STATE OF CALIFORNIA

Department of Insurance

John Garamendi
Insurance Commissioner

SOFTWARE MANAGEMENT PLAN

March 17, 2004

Dennis Ward
Deputy Commissioner
Administration and Licensing Services Branch

Daniel K. Whetstone
Chief Information Officer
Information Technology Division

Prepared by

The Project Coordination and Administrative Support Bureau

TABLE OF CONTENTS

OVERVIEW

In October 1999, the Governor of California issued an Executive Order (D-10-99) mandating each State agency work diligently to give effect to copyrights associated with computer software. In response, the Department of Finance (DOF) established a Software Management Policy (State Administrative Manual (SAM) Section 4846). The policy requires agencies to plan and implement processes to ensure compliance with any software license copyright laws or other regulations for the use of software. The agency's plan must be documented in a Software Management Plan (SMP). To ensure agency compliance with the SAM requirements, the DOF published guidelines (dated September 2002) in the State Information Management Manual (SIMM) to assist agencies with development of their SMP.

To fulfill the requirements of SAM Section 4846, the CDI formed a Software Management Team (SMT) who developed a SMP in accordance with guidelines of SIMM Section 80 and 120. The SMP defined planned processes and procedures that would be implemented to support good software management practices, including a software inventory to identify all software in use at CDI. The inventory would also identify whether the software is properly licensed and approved for use at CDI. The SMP baseline inventory and ongoing control processes and procedures were implemented in January 2003.

The following SMP provides documentation on CDI's baseline software inventory and on-going control processes and procedures for software management. The SMP was prepared in accordance with guidelines of SIMM Section 120. This SMP and the summary of CDI's software inventory are maintained in CDI files within the Information Technology Division (ITD) and are available for DOF review, upon request.

DEFINITION OF TERMS USED IN THIS SMP

1. Approved Software - Software that CDI ITD has approved for use on CDI computers. It must be purchased and installed following ITD Procurement Policy and Procedures. Approved software may consist of software that is both supported and unsupported by CDI ITD.
2. Mitigation Process - When software is identified as unlicensed, it is considered to be a breach of CDI SMP Policy. The CDI mitigation process allows users to purchase a license for the software, thereby rendering it legal for use.
3. Not Approved Software - Software that CDI ITD has not authorized for download or installation onto CDI computers.
4. Unlicensed - Software that is in use by CDI, but there is not a procurement record to support that a valid license was purchased for the software.
5. Supported Software - Software that ITD Help Desk is responsible for installation and maintenance.
6. Unsupported Software - Software that is approved by CDI ITD for installation on CDI computers but is not supported by the ITD Help Desk.

1.0 SOFTWARE BASELINE INVENTORY METHODOLOGY

The Software Management Team (SMT) conducted a baseline inventory of all software residing on CDI computers. The process used to conduct the baseline inventory was as follows:

1.1 STAFF INVOLVED WITH CONDUCTING THE SOFTWARE BASELINE INVENTORY

The SMT was responsible for conducting the baseline inventory. The team consisted of the following staff:

ITD Statewide Network Support (SNS) Bureau

- SNS Bureau Chief (Data Processing Manager (DPM) III)
- ITD Help Desk (Senior Information Systems Analyst (SISA))

ITD Application Development and Maintenance (ADAM) Bureau

- ADAM Bureau Chief (DPM III)
- Staff Programmer Analyst (SPA)
- Associate Programmer Analyst (APA)

ITD Project Coordination and Administrative Support (PCAS) Bureau

- PCAS Bureau Chief (DPM III)
- ITD Procurement Specialist (SISA)
- PMO Project Advisor (Associate Information Systems Analyst (AISA))

1.2 METHOD FOR CONDUCTING SOFTWARE BASELINE INVENTORY

The SMT used both automated and manual processes to conduct the baseline inventory. Detailed information on the methods used for conducting the baseline inventory were as follows:

1.2.1 IDENTIFICATION OF SOFTWARE LICENSES PURCHASED BY CDI

To support the baseline inventory process, the SMT manually reviewed all software purchase orders from fiscal years 2000-2001 through 2003-2004 and entered the information into a spreadsheet (Excel).

1.2.2 INVENTORY OF SOFTWARE INSTALLED ON CDI COMPUTERS

The SMT conducted an inventory of all software residing on CDI desktops, laptops, and server hardware. The processes used to identify software installed were as follows:

a. Automated Software Audit

The SMT utilized the inventory component of Track-It!, an Oracle-based Help Desk support tool to capture the software and hardware inventory for each machine connected to the network.

b. Manual Software Audit

Laptops and desktops not connected to the network or not captured by Track-It! were audited manually and the captured data was uploaded to the Track-It! database.

Network servers were manually audited and their data was entered into the spreadsheet.

Software media and associated licensing documentation (certificates) were also manually audited and the information was entered into the spreadsheet.

Software installed at the Teale Data Center (TDC) in support of CDI was not included in the baseline inventory. The CDI relies upon the TDC to follow the same practices as other state agencies and have an SMP in place to encompass all TDC installed software utilized by CDI.

