



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

CLETS Advisory Committee,

We are pleased to inform you that we are now in compliance with FBI CJIS Security Policy 5.6.2.1. If you have any further questions or concerns please contact me at:

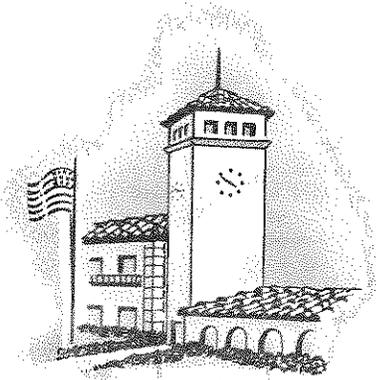
Cell (925) 525-8971

Office (925) 313-2451

e-mail [dspin@so.cccounty](mailto:dspin@so.cccounty)

David Spinelli Agency CLETS Coordinator  \_\_\_\_\_

David O. Livingston Sheriff  \_\_\_\_\_



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

October 31, 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 October 15, 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.

The Huntington Park Police Department installed encryption software that meets the FIPS 140-2 standard per 5.10.1.2 of the FBI CJIS Security Policy on October 21, 2013.

The Huntington Park Police Department has also installed Advanced Authentication software per 5.6.2.2 of the FBI CJIS Security Policy on October 25, 2013.

If we can be of further assistance to you, please contact Lieutenant Martinez 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

August 28, 2013

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

Re: Notice of Compliance with Password Security Requirements - Primary ORI  
#CA0150000

Dear Ms. Mora,

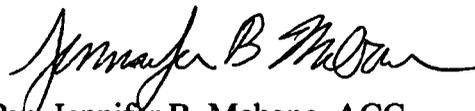
This letter serves as notice that the Kern County Sheriff's Office has achieved full compliance with the FBI CHS Security Policy 5.6.2.1 as required due to the results of the Security Audit conducted in February of 2013. We are happy to inform you that all systems that are used to access CLETS now require passwords to be at least 8 characters in length, passwords must include a certain number of specific character types to enhance security, and passwords cannot be repeated in less than 10 cycles.

This change has been implemented with all CLETS applications used by the Kern County Sheriff's Office. As a result of the changes made within the Sheriff's Office applications, all allied agencies currently accessing CLETS through the Kern County Sheriff's Office are required to comply with the password security requirements listed above. Therefore, all allied agencies behind the Sheriff's Office switch are now in compliance with this security policy as well.

Should you need any additional information regarding this issue, please do not hesitate to contact us.

Sincerely,

Donny Youngblood, Sheriff-Coroner

A handwritten signature in black ink, appearing to read "Jennifer B. Mebane".

By: Jennifer B. Mebane, ACC  
Communications Section

A handwritten signature in black ink, appearing to read "Bryan G. Armendariz - Lt. #450".

By: Bryan G. Armendariz, Lieutenant  
Communications Section



# City of Palm Springs

Office of the Chief of Police

200 South Civic Drive • Palm Springs, California 92262

Tel: (760) 323-8126 • Fax: (760) 323-8173 • TDD: (760) 864-9527 • Web: www.pspd.com

October 28, 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 Springs Police Department: AA Implementation Plan Update

Dear Ms. Mitchell:

I am submitted this update report regarding the implementation of our Advanced Authentication (AA).

1) FBI CJIS Security Policy Section 5.2:

On October 22, 2013, we completed installation and implementation of Advanced Authentication (AA) for the computers in our police vehicles.

This should satisfy all requirements and make us fully compliant. Thank you for your continued patience in this matter.

Sincerely,

  
ALBERTO FRANZ, III  
Chief of Police

ALF:BAB:rm

*"The men and women of the Palm Springs Police Department, empowered by and in partnership with the community, are dedicated to providing professional, ethical, and courteous service to all."*

Post Office Box 1830 • Palm Springs, CA 92263-1830



## THE CITY OF SAN DIEGO

IN REPLYING  
PLEASE GIVE  
OUR REF. NO.

October 31, 2013

Keith Dann  
CLETS Executive Secretary

Re: SDPD Upgrade Application Compliance Complete

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. SDPD has been working towards full compliance, documenting our efforts and progress. In July 2013 San Diego asked for a three month extension to complete the remaining two items: AD Login and Complex Password. At that time we were 70% complete.

As of today we are 100% complete and in 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](mailto:kgoodman@pd.sandiego.gov).

Sincerely,



William M. Lansdowne  
Chief of Police  
San Diego Police Department



August 21, 2013

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

Dear Teresa Mora:

The West Covina Police Department has completed and implemented the CJIS password requirements, which include the following:

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.

