



MARIN COUNTY SHERIFF'S OFFICE

3501 Civic Center Drive, Room 145, San Rafael, CA 94903

ROBERT T. DOYLE
Sheriff - Coroner
MICHAEL J. RIDGWAY
Undersheriff

CLETS Administration Section
Attention: Dave Sutherland, Marin Representative
P.O. Box 903387
Sacramento, CA 92403-3870

June 26, 2013

Re: CLETS Password Security Compliance

Dear Mr. Sutherland,

At the March CLETS Advisory Committee meeting, the committee directed the Marin County Sheriff's Office to implement software changes on its Computer Aided Dispatch system to comply with CJIS password security policies. The Sheriff's Office and its CAD vendor are currently testing the required software enhancements for password security.

The Sheriff's Office will implement the password security changes before the CLETS Advisory Committee meeting on July 25, 2013. A Sheriff's representative will report to the committee at that meeting that our CAD software is fully compliant with CJIS password security policies.

Sincerely,

Robert T. Doyle, Sheriff

RTD/rpb

AREA CODE 415

24-HOUR NUMBER
473-7233

FAX
473-4126

ADMINISTRATION
473-7250

CIVIL
473-7282

COMMUNICATION
SERVICES
473-7243

CORONER
473-6043

COURTS
473-7393

EMERGENCY
SERVICES
473-6584

INVESTIGATIONS
473-7265

JAIL
473-6655

MAJOR CRIMES
TASK FORCE
884-4878

PATROL
473-7233

RECORDS
473-7284

WARRANTS
473-7297

Memorandum

Date: DRAFT

To: California Law Enforcement Telecommunications System Advisory Committee
State of California Department of Justice
P. O. Box 903387
Sacramento, CA 94203-3870

From: **DEPARTMENT OF CALIFORNIA HIGHWAY PATROL**
Office of the Commissioner

File No.: 001. A14763.041. CLETS Non-Compliance July 2013

Subject: CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM
ADVISORY COMMITTEE COMPLIANCE REPORT

At the request of the State of California Department of Justice (DOJ), California Law Enforcement Telecommunications System (CLETS) Administration Section, the following provides documentation of non-compliance with the CLETS policy, as identified in a CLETS Application Upgrade and in the CLETS audits performed by the DOJ.

During the process of an application upgrade, the DOJ identified non-compliance in the following two areas of policy:

Per DOJ: “All wireless and handheld devices must have a personal/software-based firewall installed and active.”

The California Highway Patrol (CHP) is in the process of replacing existing laptops. It is estimated this will be complete by December 2013, and all laptops will have personal firewall software installed.

Per DOJ: “All systems must audit successful/unsuccessful login attempts and password change attempts for three years.”

This issue has been resolved. The CHP maintains audit records on successful and unsuccessful login attempts for three years.



During audits of CHP facilities, the DOJ identified non-compliance in the following area:

Per DOJ: “Policy requires that if passwords are used to authenticate an individual’s unique ID, the following password requirements must be met:

- 1. be a minimum length of eight (8) characters on all systems;**
- 2. not be a dictionary word or proper name;**
- 3. not be the same as the User ID;**
- 4. expire within a maximum of 90 calendar days;**
- 5. not be identical to the previous ten (10) passwords;**
- 6. not be transmitted in the clear outside the secure location;**
- 7. not be displayed when entered.”**

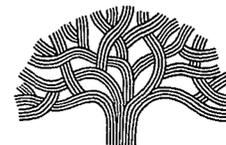
The CHP is currently transitioning between two directory environments, from Novell E-Directory to Microsoft Active Directory, as directed by California Technology Agency. Changing the password during this transition is not possible at this time. Once the transition is complete, the CHP will comply with the required changes. The CHP, Information Technology Section (ITS) estimates the transition will be completed by the end of 2014.

If you have any questions, please feel free to contact Rita Lugo, ITS, at (916) 843-4073.

J. A. FARROW
Commissioner

cc: Information Management Division
Information Technology Section

CITY OF OAKLAND



POLICE ADMINISTRATION BUILDING • 455 - 7TH STREET • OAKLAND, CALIFORNIA 94607-3985

Police Department

Telephone Device for the Deaf (510) 238-7629

July 15, 2013

Department of Justice
CLETS Administration Section
PO Box 903387
Sacramento, CA 94203-3870
Attn: Dave Sutherland

Re: Oakland Police Department – Update regarding the CLETS Network Upgrade Plan

Dear Dave,

I have consulted with Ahsan Baig, the Acting Director of the Department of Information Technology, and he has submitted the attached updated Network Upgrade Plan. This update provides a progress report on the Encryption Compliance issue as well as an update regarding the upgrade of the entire Public Safety System.