1.3 ORGANIZATION OF SOFTWARE BASELINE INVENTORY PROCESS

The CDI baseline inventory process was organized to include the following three phases:

1.3.1 DISCOVERY

This phase included identification of all software purchases.

1.3.2 SOFTWARE INVENTORY

This phase included the actual automated and manual software audits for desktops, laptops, servers, and software media.

1.3.3 REPORTING

This phase included the creation of the reports necessary to reconcile CDI licensed software with actual software installations.

Additionally, the Summary Baseline Inventory Report was created in support of Control Agency and CDI Executive Management requirements.

1.4 INFORMATION GATHERED FOR THE SOFTWARE BASELINE INVENTORY

The SMT gathered and stored the following information for the baseline inventory:

1.4.1 SOFTWARE INFORMATION

a. Product Name (and manufacturer)

b. Software Version

c. Purchasing information as maintained by the CDI Procurement Office

d. Type of License (site, individual)

e. Number of authorized user/seats for the license

1.4.2 PROCUREMENT INFORMATION

a. Purchase orders

1.5 METHOD FOR REPORTING SOFTWARE BASELINE INVENTORY INFORMATION

The CDI prepared the following reports/summary using the following methods:

a. Full Inventory Report

Track-It! provided an on-line report of all software residing on department computers.

b. Software Inventory/Software Compliance Report Summary

A summary report was developed that included all major software purchases and installations including package name, version number, number of licenses purchased, number of licenses installed, the difference between number purchased and number installed and a short description of the software package. This information was reported to the CDI Executive Management.

1.5.1 REPORT CONTENT

The Full Inventory Report included the following information:

- Software residing on CDI computers (excluding network servers)
- Username assigned to hardware
- Hardware location by IP address
- Quantities of each software residing on CDI hardware devices

The Software Inventory Summary/Software Compliance Report included the following information at a minimum:

- All software (excluding any commonly used software that was approved for use but not tracked for licensing validation, such as; Apache Web Server, an open-source software package) residing on CDI computers (excluding network servers)
- The total number of installations for each software
- The total number of licenses purchased by CDI
- Excess or shortages of licenses for software that was installed at CDI

1.5.2 STAFF WHO RECEIVED THE SOFTWARE BASELINE INVENTORY REPORTS

Distribution of the baseline inventory report defined in 1.5.1 was as follows:

a. Full Inventory Report Distribution

Due to the size of the full inventory report, it was not distributed. It is available for viewing on-line to the following staff:

- ITD Software Manager
- ITD Chief of Staff
- ITD Bureau Chiefs
- CDI's Chief Information Officer (CIO)

b. Software Inventory Summary Distribution

- ITD Software Manager
- ITD Chief of Staff
- ITD Bureau Chiefs
- CDI's CIO

c. Software Compliance Report Distribution

- ITD Software Manager
- ITD Chief of Staff
- CDI's CIO
- Software Management Team

1.6 BASELINE SOFTWARE INVENTORY COMPLETION DATE

CDI's baseline inventory was completed on January 15, 2003.

2.0 UNLICENSED/NOT APPROVED SOFTWARE IDENTIFICATION METHODOLOGY

The identification of software that is unlicensed is accomplished by comparing the results of the software inventory to the list of licensed software owned by CDI. The identification of software that is not approved for use at CDI is accomplished as follows:

2.1 RESPONSIBILITY FOR IDENTIFICATION OF SOFTWARE THAT IS UNLICENSED OR NOT APPROVED FOR USE

ITD Help Desk and other technical support staff are responsible for reporting unlicensed or unapproved software that is identified during their routine support responsibilities.

2.2 PROCESS FOR REPORTING SOFTWARE THAT IS UNLICENSED OR NOT APPROVED

ITD Help Desk and technical staff will open a ticket in Track-It! when unlicensed or unapproved software is identified. If other CDI staff identify unlicensed or unapproved software, they will contact a supervisor or the ITD Help Desk. ITD Help Desk staff will open a ticket in Track-It!.

2.3 MITIGATION PROCESS FOR SOFTWARE THAT IS UNLICENSED OR NOT APPROVED

Mitigation for software that is unlicensed or not approved is accomplished as follows:

a. If the software is deemed "critical" by the program area and the immediate removal of the software will cause a significant business impact, the program area will have five (5) business days to provide evidence of a valid license, or proof of intent to purchase a license. An approved requisition form (Form 5), will provide evidence of intent to purchase a license. If the Form 5 is not produced within five (5) business days, the software will be removed.

b. When software is not licensed and a Form 5 is not submitted, the ITD Help Desk will remove the software in accordance with Section 2.4. When the software has been removed, the inventory records will be updated and no further mitigation action will take place. Refusal to allow ITD Help Desk to remove the software will be reported to the immediate supervisor for resolution.

c. Mitigation actions may be documented and distributed to appropriate staff. Repeated violations of either copyright law, software license usage, or related CDI policy by the same employee(s) may result in corrective action and possible adverse action, as defined in Section 6.0.