Sincerely,

Paul LaCommare  
Chief of Police



Leroy D. Baca, Sheriff

*County of Los Angeles*  
**Sheriff's Department Headquarters**

4700 Ramona Boulevard  
Monterey Park, California 91754-2169



October 21, 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:

**OCTOBER 2013 - MONTHLY REPORT**  
**SECURITY COMPLIANCE MANDATE FOR MOBILE DATA COMPUTERS**

On July 25, 2013, the California Law Enforcement Telecommunications System (CLETS) Advisory Committee requested monthly status updates from the Los Angeles County Sheriff's Department in reference to compliance with encryption of network traffic, anti-virus, and firewall standards for the Department's Mobile Data Computer (MDC) environment.

This report serves as the activities done in the month of October by the Department to work towards our compliance mandate.

1. Completed revised MDC software baseline that will allow for remote security patch deployment over the Sheriff Data Network (SDN) to the MDC. This activity required extensive testing and configuration with the Microsoft System Center Configuration Manager (SCCM) platform. The month of October required comprehensive field testing in a variety of scenarios to ensure security patch deployment and remote imaging can be done in an efficient manner and to solidify workflow. The testing is being done at a patrol station in production use. The SCCM platform will allow the Department to remotely deploy critical security patches for the MDCs enterprise wide. The field testing is expected to continue through the end of October.
2. The Department deployed an additional 34 MDCs to field operations. These MDCs meet encryption, anti-virus, and firewall mandates. After the revised

*A Tradition of Service Since 1850*

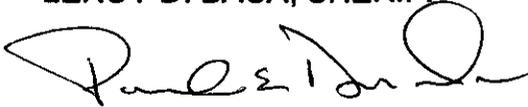
software baseline is internally approved after the 30 days of field testing (refer to Item 1 above), the Department is expected to deploy approximately 125 MDCs per month at full capacity using the SCCM platform.

3. The Department is currently testing network site fail over between the Department's data centers. This will allow for redundancy and load balancing for network traffic. This activity will span over the next couple of months to ensure all network traffic is routed appropriately through our secure encrypted transport layer.

Should you have any questions or require additional information, please contact me at (562) 345-4351.

Sincerely,

LERROY D. BACA, SHERIFF

A handwritten signature in black ink, appearing to read "Paul E. Drake". The signature is fluid and cursive, with a large loop at the end.

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](mailto:Teresa.mora@doj.ca.gov)

October 23, 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: Status Update for SBRPCA Infrastructure upgrade for CLETS Compliance

As of October 21, 2013 New electrical has been installed for the both the Cisco Core switch as well as the new server rack. Installation of the new servers and core switch is scheduled for October 24. The cores switch will be configured and tested with the existing switch still in operation. Once the configuration is verified a cutover will be scheduled and completed.

As of October 3<sup>rd</sup>, 2013 The Cisco 6509 has been assembled and is ready for installation and configuration. Additional power is required to power this switch before that can happen. A site walk was conducted in order to determine the power requirements for this installation, and a proposal is currently being generated. It was noted that SFP fiber blade for this switch will also be required but has not been procured as of this date. Installation of the 6509 will commence after the installation of additional power.

As of August 23, 2013 the design and bill of materials for the network and server infrastructure has been completed. Most of the new equipment has been purchased and received at the SBRPCA facility. Our key milestones for this project are listed below:

- Order and Delivery of all equipment (Servers and Network)
- Deployment of new network infrastructure
- Deployment of new server infrastructure
- Order and Installation of new Internet circuit from SBRPCA
- Deployment of NetMotion
- Deployment of two-factor authentication

We are slated to begin the new server deployment (physical hardware install and initial configuration) in the next month. The network infrastructure upgrade will be scheduled when the rest of the hardware has arrived.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ralph Mailloux'.

Ralph Mailloux  
Executive Director

JA:ww

Enclosures: South Bay Regional Public Communications Authority Active Directory Logical Core Design  
SBRPCA CLETS NETWORK (CURRENT)



ESTABLISHED 1850

# CITY OF VACAVILLE

650 MERCHANT STREET  
VACAVILLE, CALIFORNIA 95688-6908  
www.cityofvacaville.com

STEVE HARDY  
Mayor

DILENNA HARRIS  
Vice Mayor

CURTIS HUNT  
Councilmember

MITCH MASHBURN  
Councilmember

RON ROWLETT  
Councilmember

October 30, 2013

Executive Secretary  
CLETS Advisory Committee  
P.O. Box 903387  
Sacramento, CA 94203-3870

Dear CAC Members:

Please accept this letter as our implementation plan, with a projected completion date of January 1, 2014, for our agency to be in compliance with the password policy as described in the FBI CJIS Security Policy 5.6.2.1. We have been in contact with our CLETS representative Teresa Mora and she is familiar with our situation.

