

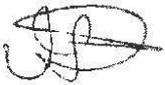
## Memorandum

*Flex your power!  
Be energy efficient!*

To: WILLIAM E. LEWIS  
Assistant Director  
Audits and Investigations

Date: April 29, 2014

File: P3020-069

From:  GIGI SMITH  
Chief Information Officer  
Information Technology

Subject: 365-DAY RESPONSE TO FINAL AUDIT REPORT ON SOFTWARE MANAGEMENT PROGRAM

Information Technology has attached the 365-Day Audit Response in response to the Audits and Investigations' report entitled *P3020-069 Final Audit Report on Software Management Program, February 25, 2013*. Submission of this response constitutes our report requirement subsequent to the audit.

Please contact Emmil Simeroth at (916) 653-2031 or Dave Miles at (916) 654-5962 if you have any questions or need additional information.

### Attachments

IT 3-Day Response to February 25, 2013 Final Audit Report on Caltrans Software Management Program

c: Francesca Negri, Chief, Division of Procurements and Contracts  
Jacob Ellwood, Chief (Acting), Security Division, Information Technology  
Laurine Bohamera, Chief, Internal Audits, Audits and Investigations  
Carolyn Pennington, Chief, IT Management Support Office, Information Technology  
Emmil Simeroth, Chief (Acting), Office of ITAM & IT Cert, IT Management Support Office, Information Technology  
Kevin Yee, Internal Audit Manager, Internal Audits, Audits and Investigations  
David Wong, Auditor-in-Charge, Internal Audits, Audits and Investigations  
Veronica Kaldani, Auditor, Internal Audits, Audits and Investigations  
Dave Miles, IT Asset Management Lead, Office of ITAM & IT Cert, IT Management Support Office, Information Technology

Attachment (1)

IT 365-Day Response to February 25, 2013 Final Audit Report  
On Caltrans Software Management Program

Finding 1

Caltrans' Software Management Policy Annual Statement of Compliance Has Not Been Retained or Supported with a Hardcopy of the Software Inventory

Recommendation I.1

ITAM prepares and retains the Annual Certification and inventory summaries for at least three years.

Response 1.1

HQ IT Asset Management (HQ ITAM) prepares the SMP Annual Statement of Compliance after preparing the Software Management Plan (SMP) in December of every year. The SMP's "*Annual Statement of Compliance*" is signed by the Director or the Director's Designee at the end of January of the following year.

COMPLETED ACTION (Emmil Simeroth): HQ ITAM and the Office of the CIO will retain electronic and hard copies of both documents for at least three years. Projected completion date: January 31, 2014.

There was no 2010 SMP Annual Statement of Compliance retained.

- 2011 SMP Annual Statement of Compliance is retained
- 2012 SMP Annual Statement of Compliance is retained
- 2013 SMP Annual Statement of Compliance is retained
- 2014 SMP Annual Statement of Compliance was retained in January 2014

Recommendation 1.2

ITAM prepares an annual software inventory report to support the Annual Certification

Response 1.2

Caltrans IT is installing ZENworks Agents on Caltrans' Macintoshes, Windows servers, UNIX/LINUX servers, computers, workstations and laptops. Future inventory summary reports will add software installation counts for these devices to the installation counts of software on Windows PCs.

COMPLETED ACTION (Emmil Simeroth): ITAM has prepared electronic and hardcopy annual inventory summary reports of all software installed on Caltrans computers and servers in December of every year and retain them for at least three years.

- Completion date: December 31, 2013
- There was no electronic or hardcopy 2011 SMP annual software installation inventory summary report retained.

- 2012 SMP Baseline Inventory 12-9-2011 by District report is retained
- 2013 SMP Installation Counts of All Software – 20121203 report is retained
- 2014 SMP Software Inventory Report was retained in January 2014

## Finding 2

Caltrans' Software Management Plan (SMP) has not been fully implemented.

### Recommendation 2.1

ITAM & IT Cert Office collaborates with DPAC to:

Track licenses of all procured software.

Identify the license terms and the unit, group, and individual responsibility for remediation.