2.4 PROCESS FOR REMOVING SOFTWARE THAT IS UNLICENSED OR NOT APPROVED

An ITD Help Desk Supervisor will contact the employee's Supervisor to inform them of the intent to remove the software. ITD Help Desk staff will remove the software. The next Track-It! workstation audit will validate that the software was removed with a "removed" reference on the audit report.

3.0 SECURE REPOSITORY

The CDI uses secure software repositories to store all software applications and related licensing documentation. Appendix B includes inventory records for the items stored in the secure repositories. Processes and procedures in support of the secure repositories are as follows:

3.1 PHYSICAL SOFTWARE REPOSITORY

All software media (disks containing original program files from the software manufacturer) are centralized in locked cabinets in each of CDI's major office sites (Sacramento, Los Angeles, and San Francisco).

All software license certificates are centralized in a locked cabinet in CDI's Sacramento office site with the ITD Procurement Officer.

3.2 VIRTUAL SOFTWARE REPOSITORY

The CDI uses a central network file server to store a copy of all software media used for installation. Access to the CDI Software drive is restricted using Microsoft Active Directory shares.

3.3 SECURITY OF THE SOFTWARE REPOSITORIES

The CDI has established secure repositories, identified staff with access rights, and specified employees who can check-out software as follows:

3.3.1 LOCATION AND ADMINISTRATION OF THE SOFTWARE REPOSITORIES

Secure Repository Administrators (SRAs) are assigned in each city to control the access rights for the physical software repositories. Information on the location of the secure repositories and the assigned SRA is as follows:

a. ADAM Bureau Software Repository

Office Site	Physical Repository Location	SRA(s)/Classification	Secondary Contact(s)
Sacramento	The cabinet is located on the West End of the Sacramento ADAM Bureau.	Cathi Christian, (SPA)	Don Powell, Senior Information Systems Analyst (ISA)
Los Angeles	The cabinet is located in Leslie's cubicle. Software is also located at w:\ Latest Quest Software versions and w:\Developer6i Patch10 drive on lafp01 server.	Leslie Brashear, SPA	Raul Nadres, AISA
San Francisco	N/A	N/A	N/A

b. SNS Bureau Software Respository

Office Site	Physical Repository Location	SRA(s)/Classification	Secondary Contact(s)
Sacramento	The cabinet is located in the hallway outside of the Training Room. Another locked cabinet is in Jesse Castillo's office.	Carol Walden, Senior ISA (Sup.) Jesse Castillo, Senior ISA (Sup.)	Rex Rowland, SISA Karen Ongerth, SISA Monico Rosales, AISA Conrad Perocho, SISA
Los Angeles	Cabinet in Computer Room; Cabinet called 'File Cabinet 2' (named after key)	Chadona Bolden, SISA (Sup.)	Henry Castellanos, SISA Peter Fajota, SISA Jay Engle, SISA
San Francisco	Cabinet is located in the IT 'Boneyard'.	Kenny Lew, SISA (Sup.)	SNS Bureau Chief, DPM III Leslie Wilson, SISA

c. Software License Certificates Respository

Office Site	Repository Location	SRA/Classification	Secondary Contact
Sacramento	The cabinet is located on the West End of the Sacramento PCAS Bureau.	Software Repository Administrator is Mary Fonseca, SISA	Althea Riley, SISA Michelle Leach, SISA

3.3.2 ACCESS RIGHTS ASSIGNED FOR SOFTWARE REPOSITORIES

Access to the repositories is granted to employees based on their work assignments and responsibilities. Access rights to both the physical and virtual software repositories are as follows:

a. Staff with Full Access Rights

Access to the physical and virtual software repositories is granted to authorized staff in each city. Full access is currently granted to the following staff:

- ITD Help Desk Supervisors in each CDI office site
- SNS Network Administrators in each CDI office site
- SNS Bureau Chief
- ADAM Bureau Chief or designee
- ITD Software Manager

b. Staff with Virtual Software Repository Access

Access rights to the virtual software repository are granted to the following staff:

- Statewide Network Support Staff including SNS Bureau Chief

c. Staff with Physical Repository Access

Access rights to the physical software repository are granted to the following staff:

- Staff with Full Access Rights (as defined in Section 3.3.2.a.)
- Designated ITD Help Desk Staff
- Wide Area Network Staff

3.3.3 STAFF WITH ACCESS TO CHECK-OUT PHYSICAL AND VIRTUAL SOFTWARE FROM THE SECURE REPOSITORIES

The SRA authorizes specified employees who can check-out software media and related documentation. Authorization to check-out software is granted to the following:

- Staff with Full Access Rights (as defined in Section 3.3.2.a.)
- ITD Help Desk Staff
- ADAM Database Administrators or designee

3.4 SECURE REPOSITORY SOFTWARE CHECK-OUT PROCEDURES

The CDI has established procedures for the removal and return (check-in/check-out) of software in the repositories. Staff authorized to access software stored in the secure repositories will use the check-out procedures, as follows:

3.4.1 SOFTWARE MEDIA CHECK-OUT PROCEDURES FOR STAFF WITH FULL ACCESS

Authorized employees must complete the check-out log. The check-out log documents the name of the employee checking out the item (requestor), the name of the person who authorized the request, the check-out date, the software product name and version, the reason for check-out, the location where the software will be installed, and the expected date the item will be returned. The staff must return the item to the file cabinet when finished and update the log to indicate when the item was returned. A sample of the check-out log is located in Appendix C.