Our Communications Center is currently using VisionAir CAD version 3.5.13.3 to access our direct connect CLETS system. We are behind schedule in implementing our CAD releases. Our vendor assures us with release version 3.6.4 or higher we will be completely CJIS compliant. We've discussed this issue with our Information Technology Division and they have put this project at the top of their list. They are already working with VisionAir to complete installing the releases. Each step involves a two to three week final testing phase before we move to the next step in order to troubleshoot any interface issues. We have completed Step 3 and Step 6 should bring us to release version 3.6.4.

If there is any other information you need from us please let me know. Thank you for your consideration in this matter.

Sincerely,

Richard L. Word  
Chief of Police  
Vacaville Police Department

Supervisor Bette Burnham  
Agency CLETS Coordinator  
Vacaville Police Department



CITY OF  
**CARLSBAD**  
Police Department

**Office of the Chief of Police**

October 1, 2013

CLETS Administration  
Michelle D. Mitchell  
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, the CLETS advisory committee approved our request for an extension at the July meeting and we continue to make progress in meeting our compliance deadline of December 2013.

The City of Carlsbad's current CAD and Mobile system was installed in May of 2005 and does not provide the functionality required to meet the password requirement in 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 July, August and September, we have made substantial progress. We completed preliminary data conversion, conducted training for system administrators and the implementation team. We are currently testing the functionality of the new system in preparation for user training. I have attached a table showing our progress and the expected completion dates of milestones.

Thank you in advance for your consideration of this matter. Please feel free to contact me at 760 931-2131 if you have any questions 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

Attachment



**Police Department**

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

<b>Completion Date (** Expected)</b>	<b>Description</b>
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
September 2013	Retraining of administrators and implementation team.
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



City of Coronado, California

# POLICE DEPARTMENT

**JON FROOMIN, CHIEF OF POLICE**

"Commitment to Community Through Professionalism, Integrity, Respect and Teamwork"

October 1, 2013

Michelle D. Mitchell, Staff IS Analyst  
Department of Justice  
CLETS Administration Section  
P.O. Box 903387  
Sacramento, CA 94203-3870

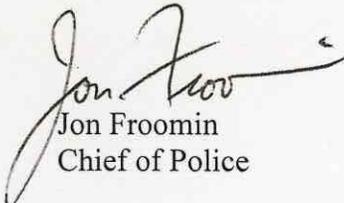
Re: Advanced Authentication Compliance for Coronado Police Department

Dear Michelle,

The City of Coronado Police Department understands the FBI's CJIS Policy section 5.6.2 requires agencies to implement advanced authentication (AA), also called "two factor authentication," in mobile devices used outside of secure locations to access CJIS services and systems. Over the past two months, we have been in contact with a few other California agencies regarding their AA solutions and with manufacturers and resellers of AA products. We have narrowed down the two possible AA solutions to 2FA and Imprivata, while also identifying NetMotion's persistent VPN product as an important network authentication/connection method to round out the secure solution.

Our plan is to finalize the product choices by January 1, 2014, request Council authorization for the purchase by March 4, 2014, begin implementation by April 28, 2014, and complete implementation by June 30, 2014. If required, we will provide project updates to the DOJ at three-month intervals.

Sincerely,

  
Jon Froomin  
Chief of Police



## Modesto Police Department Implementation Plan

Advanced Authentication – FBI CJIS Security Policy Section 5.6.2.2  
October 7, 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.**
  - Submit Purchase Request for devices chosen for the advanced authentication solution. **Purchase request approved, tokens were ordered and Modesto PD received the tokens September, 2013.**
- **Step 3.**
  - Set up and test devices in a controlled environment prior to implementation to insure functionality and network security. **Meeting scheduled with vendor to begin set-up and testing on October 23, 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

10-14-13  
Date



# ORANGE COUNTY SHERIFF'S DEPARTMENT

550 N. FLOWER STREET  
SANTA ANA, CA 92703  
714-647-7000  
WWW.OCS.D.ORG

SHERIFF-CORONER  
SANDRA HUTCHENS

## OFFICE OF THE SHERIFF

November 7, 2013

Ms. Michelle Mitchell  
CLETS Administration  
Department of Justice  
Audits, Inspections and Training Program  
Bureau of Criminal Identification and Investigative Services  
4949 Broadway, B114  
Sacramento, California 95820

Re: Implementation of Strong Passwords – ORI #CA0300000

Dear Ms. Mitchell:

This letter is to provide DOJ with an update on our progress towards compliance with the CLETS/NCIC strong password requirement. The Orange County Sheriff's Department continues to actively work on our strong password solution.