Please review the updated plan and let me know if any further information is needed.

A handwritten signature in black ink, appearing to read 'Regina Harris-Gilyard', written over a horizontal line.

Regina Harris-Gilyard
Police Services Manager
Oakland Police Department

ESTIMATED TIMELINE

A detailed timeline will be developed after the vendor selection process is completed.

PHASE	SCOPE	TARGET COMPLETION DATE
I	<p>Selection of a Consultant to develop an RFP – Estimated completion by July 2013 – Estimated Cost \$150K</p> <ul style="list-style-type: none"> • Business, Operational, and Functional Requirements gathering and validation • Technical Specifications and Security Requirements • RFP development 	<p>(March 2013 – Previous Date) July 2013</p>
II	<p>Selection of a Vendor to design and build the Public Safety Network - Estimated completion by September 2014 – Estimated Cost \$3.2M</p> <ul style="list-style-type: none"> • Vendor Selection and validation of proposed designed solution • Scheduling and deployment of solution • Segmentation of DOJ only and other non-law enforcement telecommunications • Network Cutover 	<p>(December 2013 – Previous Date) September 2014</p>
III	<p>Selection of a Vendor to design, build and maintain the Next Generation Public Safety systems - Estimated completion by September 2015 – Estimated Cost \$8.1M</p> <ul style="list-style-type: none"> • Vendor Selection • Staff Report and Council Approval • Design, Build and Maintain Contract Negotiations and sign-off • Statement of Work and Project Plan • Design, Install, Integrate, Test, Train and Final Acceptance • Maintenance Begins 	<p>(July 2015 - Previous Date) September 2015</p>



CONTRA COSTA COUNTY OFFICE OF THE SHERIFF
DAVID O. LIVINGSTON
SHERIFF - CORONER

CLETS Advisory Committee,

The recent Client Services Program audit identified that our agency is not compliant with FBI CJIS Security Policy 5.6.2.1. This Policy requires an eight digit password, cannot be a dictionary word or proper name, cannot be the userid, must be changed every 90 days and cannot be identical to any of the previous 10 passwords. The Contra Costa County Office of the Sheriff will meet these requirements as of September 10th 2013 when we go live with the Tiburon Command CAD version 2.8 and Law Records version 7.9. This version of the Tiburon product gives us the option of setting minimum length of password, requiring a special character (non dictionary word), enforcing non userid password, expiring passwords every 90 days, not allowing the password to match one of the last 10. As I stated above, this system is currently in place and will be live September 10th 2013. If there are any further questions or concerns please contact me at:

Cell (925) 525-8971

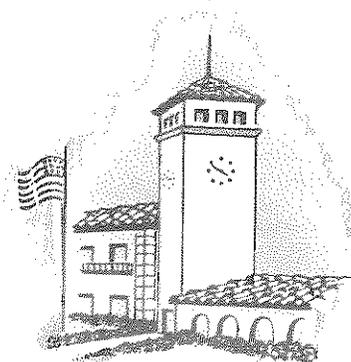
Office (925) 313-2451

E-mail dspin@so.cccounty.us

David Spinelli Agency CLETS Coordinator

David O. Livingston Sheriff

7-2-13



City of
HUNTINGTON PARK California
POLICE DEPARTMENT

6542 MILES AVENUE, HUNTINGTON PARK, CALIFORNIA 90255-4386
TEL. (323) 826-6629 • FAX (323) 826-6680

JORGE CISNEROS
CHIEF OF POLICE

July 1, 2013

Teresa Mora, Analyst
California Department of Justice
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203-3870

Dear Ms. Mora:

In response to your e-mail dated June 24, 2013, the following action has been taken by our agency to come into compliance with the California Law Enforcement Telecommunications System (CLETS) and National Crime Information Center (NCIC) policies.

QUESTION 3.15 FBI CJIS Security Policy 5.10.1.2 – The 128-bit encryption requirement was completed on or about May 01, 2013. This will cover all communication between the mobile unit and the message switch.