Document the remediation strategy and to:

Ensure that all Caltrans' contractors have appropriate controls in place to ensure State funds are not be used in violation of copyright law.

### Response 2.1

Caltrans' current policy is that software license assignment, tracking, and compliance is the responsibility of the districts and divisions that procure software. HQ ITAM buys and manages the licenses for Caltrans's Enterprise Volume License Agreements (EVLA).

Caltrans' policy is that all computer users have power user rights by default. Employees must submit an Administrative Rights Exception Request Form with a legitimate "Business Need Statement" that explains why administrative rights are needed and as such, why IT cannot provide the needed support. The Form must receive signed approval from the requester's supervisor, the IT Support Manager, the IT Infrastructure Division Chief, and the CIO (or delegated alternates).

**ACTION (Emmil Simeroth):** HQ ITAM will populate the ZENworks Asset Management database with license purchase data. Projected completion date: December 31, 2014.

ITAM has created a License Information Decision Guide spreadsheet to summarize software license terms for products on the Caltrans Approved Software List. The *Caltrans Approved Software List* guides ITAM staff's decisions during the approval process regarding software installation.

**PENDING ACTION (Emmil Simeroth):** HQ ITAM and Tom Dolce of IT PMO are working with the districts and business programs to identify the Software License Information Coordinator (SLIC) for each location and to develop a plan to educate and collaborate with the SLIC on the inventory and remediation effort. Projected completion date: December 31, 2014.

**PENDING ACTION (Emmil Simeroth):** HQ ITAM is in the process of sharing and communicating the standardized software remediation procedure with all the districts and business programs. Projected completion date: December 31, 2014.

**COMPLETED ACTION (Emmil Simeroth):** The Division of Procurement and Contracts (DPAC) is the delegated procurement authority for Caltrans. DPAC has indicated that language has been added to IT Contracts to certify that contractors have the appropriate controls in place to ensure State funds are not used in violation of software copyright law. In addition, DPAC

management is reviewing SIMM 120 in order to determine the requirement for contractor certification in non-IT agreements. Expected completion date is May 03, 2013.

Language: "The Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Contract for the acquisition, operation, or maintenance of computer software in violation of copyright laws." -- Jennifer Burnett, DPAC IT Acquisitions & Property Control Office Chief, 5/03/2013.

"We are including this language as appropriate in all IT, consulting, and A&E contracts. We are not including the language in all contracts executed by DPAC." -- Kelly Takigawa, DPAC Assistant Division Chief, 5/03/2013.

#### Recommendation 2.2

ITAM establishes a reporting structure by which districts and divisions performing remediation certify compliance with SAM 4846 annually and retain these certifications for three years.

#### Response 2.2

PENDING ACTION (Emmil Simeroth): HQ ITAM will create and distribute remediation compliance instructions to districts and divisions. Projected completion date: December 31, 2014.

PENDING ACTION (Emmil Simeroth): HQ ITAM will create and distribute a "remediation compliance certification" document, which district and division chiefs will sign. Projected completion date: December 31, 2014.

#### Recommendation 2.3

ITAM updates the Software Management Plan to reflect actual procedures in the Ongoing Inventory and Control Methodology and the Contractor's Certification section.

#### Response 2.3

HQ ITAM has established a standard software approval/denial procedure to verify the assignment of an available license to the customer prior to software installation.

COMPLETED ACTION (Emmil Simeroth): ITAM communicated the standardized software license approval/denial procedure with all the districts and business programs. Expected completion date is April 30, 2013.

PENDING ACTION (Emmil Simeroth): ITAM will review all the Department's actual inventory control procedures and processes and update them. ITAM will update Caltrans' 2014 Software Management Plan's Ongoing Inventory and Control Methodology section. Projected completion date: December 31, 2014.

COMPLETED ACTION (Emmil Simeroth): HQ ITAM will update the 2014 Caltrans SMP's Contractor Certification section. Expected completion date is December 31, 2013.

#### Recommendation 2.4

ITAM reconciles the differences between ZAM and EPO to determine the universe of workstations.