As the County Control Agency, we provide ELETE (our CLETS interface software) to 50 client agencies. Currently password management is handled directly on the mainframe for OCS.D users and through an internal web interface for our client agencies. With the implementation of strong passwords, we have developed a solution which will incorporate internal and external agencies through a single security application. We expect to deploy this solution within OCS.D by December 2013, and then to our external clients over the first six months of 2014.

At this time, the development of our strong password application is complete and is now going through our quality assurance review/testing. Starting the second week of December, OCS.D will be rolling out a new version of ELETE internally that directs end-users to update their passwords to the DOJ/NCIC mandated password criteria. We also have the new ELETE installed in one of our client agencies and testing is nearly complete. Once the internal roll out is complete, we will immediately begin working with our remaining client agencies on the same process. It is estimated this project is 80% complete. Please consider allowing our agency an extension to ensure a smooth transition to strong passwords, countywide, no later than July 1, 2014.

Ms. Michelle Mitchell  
Page 2  
November 7, 2103

If you have any questions regarding the implementation, please contact our CIO, Kirk Wilkerson at [kwilkerson@ocsd.org](mailto:kwilkerson@ocsd.org) or (714) 834-6450. Kirk will be attending the November CAC meeting to provide you with an update on our progress and respond to any questions the CAC may have.

Sincerely,



Sheriff Sandra Hutchens

SH/bf

Cc: Kirk Wilkerson  
Ed Lee  
Irene Smith



**OFFICE OF THE SHERIFF  
CITY AND COUNTY OF SAN FRANCISCO**

**1 DR. CARLTON B. GOODLETT PLACE  
ROOM 456, CITY HALL  
SAN FRANCISCO, CALIFORNIA 94102**



**Ross Mirkarimi  
SHERIFF**

**November 7, 2013  
Reference: 2013-227**

**Michelle D. Mitchell  
California Department of Justice  
CLETS Administration  
4949 Broadway  
Sacramento, CA 95817**

**Dear Ms. Mitchell,**

**This letter is an amendment to our October 18<sup>th</sup> letter to update you on the status of outstanding issues which came to light as a result of the FBI CJIS audits conducted last year.**

- Issue 1: Security Awareness training for IT and private contractors. This issue was resolved in May 2013**
- Issue 2: Advanced authentication on laptops and remote connections. This issue was resolved in April, 2013**
- Issue 3: Encryption meeting NIST certification in accordance with FIPS 140-2 on segments utilizing public, wireless and Internet network segments transmitting CJI (CLETS data).**

**Proposed Amended Resolution: The Department is has installed in cooperation with the City's Department of Technology, new Netscaler devices that are FIPS 140-2 compliant. These devices are now configured but are not being used as yet pending a CLETS upgrade application which we submitted at the end of October. Based on discussions between your office and my I.T. staff, we are going to implement the use of these compliant devices in advance of the application based on your approval to do so ahead of the application approval. We began the transition to the new devices last week and will have all the Department's users provisioned**

**PHONE: 415-554-7225 FAX: 415-554-7050**

**WEBSITE: WWW.SFSHERIFF.COM**

**EMAIL: SHERIFF@SFGOV.ORG**

using the new access by December 2, 2013. Thank you for your guidance and patience during this large and costly project and to bring the San Francisco Sheriff's Department into compliance.

If you have any questions regarding this information please do not hesitate to contact Lieutenant David Hardy at (415) 575-4449.

Sincerely,



---

ROSS MIRKARIMI  
Sheriff

cc: Chief of Staff



# HUMBOLDT COUNTY SHERIFF'S OFFICE

MICHAEL T. DOWNEY, SHERIFF

CIVIL/COURTS  
(707) 445-7335

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

CUSTODY SERVICES  
(707) 441-8159

10/21/2013

To whom it may concern,

This letter is to provide an update of progress toward meeting password security compliance.

The current message switch for Humboldt County is unable to be programmed to meet current password parameters. We have chosen a vendor that can address the password compliance issues.

When the vendor was chosen, funding solutions were sought and in July 2013 the expenditure for a new message switch was approved for the 2013/14 budget cycle.

It was originally projected that once funding was acquired the purchase and installation would take approximately two months. Those projections were ambitious at best and we have failed to meet the September target date.

I have been advised that currently the county and vendor are reviewing contracts and an upgrade application is in development.

The vendor has provided the county a scope of work. The vendor is projecting delivery in February 2014 with training and testing to be completed by the end of March 2014.

Thank you,

Cheri Williams, ACC, Humboldt County Sheriff's Office

Michael Downey, Sheriff, Humboldt County