The NIST FIPS 140-2 requirement is pending as we have a conference call set with a vendor and our IT staff on 07-02-13. We are also in the process of obtaining funding approval through an existing grant and that process should be complete in the near future. It is anticipated that the necessary encryption requirements will be met in approximately three to four months if not sooner.

If we can be of further assistance to you, please contact me, Tuesday through Friday, 8:30 a.m. to 6:30 p.m. at 323-826-6649.

Sincerely,

A handwritten signature in black ink, appearing to read "Jorge Cisneros", is written over a horizontal line.

JORGE CISNEROS
Chief of Police



1350 Norris Road
Bakersfield, California 93308-2231

June 28, 2013

California Department of Justice
CLETS Administration Section
Attn: Teresa Mora, Staff Information Systems Analyst
P.O. Box 903387
Sacramento, CA 94203-3870

Re: Notice of Actions Being Taken to Achieve Compliance with Password Security Requirements - Primary ORI #CA0150000

Dear Ms. Mora,

Below you will find a list of the actions our office is taking to achieve full compliance with the FBI CHS Security Policy 5.6.2.1 as you requested. We anticipate these solutions to be in place no later than August 30, 2013. This date should allow sufficient time for receipt, set-up, testing, training, and implementation of the newly purchased equipment; however, we are working to get this solution in place as soon as possible.

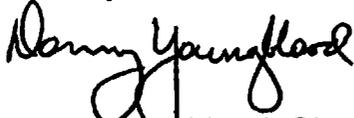
Password Application Software and Advanced Authentication - Our office has purchased a Password Application from Digital Persona that will be utilized on all office and mobile data computers. This application requires users to sign in using a unique PIN code followed by a fingerprint scan to meet the two-factor Advanced Authentication requirement. The software will require users to create a new master PIN code every 90 days and require the PIN codes, at a minimum, to meet all criteria as listed in FBI CJIS Security Policy 5.6.2.1.

After users are signed in to this application, the application itself will automatically assign, maintain, and change passwords in all other applications used by our office as set to our password combination security specifications. All subsequent applications will be set at a minimum to meet the same requirements as the password application itself. Furthermore, this product has been purchased by our Regional Area Network committee and the equipment and software will be

distributed to all our allied agencies for use on all their office and mobile computers. Our Security Point Of Contact, Kevin Fisher, has been in contact with the technical staff at California DOJ and NCIC and has received confirmation that this product meets all security requirements and is a viable option.

Once this solution has been successfully implemented, I will send a letter of notification to your office. If you have any further questions please feel free to contact me.

Sincerely,

A handwritten signature in black ink that reads "Donny Youngblood". The signature is written in a cursive, flowing style with a large, prominent initial "D".

Donny Youngblood, Sheriff
County of Kern

/jbm



Erroy D. Bava, Sheriff

County of Los Angeles
Sheriff's Department Headquarters

4700 Ramona Boulevard
Monterey Park, California 91754-2169



July 2, 2013

Teresa Mora, Staff Information Systems Analyst
California Department of Justice - CLETS Administration Section
Post Office Box 903387
Sacramento, California 94203-3870

Dear Ms. Mora:

The purpose of this letter is to provide you with a quarterly status report on the efforts the Los Angeles County Sheriff's Department (LASD) has taken to address compliance issues relating to CLETS security policy compliance. Specifically, the following issues have been raised:

Issue: The LASD does not comply with the authentication policy on their local, public, and wireless network segments. Passwords did not expire at least once every 90 days. It is recommended that passwords used for authentication follow the secure password attributes on the local, public, and wireless network segments.

Status: This issue has been resolved/completed as of June 1, 2013.

Issue: The LASD's Mobile Data Terminal (MDT) dispatch system does not provide the minimum recommended 128 bit NIST certified encryption.

Status: Working on issue. Expected completion July 2014.

In 2011, the LASD entered into a contract agreement with Raytheon Corporation to replace all MDTs with new Mobile Data Computers (MDCs). The new MDCs meet all security policies and procedures. The MDT replacement project is now fully underway and over 1722 MDCs have been deployed. The department plans to deploy 70 MDCs a month until all MDTs have been replaced. The new MDC network uses NetMotion to encrypt the traffic end-to-end which meets NIST certified encryption standards. Additionally, all fixed CLETS devices do not use the county microwave system. All CLETS fixed devices use fully encrypted WAN links. The MDC Deployment schedule has been delayed to July 2014 due to technical issues with the current MDCs.

