VALUE: MED CERTIFICATION STATUS :
UNDETERMINED

CLETS Testing Requirements

The California Department of Justice has an online tool available for agencies called nexTEST, which ensures testing compliance. An agency may elect to use any of the nexTEST tests as an option for their agency. Or, they may create their own tests as long as they are providing the appropriate level of testing to personnel that have varying levels of access to the Criminal Justice Information (CJI) data.

There are three tests available via NexTEST:

1. Full Access (enters/inquires);
2. Less Than Full Access (inquiry); and
3. Security Awareness (Employee is around CJI information but doesn't access databases).

Per FBI CJIS Security Policy 5.2, Security and Awareness Training is required for "all personnel who have access to CJI." The policy applies to anyone who has undergone a limited background check as part of the hiring process. Thus, it applies to a variety of staff that are not escorted as visitors, such as janitors and vendors.

Completion of the Security Awareness Training helps educate staff to the sensitivity of information they may have proximity to and teaches them to appropriately respond to information they may possibly come across, but shouldn't have seen if/when needed. The Security Awareness Training requirement can be satisfied using multiple resources. As mentioned, nexTEST is an option, is web-based and provides a certificate upon completion for verification; however, nexTEST is not required. Your agency can opt to use another training method for the Security Awareness Training. For example, some agencies conduct the training using a PowerPoint presentation and track completion on a training spreadsheet.

**ELECTRONIC FRONTIER FOUNDATION***Protecting Rights and Promoting Freedom on the Electronic Frontier*

March 10, 2015

VIA EMAIL

CLETS Administration Section
California Department of Justice
4949 Broadway Room J231
Sacramento, CA 95820
Email: steve.kennedy@doj.ca.gov

RE: CLETS Advisory Committee/Standing Strategic Planning Subcommittee

To Whom It May Concern:

I am writing on behalf of the Electronic Frontier Foundation (EFF), a San Francisco-based non-profit that defends civil liberties in the digital age. Having reviewed recent meeting minutes from the CLETS Advisory Committee (CAC) and its Standing Strategic Planning Subcommittee (SSPS), as well as documents obtained through the California Public Records Act, EFF is deeply concerned about the privacy and civil rights implications of CAC/SSPS's recent actions and proposals. Please enter this letter into the public record for the March 25 meetings of both CAC and SSPS.

The public records indicate that these bodies are moving beyond mere advisory roles by applying for grants and meeting with heads of law enforcement agencies to expand both the collection of personal information and the sharing of this sensitive information with outside entities. In particular, CAC/SSPS appears headed towards a process of sharing facial images held by the California Department of Motor Vehicles (DMV) and enabling facial recognition for investigative purposes, despite DMV concerns that some of these steps may be insecure and inconsistent with existing statutory authorization.

First, EFF is greatly concerned about CAC/SSPS's recent efforts to obtain funding to build out DMV's infrastructure and to allow the state to access driver license photos from other states through the National Law Enforcement Telecommunications System (NLETS). While this may not directly affect California drivers, it is clear from the documents that CAC/SSPS believes that this first step will open the door—both in terms of policy and technology—for the sharing of California drivers' photos nationwide. We share the concerns of the director of the DMV, who stated in response to CAC/SSPS inquiries:

[T]he transmission and wholesale sharing of DL/ID photos between Cal-Photo and NLETS raises significant concerns. DMV has a statutory and regulatory obligation to protect all information, including photos that are maintained in the department's database. There is no viable method for DMV to account for each disclosure of California DL/ID photos via NLETS under this proposal. The proposed expansion of photo-sharing between CLETS/Cal-Photo and NLETS may open the door to random accessing of photos without providing identifying points of information. The inability to account for each California DL/ID photo disclosure via NLETS would make it difficult, if not impossible to track the source of a security breach involving the NLETS network.

At this time, DMV cannot support Goal #8 to the extent it depends on the use of any California DMV information, specifically DL/ID photos. Existing statute and regulations require a vast array of security measures to protect DMV record information for the reasons stated.

815 Eddy Street • San Francisco, CA 94109 USA

voice +1 415 436 9333*fax* +1 415 436 9993*web* www.eff.org*email* information@eff.org

Despite this warning from the DMV, CAC/SSPS is continuing to move forward with this proposal, as well as pursuing the ability for law enforcement to leverage facial recognition technology against DMV records for investigations.

Beyond the obvious civil liberties concerns, there are also data security issues with these CAC/SSPS proposals. CAC meeting minutes regularly outline deficiencies in encryption and other security compliance failures among California law enforcement agencies, including problems in the Los Angeles County Sheriff's Office and the Los Angeles Police Department, two of the largest law enforcement agencies in the state. No personal information should be collected, stored, or shared without effective security techniques and detailed auditing to ensure this sensitive information is adequately safeguarded.

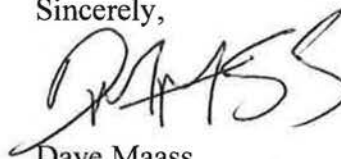
Finally, we are concerned with CAC/SSPS efforts to collect thumbprints from Californians during traffic stops for low-level infractions and misdemeanors, as well as the expansion of GPS tracking and sharing of locational data statewide. Although CAC/SSPS cited Proposition 47 as justification for these measures, the primary purpose of Proposition 47 was to reduce the consequences of non-violent and less serious crimes. These proposals simply serve as an end-run around the will of California voters.

Given the specific privacy and security concerns surrounding these proposals, and the growing concerns about privacy and government surveillance generally among the public and state legislators, it was surprising to see CAC/SSPS is scheduling meetings with law enforcement officials on these issues without engaging civil liberties advocates and other stakeholders.