#### Response 2.4

No reconciliation is possible. The counts differ and vary daily because of many factors. New PCs connect to the network. Old PCs taken out of service but are not immediately deleted from the databases. Laptops may not connect to the network for months.

Novell ZENworks Asset Management (ZAM) is Caltrans' official IT asset management tool. Its counts and inventory reports determine Caltrans' official "universe of workstations".

#### Recommendation 2.5

ITAM ensures Information Technology's website is updated with the most recent approved version of the Caltrans' Software Management Plan and informs district IT managers of procedural changes.

#### Response 2.5

COMPLETED ACTION (Emmil Simeroth): HQ ITAM posted the signed 2013 Software Management Plan on the ITAM website. Expected completion date is February 28, 2013.

COMPLETED ACTION (Emmil Simeroth): HQ ITAM communicated the web link of the 2013 Software Management Plan to all District IT Managers and to HQ IT Managers and informed them of procedural changes. Expected completion date is February 28, 2013.

### Finding 3

Software Management Training is Inadequate

#### Recommendation 3.1

Caltrans should include the following in the Information Security and Privacy Awareness Training (Core and Annual):

- Definition and examples of software piracy
- Federal Copyright Act (Annual Training)
- Statewide and departmental policies and procedures relating to software management

#### Response 3.1

The Information Security Office included the required educational components in the Information Security and Privacy Awareness Training (Core and Annual). David Wong, of the Division of Audits and Investigations verifies that ISO training has been strengthened since the 2011 audit. David confirms that there is no training issue now.

COMPLETED ACTION (Emmil Simeroth): ITAM wrote a New Employee Orientation handout describing state and Caltrans software copyright policies, software piracy, and Caltrans process for validating and approving installation of licensed software. ITAM sent the NEO handout to Maslyn Kanipe, the Learning & Development Office's NEO Coordinator. Maslyn Kanipe

William E. Lewis  
February 26, 2014  
Page 6 of 6

replied, "I am pushing this information on to our eLearning Team as our office has delivered an online version of NEO. I am not sure if our office will continue delivering the classroom method of this course, but if we do, I will add this to the training curriculum."  
Expected completion date is June 19, 2013.

## Memorandum

*Flex your power!  
Be energy efficient!*

**To:** WILLIAM E. LEWIS  
Assistant Director  
Audits and Investigations

**Date:** August 21, 2013

**File:** P3020-069

**From:** GIGI SMITH  
Chief Information Officer  
Information Technology

**Subject:** 180-DAY RESPONSE TO FINAL AUDIT REPORT ON SOFTWARE MANAGEMENT PROGRAM

Information Technology has attached the 180-Day Audit Response in response to the Audits and Investigations' report entitled *P3020-069 Final Audit Report on Software Management Program, February 25, 2013*. Submission of this response constitutes our report requirement subsequent to the audit.

Please contact Dan Nguyen at (916) 651-8466 or Dave Miles at (916) 654-5962 if you have any questions or need additional information.

### Attachments

- (1) IT 180-Day Response to February 25, 2013 Final Audit Report on Caltrans Software Management Program
  
- c: Francesca Negri, Chief, Division of Procurements and Contracts  
Jacob Ellwood, Chief (Acting), Security Division, Information Technology  
Laurine Bohamera, Chief, Internal Audits, Audits and Investigations  
Carolyn Pennington, Chief, IT Management Support Office, Information Technology  
Dan D. Nguyen, Chief (Acting), Information Technology Asset Management and Acquisition Office  
Kevin Yee, Internal Audit Manager, Internal Audits, Audits and Investigations  
David Wong, Auditor-in-Charge, Internal Audits, Audits and Investigations  
Veronica Kaldani, Auditor, Internal Audits, Audits and Investigations  
Dave Miles, IT Asset Management Lead, Information Technology Asset Management and Acquisition Office

Attachment (1)

## **IT 180-Day Response to February 25, 2013 Final Audit Report On Caltrans Software Management Program**

### **Finding 1**

**Caltrans' Software Management Policy Annual Statement of Compliance Has Not Been Retained or Supported with a Hardcopy of the Software Inventory**

#### **Recommendation 1.1**

**ITAM prepares and retains the Annual Certification and inventory summaries for at least three years.**

#### **Response 1.1**

IT Asset Management (ITAM) prepares the SMP Annual Statement of Compliance after preparing the Software Management Plan (SMP) in December of every year. The Director or Designee (CIO) signs the SMP Annual Statement of Compliance at the end of January of the following year.