A Tradition of Service Since 1850

Production and deployment will resume after these technical issues are resolved. Due to these recently discovered technical issues, the Department will not be able to meet the initial July 2013 completion date. The Department will make every effort to expend resources to ensure that we meet the new expected project completion date of July 2014.

Issue: The LASD's Mobile Data Terminal does not utilize personal firewalls on their access devices on wireless network segment.

Status: *Working on issue. Expected completion July 2014.*

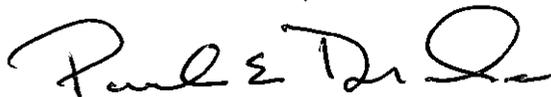
Conversion to the new MDC's as stated above will provide for personal firewalls and address this issue.

Issue: The LASD's Mobile Data Terminal does not utilize virus protection software on the wireless devices.

Status: *Working on issue. Expected completion July 2014.*

Sincerely,

LEROY D. BACA, SHERIFF

A handwritten signature in black ink, appearing to read "Paul E. Drake". The signature is written in a cursive, flowing style.

Paul E. Drake, Captain
Data Systems Bureau



South Bay Regional Public Communications Authority
4440 West Broadway • Hawthorne, California 90250



Via Email: Teresa.mora@doj.ca.gov

June 27, 2013

Ms. Teresa Mora
California Department of Justice
Bureau of Criminal Information and Analysis
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203

Re: South Bay Regional Public Communications Authority

Dear Ms. Mora:

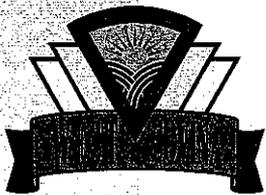
Please be advised of the South Bay Regional Public Communications Authority's status on the following: We have finalized the selection of the Mobile VPN/Encryption Software (Netmotion). We are finalizing an RSA Fob Based Two Factor Authentication System, a Microsoft System Center End Point Protection Anti Virus/Firewall Package and a Windows Update Services Patch Management Solution. Additionally, we are physically separating the administrative and dispatch networks. We are in the process of creating the CLETS upgrade application for presentation to Los Angeles County Sheriff's Department and the CLETS Advisory Committee and anticipate proof of concept installation in early August pending approval. Operations Manager Shannon Kauffman (skauffman@rcc911.org) and/or Administration Supervisor John Krok (jkrok@rcc911.org) will attend the CLETS Advisory Committee meeting on July 25th.

Sincerely,

A handwritten signature in black ink, appearing to read "SKA", written over a white background.

Shannon Kauffman
Operations Manager

JA:JR/ww



PAUL LACOMMARE
Chief of Police

July 8, 2013

California Department of Justice
Attn: Teresa Mora
P.O. Box 944255
Sacramento, CA 94244-2550

Dear Teresa Mora:

We are aware of the current standard authentication (password) credentialing. They include:

1. Minimum length of eight (8) characters.
2. Not a dictionary word or proper name.
3. Not be the same as the user identification.
4. Expire within a maximum of ninety (90) calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

My staff is actively working on the code changes required for this to occur. Our current plan is to have the aforementioned requirements implemented by August 31, 2013.

Sincerely,

Paul LaCommare
Chief of Police



HUMBOLDT COUNTY SHERIFF'S OFFICE

MICHAEL T. DOWNEY, SHERIFF

MAIN STATION

CIVIL/COURTS
(707) 445-7335

826 FOURTH STREET • EUREKA CA 95501-0516
PHONE (707) 445-7251 • FAX (707) 445-7298

CUSTODY SERVICES
(707) 441-5159

6/25/2013

To whom it may concern,

This letter is to provide an update of progress toward meeting password security compliance addressed in our agency's recent audit.

The current message switch for Humboldt County is unable to be programmed to meet current password parameters.

We have selected a vendor that best meets our needs to replace our message switch and bring us into compliance.

We have included the purchase in the 2013/2014 fiscal year budget which takes effect July 1, 2013. At this time we will proceed with the purchasing process and installation. Current estimates for a completion date are September 2013.

Thank you,

A handwritten signature in cursive script that reads "Cheri Williams".