3.4.2 SOFTWARE MEDIA CHECK-OUT PROCEDURES FOR OTHER AUTHORIZED STAFF

Authorized employees must submit a request to the SRA indicating the same information contained in the check-out log (defined in Section 3.4.1). The SRA will evaluate the request based on whether the employee is granted check-out access, and if the installation and use of the software is properly licensed. If the request is granted, the SRA will physically retrieve the item from the secure repository and manually update the check-out log indicating the name of the requestor. If the request is not granted, the SRA will notify the requestor of the reason for denial and alternatives for accomplishing the installation. When finished with the item, the

requestor must return the item to the SRA who will verify all items are returned, re-file the items in the secure repository, and update the log accordingly.

3.4.3 CHECK-OUT FOR SOFTWARE IN THE VIRTUAL SOFTWARE REPOSITORY

Access to the virtual software repository is granted through a SNS Network Administrator. Employees must be granted the right to map to the share drive that contains CDI software. Access is restricted to Statewide Network Support personnel where the job duties include software installation on for both PCs and servers.

3.4.4 GENERAL CHECK-OUT RULES

Employees authorized to check-out physical software media must abide by the following applicable rules:

a. Items may only be used for the reason they were checked out.

b. All log information must be complete before any item is checked out.

c. Items must be kept secure while checked-out. This requires: 1) keeping the item in a locked area when not in use; 2) never taking the item home unless this location is used for official business; 3) never giving items to an unauthorized employee.

d. Any copies made of the software must be made for business use and must be kept in a locked area when not in use.

e. Items may be checked out for a maximum of three (3) business days for use at CDI's major headquarter office site. Items may be checked out for a maximum of 15 business days for use at a CDI remote office location.

f. The employee will be accountable for following proper procedures for inventory control of the software.

g. At the time of check-in, the SRA will verify that all items have been returned, and update the log accordingly.

h. The SRA will maintain documentation of all check-in and check-out activities including requests that have been denied.

i. If the expected check-in date passes and the items have not been returned, the SRA will follow up with the employee who checked the items out and takes necessary steps to have the items returned.

4.0 ON-GOING INVENTORY AND CONTROL METHODOLOGY

The CDI has established ongoing inventory control processes. This ensures that software additions, changes, or disposal are properly reflected in the software inventory.

4.1 STAFF RESPONSIBLE FOR ON-GOING INVENTORY CONTROL PROCESSES AND PROCEDURES

The SNS Bureau Chief and the PCAS Bureau Chief will have the overall responsibility for ensuring the necessary inventory control processes and procedures are developed, implemented and maintained. In addition, the ITD Software Manager has responsibility for oversight of the inventory control processes and procedures.

Each ITD Bureau (SNS, ADAM, PCAS) will be accountable for ensuring the software in their area of responsibility complies with ongoing inventory control processes.

4.2 ONGOING INVENTORY CONTROL PROCESSES FOR RECEIPT AND INSTALLATION OF SOFTWARE, REMOVAL AND DISPOSAL OF SOFTWARE, AND CHANGE CONTROL

Inventory control processes for software receipt, installation, removal, disposal and change control are established, as follows:

4.2.1 INVENTORY CONTROL PROCESSES FOR RECEIPT AND INSTALLATION OF SOFTWARE

Receipt and installation of software on a CDI computer must be controlled, as follows:

a. Inventory Control Processes for New Software

When a program area identifies the need for software, they must contact the ITD Help Desk who will initiate a help desk ticket for the request. If a software license is available, it will be installed. If a software license is not available, the requestor will be instructed on the proper procurement process to purchase the software. An approved requisition form (Form 5), will provide evidence of intent to purchase a license and, if available, the software may be installed.

The following general procedures are to be followed for new software installations in support of inventory control:

1) All software items are received by the SRA, after receipt by ITD Procurement. The SRA ensures that the order is complete and signs the invoice.
2) The pertinent license information is recorded in the spreadsheet. The ITD support level (supported or unsupported) is also documented.
3) The SRA loads the software into CDI's virtual network repository and notifies Statewide Network Support personnel that it is available for installation.
4) All software media is stored in the secure repository, and all (original) software license certificates are forwarded to the ITD Procurement Officer.
5) The ITD Procurement Officer will ensure proper documentation is maintained and update license agreement information maintained for standard CDI software in the spreadsheet.
6) The Procurement Officer reviews the software certification or license and stores them in a secured cabinet. All necessary registration cards or other proof of registration will be completed in the name of CDI.
7) Installation activities will be maintained in the Track-It! Help Desk logs.
8) For Enterprise Software (i.e., Oracle) the ADAM supervisors should be informed that an installation has occurred.