EFF asks CAC/SSPS to immediately put the brakes on these plans. These policies will have substantial and long-lasting ramifications for both law enforcement and the public. Therefore, decisions of this magnitude must be made with full public engagement and the involvement of the legislature, not in obscure advisory and planning committee meetings or in closed-door sessions with law enforcement associations.

In the coming days, we plan to publicize our position on these issues in anticipation of the CAC/SSPS March 25 meetings, with a goal of generating letters for public comment. If representatives of these committees would like to speak with us directly, you can reach me at dm@eff.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'DMASS', written over a horizontal line.

Dave Maass
Investigative Researcher

CC: Attorney General Kamala Harris
attorneygeneral@doj.ca.gov

815 Eddy Street • San Francisco, CA 94109 USA

voice +1 415 436 9333

fax +1 415 436 9993

web www.eff.org

email information@eff.org

Electronic Frontier Foundation – Dave Maass Public Comment

My name is Dave Maass and I am an investigative researcher at the Electronic Frontier Foundation, a San Francisco non-profit that defends civil liberties in the digital world. Today I speak on behalf of more 1,500 Californians who joined us in opposing Goal 8 of the strategic plan, which would share DMV photos nationwide and allow law enforcement to deploy facial recognition.

In 1977, the California Legislature passed the Information Practices Act, reaffirming that the right to privacy is a personal and fundamental right protected by the California Constitution. To quote from the legislature's statement of intent codified into law:

"The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information... In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

The CLETS Advisory Committee's Standing Strategic Planning Subcommittee has repeatedly disregarded warnings from the California Department of Motor Vehicles that connecting Cal-Photo to NLETS runs counter to both the intent and the letter of the law. Facial recognition would run into even more legal roadblocks. Nevertheless, these committees have moved forward, despite their responsibility to consider the privacy of Californians. Nothing on the record indicates that civil liberties have played a role in discussion over this goal.

Californians have the power to hold state and local law enforcement accountable, but we have little ability to control policy and oversight outside of the state's boundaries. We certainly have no say over law enforcement policies outside of the U.S.—and I'll remind you that Mexico and Canada are also partners in NLETS.

But let's also look at the issue of transparency. NLETS is a private entity and not subject to the Freedom of Information Act, the California Public Records Act, or open meeting laws. If Cal-Photo is connected to NLETS, the public will have no opportunity to inspect or influence policy changes at NLETS. Handing over our photos to an entity with no public accountability measures is unacceptable.

As the DMV stated, under this plan, there would be little we could do to track or prevent random accessing of our DMV photos or trace data breaches.

Goal 8 must be removed from the strategic plan, but it is not the only problematic goal that CLETS Advisory Committee and its subcommittee have approved. In the coming weeks and months, we intend to dig deeper into issues of biometrics, finger and thumb printing and GPS tracking.

We're putting the spotlight on this committee and 1,500 emails is only the beginning.



California CLETS Users Group

PO Box 294, Lake Elsinore, CA 92531

Tax ID # 20-4416174

Hello, I'm Brian Barnes, Executive Director of the California CLETS Users Group, more commonly referred to as CCUG or C-CUG. I wanted to take a few moments today to share a little about our organization.

In 1983, California DOJ fostered a users group to provide CLETS training, news, and updates to better communicate with law enforcement and criminal justice agencies. Since CCUG originated, our mission has been to represent the approximately 1,300 law enforcement and criminal justice agencies in California. Our membership includes management, supervisory, technical staff, and line level users representing agencies that access CLETS to do their daily jobs.

CCUG's chapters divide the state geographically; northern, central, and southern. Each chapter has their own board to coordinate training and communicate with local users. We currently have 110+ agencies and over 350 members registered with us. Our membership is 44% dispatch, 38% records, 7% IT, 6% training, and 5% courts, probation, and federal agencies. Our 14 board members are elected by our membership and volunteer their time to CCUG in addition to their full time law enforcement employment.

We provide two types of training; quarterly chapter training and an annual seminar. Each chapter hosts 3 quarterly trainings each year. Chapter training topics vary throughout the year and typically include one if not two DOJ/CLETS topics. So far this year our Southern Chapter presented *New Laws for 2015* and *Tactical Stress Response, Why Peer Support Works*. Last month, the central chapter had DOJ present on *nexTest* and *Smart Justice/Justice Mobile*.

Once a year CCUG hosts our 24-hour Annual Training & Technology Seminar. We alternate between northern and southern California each year with last year in Sacramento and this year in Anaheim. Our seminar is certified by POST and gives each attendee 24 hours of CPT credit. It is a great opportunity to meet and receive training from DOJ, DMV, NCIC, and local law enforcement leaders.

If you looked at last year's training topics, you would have noticed about 10% were not directly CLETS related. We try to incorporate training topics that focus on professionalism, career development, and empowering a well-rounded person. We strongly believe training that enhances a person's life on any level improves their performance in the workplace.

Lastly, we provide a space for DOJ to present their Training for Trainers, commonly referred to as T4T, immediately preceding our annual seminar. Several of the T4T attendees also attend the seminar.

Since CCUG's inception we have continued to provide CLETS users the best forums available for CLETS training and information exchange. Considering the events of the last several years and the added emphasis on tightened security, system training, and other related issues, training is still a smart investment for our CLETS users. We take pride in providing our member agencies with CLETS and NCIC training and connecting them with the experts that have the right answers. I appreciate this opportunity to speak with you today, thank you!

**Executive
Director**
Brian Barnes

**Northern Chapter
Director**
Dawn Shepherd

**Central Chapter
Director**
Mila Baranov

**Southern Chapter
Director**
Debbie Konstantakos

**Northern Chapter
Assistant Director**
Peggy Mobley

**Central Chapter
Assistant Director**
Chris Guerrero

**Southern Chapter
Assistant Director**
Jessica Moore