Cheri Williams

ACC, Humboldt County Sheriff's Office





CITY OF
CARLSBAD
Police Department
Office of the Chief of Police

June 27, 2013

Michelle D. Mitchell
CLETS Administration
Department of Justice, CLETS Administration
PO Box 903387
Sacramento, CA 94203-3870

Dear Ms. Mitchell,

I write this letter to update you on the status of our compliance with the CJIS Security Policy. As you know, Carlsbad Police Department's current CAD and Mobile system was installed in May of 2005 and does not provide the functionality required to meet the password requirements of CJIS Security Policy Version 4.5, Section 7.3.3.

In order to achieve compliance, we negotiated an agreement with our CAD vendor, Tiburon, for an upgrade that would provide the functionality necessary to meet the password requirements. The agreement specified that all CAD and Mobile servers were to be implemented on an industry-standard virtual platform. We began the upgrade implementation in June of 2012 but Tiburon was unable to complete the project due to an incompatibility with virtual servers. The Police Department then began to negotiate new terms to the upgrade agreement and develop a new project plan. In May of 2013 the Carlsbad City Council approved a new agreement with Tiburon with an expected completion date of December 2013.

During the months of May and June 2013, we have made substantial progress. We have redeployed all of the virtual servers necessary for the new environment and purchased the physical server necessary for the main CAD application server. Our staff has attended the CAD mapping training and begun development of our dispatch and patrol maps. We expect to install the new physical CAD server in July and begin data conversion and testing.

The Carlsbad Police Department will attend the next CAC meeting in July to request an extension, further explain the reasons for our delay in achieving compliance, and to answer any questions the committee members may have. We recognize the importance of being in compliance and will work diligently with Tiburon to complete the upgrade. We have attached a timeline of completed and future milestones and ask for your consideration to have the deadline for compliance be extended to December of 2013.

Thank you in advance for your consideration of this matter. Please feel free to contact our Safety IT Manager, Maria Callander, at 760 931-2176 if you have any questions or concerns regarding this request.

Sincerely,

A handwritten signature in black ink, appearing to read "Gary W. Morrison", written over a horizontal line.

Gary W. Morrison
Chief of Police



Police Department

2560 Orion Way | Carlsbad, CA 92010 | 760-931-2131 | 760-931-8473 fax

Completion Date (** Expected)	Description
May 2005	Current Tiburon CAD and Mobile system went into production
April 2011	Reached an agreement with Tiburon Inc. to complete upgrade of CAD and Mobile system on virtual servers.
December 2011	Began project planning with CAD vendor
January 2012	Carlsbad submitted DOJ application for CAD upgrade
February 2012	Carlsbad purchased and installed server hardware for CAD upgrade
April 2012	Carlsbad purchased Imprivata advanced authentication hardware and software and began installation
June 2012	Carlsbad received approval from Department of Justice for CAD upgrade
June 2012	Tiburon deploys new CAD, Mobile, Mapping, and Interface application software in Carlsbad virtual environment
June 2012	Tiburon announces that they will no longer support the virtualization of the CAD application.
June 2012	Due to Tiburon's lack of support of the upgraded CAD and Mobile system, the City begins negotiating a new project plan and projected completion date
August 2012	In expectation of reaching an agreement, Carlsbad conducts and completes all administrator and user training on the new system.
March 2013	Carlsbad and Tiburon meet to discuss terms for the resumption of upgrade activities.
May 2013	Carlsbad City Council approved amended upgrade agreement with Tiburon
May 2013	Redeployment of Tiburon CAD and Mobile software upgrades on virtual servers
June 2013	Physical server purchased for CAD application server
June 2013	CAD mapping redeployed and staff retrained on software
July 2013 **	Preliminary data conversion and testing
August 2013**	Retraining of administrators and implementation team.
Oct-Nov 2013**	Retraining of all police personnel in use of new CAD and mobile software
November 2013**	Final data conversion and testing
December 2013**	Final Cutover to upgraded system



**Modesto Police Department
Implementation Plan
Advanced Authentication – FBI CJIS Security Policy Section 5.6.2.2
June 26, 2013**

Dear Ms. Mitchell:

Below are the steps that the Modesto Police Department will be performing to ensure compliance with Advanced Authentication on wireless mobile data computers (MDC) CLETS devices as required by the FBI CJIS Security Policy Section 5.6.2.2

Our Public Safety System software vendor (Tiburon) has scheduled an update to our current MDC software in the next few months. It is our intention to implement Advanced Authentication during this update.