b. Inventory Control Processes for Redistributed Software

A Help Desk ticket is opened when software is redistributed from one machines to another. The Software redistribution procedure is as follows:

1) ITD Help Desk staff will remove the software from its current location following procedures for removal defined in Section 4.2.2. The Track-It! inventory records will reflect the de-installation.
2) ITD Help Desk staff will reinstall from their copy of the original media, or from the purchase repository. (as defined in Section 3.3).
3) Redistributed software activities will be maintained in the Track-It! Help Desk logs.

c. Inventory Control Processes for Reinstalled Software

A Help Desk ticket is opened when software is reinstalled (malfunction, hardware replacement, etc.) The software reinstallation process is as follows:

1) ITD Help Desk staff will reinstall from their copies of the original software media or access the network based software from the secure repository. If original media is required, ITD Help Desk staff will check-out the software using the regular procedure.

d. Inventory Control Processes for Software Upgrades

The following general procedures are to be followed for new software installations in support of inventory control:

1) The ITD Procurement Officer will ensure proper documentation is maintained and update license agreement information maintained for standard CDI software in the spreadsheet.
2) All software items are received by the SRA who ensures that the order is complete and signs the invoice.
3) The pertinent license information is recorded in the spreadsheet The ITD support level (supported or unsupported) is also documented.
4) The SRA loads the software into CDI's virtual network repository and notifies Statewide Network Support personnel that it is available for installation.
5) All software media is stored in the secure repository, and all (original) software license certificates are forwarded to the ITD Procurement Officer.
6) The Procurement Officer reviews the software certification or license and stores them in a secured cabinet. All necessary registration cards or other proof of registration will be completed in the name of CDI.
7) Installation activities are maintained in the Track-It! Help Desk Inventory.

4.2.2 REMOVAL AND DISPOSAL OF CDI SOFTWARE

Removal and disposal of software is generated by a Help Desk ticket. An assigned ITD Help Desk staff will physically go to the computer and remove (uninstall) the software. Help Desk logs will be updated to reflect the removal. Track-It!'s automatic workstation audit process will reflect the change.

When software is determined to be no longer needed at CDI, any network installations for the software or any software media and related licensing for the software will be disposed, in accordance with Section 8.0.

Software that is no longer licensed or approved for use at CDI is removed from the ITD Supported Software List.

4.2.3 CHANGE CONTROL OF ONGOING INVENTORY AND CONTROL PROCESSES

Any changes in software (including new installations, redistribution, upgrade, removal, etc.) will be updated to the Track-It! database upon audit of the affected computer. The ITD will prepare and distribute reports in accordance with the reporting process defined during the baseline inventory (Section 1.5).

4.2.4 QUALITY CONTROL OF ONGOING INVENTORY AND CONTROL PROCESSES

The ITD Software Manager will monitor the software inventory to evaluate whether the processes and procedures are effectively controlling the use and management of software within CDI.

The CDI will continue evaluation of the use of automated tools for software management, and will consider replacing or upgrading current automated processes if new software is determined to be more efficient and cost effective.

4.3 STAFF RESPONSIBLE FOR ENSURING ONGOING INVENTORY CONTROL PROCESSES AND PROCEDURES ARE ACCURATELY AND CONTINUOUSLY FOLLOWED

All ITD Bureau staff (SNS, ADAM, PCAS) involved with software activities are responsible for ensuring ongoing inventory and control processes are followed in their area of responsibility.

The ITD CIO and ITD Bureau Chiefs will support resource needs to fully implement ongoing inventory control processes. Supervisors of the ITD Help Desk and other technical support staff will ensure that inventory and control processes are properly followed. ITD Supervisors will ensure that staff members have appropriate education on software management policies and procedures and that mitigation activities occur, as defined in Section 2.3.

The ITD Software Manager is responsible for oversight and will monitor processes to verify that inventory information is updated in a manner consistent with the SMP.

4.4 STAFF RESPONSIBLE FOR CONDUCTING ONGOING INVENTORIES

The SNS Bureau, with assistance from ADAM and PCAS Bureau as needed, will be responsible for ensuring that ongoing software inventory is properly controlled and reported.

4.5 STAFF RESPONSIBILITY AND PROCESS FOR ENSURING ONGOING INVENTORIES OCCUR

The SNS Bureau Chief and assigned Network Administrators will maintain the Track-It! Help Desk software to ensure regular audits of all network attached desktops and laptops.

CDI's inventory records will reflect software counts as of the last automatic audit performed on the workstation. Access to current software inventory information is available at all times. Point in time inventory reports will be prepared on an annual basis to reflect that ongoing inventories are consistent with the requirements of the SMP.

4.6 INVENTORY SAMPLES

Track-It! Inventory audits occur on a continual basis: the CDI does not conduct sample inventories.