**ACTION (Dan Nguyen):** ITAM will continue to retain electronic and hard copies of both documents for at least three years. ITAM has retained:

- 2011 SMP Annual Statement of Compliance
- 2012 SMP Annual Statement of Compliance
- 2013 SMP Annual Statement of Compliance

#### **Recommendation 1.2**

**ITAM prepares an annual software inventory report to support the Annual Certification**

#### **Response 1.2**

Caltrans IT is installing ZENworks Agents on Caltrans' Macintoshes, Windows servers, UNIX/LINUX servers, computers, workstations and laptops. Future inventory summary reports will add software installation counts for these devices to the installation counts of software on Windows PCs.

**ACTION (Dan Nguyen):** ITAM will prepare electronic and hardcopy annual inventory summary reports of all software installed on Caltrans computers and servers in December of every year and retain them for at least three years. Projected completion date: December 31, 2013. ITAM has retained:

- 2012 SMP Baseline Inventory 12-9-2011 by District report
- 2013 SMP Installation Counts of All Software – 20121203 report

## **Finding 2**

### **Caltrans' Software Management Plan Has Not Been Fully Implemented.**

#### **Recommendation 2.1**

##### **ITAM & IT Cert Office collaborates with DPAC to:**

- 1. Track licenses of all procured software;**
- 2. Identify the license terms and the unit, group, and individual responsibility for remediation;**
- 3. Document the remediation strategy; and**
- 4. Ensure all Caltrans contractors have appropriate controls in place to ensure State funds are not used in violation of copyright law.**

#### **Response 2.1**

1. Caltrans' current policy is that software license assignment, tracking, and compliance is the responsibility of the districts and divisions that procure software. HQ ITAM buys and manages the licenses for Caltrans's enterprise volume license agreements.

Caltrans' policy is that all computer users have power user rights by default. Employees must submit an Administrative Rights Exception Request Form with a Legitimate Business Need Statement that explains why administrative rights are needed and why IT cannot provide the needed support. The Form must receive signed approval from the requester's supervisor, the IT Support Manager, the IT Infrastructure Division Chief, and the CIO (or delegated alternates).

**ACTION (Dan Nguyen):** ITAM will populate the ZENworks Assct Management database with license purchase data. Projected completion date: December 31, 2014.

2. ITAM has created a License Information Decision Guide spreadsheet to summarize software license terms for products on the Caltrans Approved Software List. This "living" document guides ITAM staff decisions during the approval process.

**ACTION (Dan Nguyen):** ITAM and Tom Dolce of PMO are working with the districts and business programs to identify the Software License Information Coordinator (SLIC) for each location and to develop a plan to educate and collaborate with the SLIC on the inventory and remediation effort. Projected completion date: December 31, 2014.

3. **PENDING ACTION (Dan Nguyen):** ITAM is in the process of sharing and communicating the standardized software remediation procedure with all the districts and business programs. Projected completion date: December 30, 2013.
4. The Division of Procurement and Contracts (DPAC) is the delegated procurement authority for Caltrans. DPAC has indicated that language has been added to IT Contracts to certify that contractors have the appropriate controls in place to ensure State funds are not used in violation of software copyright law. In addition, DPAC management is

reviewing SIMM 120 in order to determine the requirement for contractor certification in non-IT agreements.

COMPLETED ACTION (Dan Nguyen): "DPAC will include the following provision in both consulting services and A&E contract boilerplates: *The Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Contract for the acquisition, operation, or maintenance of computer software in violation of copyright laws.*" - Jennifer Burnett, DPAC IT Acquisitions & Property Control Office Chief, 5/03/2013.

"We are including this language as appropriate in all IT, consulting, and A&E contracts. We are not including the language in all contracts executed by DPAC." - Kelly Takigawa, DPAC Assistant Division Chief, 5/03/2013. Completion date: May 03, 2013.