- **Step 1.**
Contact Vendors and determine which solution Modesto PD will move forward with (fingerprint reader / Security token – key fob)
The decision was made to proceed with Security Tokens for our Advanced Authentication solution.
- **Step 2.**
 - Set up and test devices in a controlled environment prior to implementation to insure functionality and network security
Estimated completion date September 1, 2013
- **Step 3.**
 - Submit Purchase Request for devices chosen for the advanced authentication solution
June 20, 2013 Purchasing has sent out Security Token requirements for bid. Estimated completion date August 15, 2013.
- **Step 4.**
 - Implement Advanced Authentication on the Mobile Data computers during the system upgrade by Tiburon.
Estimated completion date November 30, 2013

**City of Modesto
Police Department**

600 Tenth Street
Modesto, CA 95354
(209) 572-9500
Fax (209) 523-4082

Hearing and Speech
Impaired Only
TDD (209) 526-9211

Administration Division

(209) 572-9501
(209) 572-9669 Fax

Investigations Division

(209) 572-9551
(209) 572-0741 Fax

Operations Division

(209) 572-9565
(209) 572-9656 Fax

Support Division

(209) 342-9164
(209) 572-9669 Fax

Galen L. Carroll
Chief of Police

06-26-13
Date



City of Palm Springs

Police Department
200 South Civic Drive · Palm Springs, California 92262
Tel: (760) 323-8116 · Fax: (760) 323-8178 · TDD (760) 864-9527

June 30, 2013

Michelle D. Mitchell, CLETS SISA
Department of Justice – Hawkins Data Center
Technology Support Bureau
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203-3870

RE: Palm Spring Police Department – Implementation Plan

Dear Ms. Mitchell:

I am submitting this update report on the two items which were preventing us from being fully compliant.

1) FBI CJIS Security Policy Section 5.2:

Our agency now has a Security Awareness Training Plan in place pursuant to the FBI CJIS Security Policy Section 5.2. We will begin implementation of the Plan on July 1, 2013 with a completion date of July 15, 2013. We will continue this training on a biennial basis. Please find our Policy attached.

2) FBI CJIS Security Policy Section 5.3:

Our agency now has an established Incident Handling Plan in place pursuant to FBI CJIS Security Policy Section 5.3. This was completed on June 6, 2013. Please find our Policy attached.

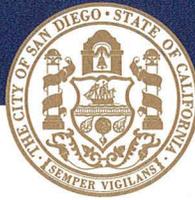
In regard to Item 1 above, we are still in the process of procuring and implementing Advanced Authentication (AA) for the computers in our police vehicles. It is our intent to have this in place by the deadline of September 30, 2013.

I appreciate your patience on this matter.

Sincerely,


ALBERTO FRANZ, III
Chief of Police

ALF:dem



THE CITY OF SAN DIEGO

IN REPLYING
PLEASE GIVE
OUR REF. NO.

July 9, 2013

Keith Dann
CLETS Executive Secretary

Re: Extention Update for SDPD

Mr. Keith Dann;

The San Diego Police Department submitted an application for CLETS Upgrade in 2010. After approval, some specific questions were raised by DOJ in regards to the FIPS requirements. Specific action items identified and SDPD has been working towards full compliance, documenting our efforts and progress. Two items remain: AD Login and Complex Password.

When the Department deployed the security changes as planned, new modems and new MCT client software were implemented resulting in intermittent application errors. Initial results indicated a problem with our message switch so deployment continued while working on a solution. It was later determined to be an application error. The impact of the error caused police officers to drop connectivity resulting in an officer safety issue. The decision was made to mitigate the operational impact through re-deployment rather than leave these faulty units in service. This required adjustments to the already completed commands and resulted in a delay of approximately four months. The Department is now re-engaged in the implementation of the balance of commands. The current configuration has demonstrated acceptable stability. We are currently 70% complete and now estimating October 2013 for full compliance.

If you have any questions, please contact our department ACC, Karen Goodman at (619) 531-2392 or via email at kgoodman@pd.sandiego.gov.

Sincerely,



William Lansdowne
Chief of Police
San Diego Police Department



Office of the Chief of Police

1401 Broadway • San Diego, CA 92101-5729

Tel (619) 531-2000