5.0 INTERNAL AUDITS

5.1 STAFF RESPONSIBLE FOR PERFORMING INTERNAL AUDITS

The CDI Internal Audit Bureau will review (audit) CDI's SMP processes and ensure there are no deviations from the mandatory requirements of the Software Management Policy in SAM Section 4846 including all applicable laws associated with software licensing.

5.2 STAFF NOTIFIED OF INTERNAL AUDIT RESULTS

Findings from CDI Internal Audit Bureau will be given to the ITD CIO and ITD Bureau Chiefs.

5.3 COMMUNICATIONS FOR INTERNAL AUDIT RESULTS

The ITD will require the audit report provide specific information to convey results of internal compliance review. The compliance review report must provide:

- Brief description of the review procedure.
- Audit findings of the processes and procedures used at CDI in support of compliance with SAM requirements for software management.
- Recommendations on actions that should be taken to remedy any issues found during the compliance review.

6.0 CORRECTIVE ACTION/ADVERSE ACTION

Corrective action and possible adverse action may be taken whenever repeated violations of policies and procedures defined in the SMP occur. The following processes will support corrective actions and when necessary, adverse action.

6.1 STAFF RESPONSIBLE FOR CORRECTIVE ACTION/ADVERSE ACTION

The SNS Bureau Chief is responsible for ensuring that mitigation actions (defined in Section 2.3) occur for each software infraction. When circumstances exceed two mitigations and may require corrective action, the Bureau Chief level manager representing the employee and the SNS Bureau Chief must be equally informed of the software violation with supporting documentation prior to CDI Human Resources (HR) notification. The employee's direct supervisor and/or manager will determine when HR is contacted. HR is used as a resource for advice regarding the kind of corrective action that may be appropriate, such as; verbal counseling or written warning/memo. When corrective action steps have been exhausted, repeated violations of policies and procedures have occurred, and it has been deemed appropriate by the employee's direct supervisor, the HR manager will be contacted regarding the adverse action process.

6.2 PROCESS FOR ACCOMPLISHING CORRECTIVE ACTION/ADVERSE ACTION

CDI HR Management Division has an existing process in place for accomplishing Corrective Action/Adverse Action. For guidance and direction regarding these processes the HR Management Division should be contacted.

The basis for corrective action is as follows:

a. Repeated violations of either copyright law, software license usage, or related CDI software policy by the same employee(s).

b. Repeated violations of policies and procedures, as defined by this SMP by the same employee(s).

c. Evidence that an infraction by an employee or group of employees was intentional.

The basis for adverse action is as follows:

a. Repeated violations of either copyright law, software license usage, or related CDI software policy by the same employee(s), after corrective action has been taken to correct this issue.

b. Repeated violations of policies and procedures, as defined by this SMP by the same employee(s), and corrective action has not resolved this issue.

c. Evidence that an infraction by an employee or group of employees was intentional, and corrective action has not resolved this issue.

CDI ITD will provide documentation related to the mitigation(s) that occurred.

6.3 STAFF NOTIFIED OF CORRECTIVE ACTION

When corrective action/adverse action is recommended, the employee's Bureau Chief, the CIO, and HR will be contacted. Notification will include the following information:

- Description of the reason the corrective action/adverse action may be necessary.
- Documentation supporting steps previously taken to resolve the software infraction.

6.4 PROCESS FOR KEEPING INFRACTIONS FROM REOCCURRING

To keep software infractions from reoccurring, supervisors will be responsible for ensuring their employees fully understand the ramifications and consequences of a software violation. All technical

support staff will be educated and responsible for adhering to CDI software policies, software copyright laws, software licensing agreements mitigation procedures.

7.0 CONTRACTOR'S CERTIFICATION

7.1 STAFF RESPONSIBLE FOR ENSURING CONTRACTOR CERTIFICATION

The CDI Procurement Office in the Business Management Bureau (BMB) will ensure that all new purchase orders or contract agreements for the purchase of software include or reference the necessary software compliance language, as defined by the Department of General Services (DGS). The ITD Procurement Officer will ensure that software vendors are aware that a certification is required as part of any contract award or release of a purchase order to the vendor.

7.2 PROCESS FOR RECEIVING CONTRACTOR CERTIFICATION OF COMPLIANCE

The BMB Procurement Staff and the Contract Manager will ensure certification has occurred. Any necessary signed certification statement will be submitted to the ITD Procurement Officer as part of the final contract. Contracts, including certifications, are maintained with the official procurement records within the BMB.

7.3 MEASURES TAKEN TO ENSURE CONTRACTOR COMPLIANCE

The BMB Procurement Staff will ensure the final signed contract includes certification of compliance, as stated in Section 7.1.

7.4 MEASURES TAKEN IF CONTRACTOR DOES NOT COMPLY

The Contract Manager must document any evidence of non-compliance. The Contract Manager may request vendors provide validation that they have appropriate systems and controls in place to ensure their use and maintenance of CDI funded software will not violate copyright laws. If a Contractor is deemed to be in non-compliance, the contract may be terminated, which must be supported by adequate documentation of non-compliance provided by the Contract Manager.