#### **Recommendation 2.2**

**ITAM establishes a reporting structure by which districts and divisions performing remediation certify compliance with SAM 4846 annually and retain these certifications for three years.**

#### **Response 2.2**

PENDING ACTION (Dan Nguyen): ITAM will create and distribute remediation compliance instructions to districts and divisions. Projected completion date: December 30, 2013.

PENDING ACTION (Dan Nguyen): ITAM will create and distribute a remediation compliance certification document, which district and division chiefs will sign. Projected completion date: December 30, 2013.

#### **Recommendation 2.3**

**ITAM updates the Software Management Plan to reflect actual procedures in the Ongoing Inventory and Control Methodology and the Contractor's Certification section.**

#### **Response 2.3**

ITAM has established a standard software approval/denial procedure to verify the assignment of an available license to the customer prior to software installation.

PENDING ACTION (Dan Nguyen): ITAM communicated the standardized software license approval / denial procedure with all the districts and business programs. Completion date: December 30, 2013.

ACTION (Dan Nguyen): ITAM will review all the Department's actual inventory control procedures and processes and update them. ITAM will update Caltrans' 2014 Software Management Plan's Ongoing Inventory and Control Methodology section. Projected completion date: December 31, 2013.

PENDING ACTION (Dan Nguyen): "DPAC will include the following provision in both consulting services and A&E contract boilerplates: *The Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Contract for the acquisition, operation, or maintenance of computer software in violation of copyright laws.*" - Jennifer Burnett, DPAC IT Acquisitions & Property Control Office Chief, 5/03/2013.

"We are including this language as appropriate in all IT, consulting, and A&E contracts. We are not including the language in all contracts executed by DPAC." - Kelly Takigawa, DPAC Assistant Division Chief, 5/03/2013. ITAM will update Contractor's Certification section in the Caltrans' 2014 Software Management Plan. Projected completion date: December 30, 2013.

#### **Recommendation 2.4**

**ITAM reconciles the differences between ZAM and EPO to determine the universe of workstations.**

#### **Response 2.4**

No reconciliation is possible. The counts differ and vary daily because of many factors. New PCs connect to the network. Old PCs are surveyed out but are not immediately deleted from the databases. Laptops may not connect to the network for months.

Novell ZENworks Asset Management (ZAM) is Caltrans' official IT asset management tool. Its counts and inventory reports determine the official "universe of workstations".

#### **Recommendation 2.5**

**ITAM ensures Information Technology's website is updated with the most recent approved version of the Caltrans' Software Management Plan and informs district IT managers of procedural changes.**

#### **Response 2.5**

COMPLETED ACTION (Dan Nguyen): ITAM posted the signed 2013 Software Management Plan on the ITAM website. Completion date: February 28, 2013.

PENDING ACTION (Dan Nguyen): ITAM communicated the web link of the 2013 Software Management Plan to all District IT Managers and to HQ IT Managers and informed them of procedural changes. Completion date: December 30, 2013.

### **Finding 3**

**Software Management Training is Inadequate**

#### **Recommendation 3.1**

**Caltrans should include the following in the Information Security and Privacy Awareness Training (Core and Annual):**

- **Definition and examples of piracy.**
- **Federal Copyright Act (Annual Training)**
- **Statewide and departmental policies and procedures relating to software management.**

**Response 3.1**

The Information Security Office included the required educational components in the Information Security and Privacy Awareness Training (Core and Annual). David Wong of the Division of Audits and Investigations verifies that ISO training has been strengthened since the 2011 audit. David confirms that there is no training issue now.

COMPLETED ACTION (Dan Nguyen): ITAM developed a New Employee Orientation handout describing state and Caltrans software copyright policies, software piracy, and Caltrans process for validating and approving installation of licensed software. ITAM sent the NEO handout to Maslyn Kanipe, the Learning & Development Office's NEO Coordinator. Maslyn Kanipe replied, "I am pushing this information on to our eLearning Team as our office has delivered an online version of NEO. Completion date: June 19, 2013.