8.0 DISPOSAL OF HARDWARE AND SOFTWARE

8.1 STAFF RESPONSIBLE FOR DISPOSAL OF HARDWARE AND SOFTWARE

The following positions will be responsible for the disposal of software and hardware components in their respective areas from an inventory control and asset management perspective:

- The SNS Bureau Chief will be responsible for the disposal preparation including documentation of inventory records.
- The BMB will be responsible for the actual disposal of the hardware and software.

8.2. HARDWARE AND SOFTWARE DISPOSAL PROCEDURES

The CDI has developed the following software disposal procedures:

a. The software name, manufacturer, and version are identified.

b. The authorized technical resource will remove any installation copies of the software installed on network servers and/or network installation servers.

c. The authorized technical resource will permanently check-out for disposal, all hard copies of the media, manuals, and license information specific to that one serialized piece of software from the Secure Repository.

d. The authorized technical resource will remove the identified software from all applicable technology equipment.

e. If all the original documentation is located and the software licenses have not been used for competitive upgrades, the software may be donated to charitable organizations. The BMB may donate the official software media/license package according to CDI policy and procedures.

f. If the original media or license is missing, the BMB will ensure destruction of the remaining items. Software media and documentation earmarked for destruction will be periodically taken to a disposal facility by the Business Management Bureau.

g. The spreadsheet will be updated to document final disposition information including: date of disposal, method of disposal (donation, return, destruction), and person who disposed of the item.

h. Track-It! will identify software removed from the network through its automatic scanning process.

Hardware will be disposed when it is no longer operational or supported by the manufacturer and is deemed unusable by CDI ITD. When hardware is disposed of, there are additional steps to be completed prior to disposal, such as disposal of software, removing department data, identification tags, etc. that reside on the hardware.

9.0 ROLES AND RESPONSIBILITIES FOR THE ADMINISTRATION OF THE SOFTWARE MANAGEMENT PROGRAM

The following roles and responsibilities are defined for the administration of CDI's software management program:

9.1 ROLES AND RESPONSIBILITIES OF CDI EXECUTIVE STAFF

a. Ensure software management policies and consequences for not following policies are communicated to all employees.

b. Demonstrate compliance and support of the plan through his/her own actions and response to others when infractions occur.

c. Support mitigation/corrective action processes when employees and contractors are found to have not complied with CDI policies and procedures.

9.2 ROLES AND RESPONSIBILITIES OF CDI DEPARTMENT MANAGEMENT

a. Enforce software compliance through employee awareness and signature of the Code of Ethics.

b. Maintain information on any specific software infractions in their areas.

c. Report unlicensed software and/or software that is not approved for use to the ITD Help Desk or ITD Help Desk Supervisor.

d. Verify that employees do not have any CDI hardware or software in their possession at the time of separation from the CDI.

e. Proactively plan for software needs and ensure needed software licenses are properly procured.

f. Do not request or endorse unlicensed or not approved software to be installed on any CDI computer.

g. Initiate mitigation/corrective actions when employees are found to have not complied with CDI policies and procedures.

h. Ensure contractors maintain compliance with software licensing when supporting CDI processes.

i. Implement mitigation actions if a contractor is not in compliance.

9.3 ROLES AND RESPONSIBILITIES OF CDI USERS

CDI Employees will:

a. Become knowledgeable on CDI software management practices.

b. Adhere to CDI Software Management policies and procedures.

c. Report any software that is unlicensed or not approved for use to immediate supervisor or manager.

d. Do not request or endorse unlicensed or not approved software to be installed on any CDI computer.

e. Return any CDI software or hardware in their possession prior to their separation from the CDI.

CDI Contractors will:

a. Comply with California state and federal policies and regulations relating to copyright laws.

b. Provide signed statement of software compliance for each CDI business agreement, when requested.

9.4 ROLES AND RESPONSIBILITIES OF THE CDI SOFTWARE MANAGEMENT TEAM (SMT)

CDI SMT as a group will**:**

a. Develop, implement, and maintain the necessary and appropriate policies, processes, and procedures to effectively manage the CDI's software and software license related activities.

b. Develop an education plan for CDI employees on software management policies and practices, coordinate the delivery of the Software Management Education Policy to all employee groups, and report status, as deemed appropriate.

c. Communicate the requirement and value of compliance with software licenses.

d. Enforce software management policies and procedures.

e. Ensure on-going inventories occur and that methods used are consistent and reliable.

f. Ensure the various tasks, processes, and activities that occur on a daily basis to support computer users and network systems are structured to comply with the requirements of CDI's Software Management Plan.

g. Work closely with the SNS to periodically monitor activities associated with the Secure Repository to uphold compliance standards.

h. Verify for CDI Managers and Supervisors whether departing employees have items checked out of the Secure Repository.

i. Ensure that Control Agency reports are completed and submitted/available according to reporting requirements.

SNS Manager & Staff will:

a. Monitor the progress of the inventory, ensure the spreadsheet is updated, and serve as the primary point of contact for questions or issues.

b. Utilize the ITD Help Desk system to track mitigation activities.

c. Participate and/or cooperate in inventories, audits, illegal and/or not approved software identification, and mitigations.

d. Perform on-going inventories using consistent and reliable methods.

e. Follow all policies and procedures developed to support this plan and maintain full compliance with State software management requirements and copyright laws.

f. Follow all processes and procedures for software and hardware disposal.

g. Manage desktop software media checked out from the Secure Repository.

h. Verify available licenses before any piece of software is installed.

i. Ensure that the automated tool(s) capture the necessary inventory information.

j. Provide Track-It! and ITD Help Desk data/reports as required by the reporting needs of the plan.

k. Provide the Procurement Officer with the original registration card or other proof of registration for all new software purchases.

ITD Help Desk Staff will:

a. Inventory laptops, scanners, printers and other applicable equipment not consistently connected to the network.

b. Use the ITD Help Desk system for all activities and issues associated with software.

c. Prepare hardware for disposal by performing a 'clean disk.'

ITD Manager/Supervisor who receives the software for the CDI will:

a. Practice software and software license receiving procedures.

CDI Information Security Officer / Internal Auditors / HR will:

a. Respond to reports of suspected software violations or illegal software practices.

b. Conduct internal audits annually to monitor the compliance of ITD to the CDI Software Management Plan.

c. Document reports of all internal audit findings and provide to the CIO and ITD's Branch Deputy Director.

ITD Procurement Staff will:

a. Maintain original records of software licensing types and current CDI licensing arrangements.

b. Ensure completion of the original registration card or other proof of registration.

c. Negotiate (and renegotiate) contracts and contract addendums to include necessary software compliance clauses, when necessary.

d. Verify contractors have appropriate software compliance language in their contracts before any software is installed, when necessary.

In addition, the ITD has designated a staff from the PCAS Bureau as the ITD Software Manager. This staff person has responsibility for oversight of the software management processes and procedures.

10.0 ACTION PLAN

An Action Plan was developed by the CDI SMT to identify the activities that occurred to bring CDI into full compliance with the Executive Order (D-10-99) and to maintain an ongoing Software Management Program. The Action Plan is documented in the SMP 2003.

11.0 TIMELINE

The CDI is currently in full compliance with the Executive Order (D-10-99) mandating each State agency work diligently to give effect to copyrights associated with computer software. The CDI has developed and implemented software management practices in accordance with software management plans initiated in 2002. The CDI has certified that software management policies and procedures defined in this SMP 2004 are in effect.

12.0 SUPPORTED SOFTWARE LIST

The CDI has developed a comprehensive list of software that CDI supports. This list includes information to identify the type of software, who uses it, who buys it, and the ITD Help Desk support level that will be provided for the software. This supported software list is referred to as the List of Approved Standard Hardware/Software or Services.

13.0 SOFTWARE MANAGEMENT EDUCATION

All CDI employees granted access to CDI funded technology equipment and software will be educated on software piracy, the role of government in combating piracy, specific CDI policies and procedures for complying with Federal and State copyright law, and information on good software management practices. New employees will receive this software management training as part of their new hire orientation. Continuing software education will be provided through technology-specific classes, periodic communications such as newsletters, Intranet postings, and CDI IT Circulars.

Subject-specific training will also be delivered to certain CDI groups including executives/management, procurement, receiving, ITD Help Desk, desktop/server/network administration, and internal auditing. This subject-specific training will further explain the roles, processes, responsibilities, and accountability each of these groups has in helping the CDI administer and enforce its software management plan.

It is the practice of the CDI to respect and govern business operations according to all computer software copyrights and to adhere to the terms of all software licenses to which the State of California and its entities are a party. The CDI employees are obliged to adhere to the Software Copyright Policy and fully participate in upholding legal and proper use of software residing on CDI equipment.

Any person illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. All employees must refrain from explicitly or implicitly condoning illegal copying of software under any circumstances. CDI may take disciplinary action against staff who breach the policy. According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages, criminal penalties, and imprisonment.

Any employee who is aware that there may be a misuse of software within the Department will notify his/her manager or the CDI ITD Help Desk.

The Software Management Plan and Software Copyright Policy are located on the **CDI Intranet site.**

14.0 SUBMISSION OF AND UPDATES TO THE SOFTWARE MANAGEMENT PLAN

The CDI has prepared an SMP in accordance with SAM 4846, and the guidelines of SIMM Section 120. The CDI certifies that the SMP is in effect. The SMP documentation and the summary of CDI's software inventory are maintained in CDI files within the Information Technology Division and are available for Control Agency review, upon request.

APPENDIX A – SOFTWARE INVENTORY SUMMARY

Publisher/Software Title	Version	Number of Installations (A)	Licenses Owned (B)	Reconciliation Number (B - A)
ACL for Windows	7.2	12	22	10
Adobe Acrobat 5.x	5.0.5.0	109	60	(49)
Adobe Acrobat 6.x	6.0.0.0	7	7	0
Adobe Illustrator	8.0	4	12	8
Adobe Pagemaker	7.0	10	15	5
Adobe Photoshop	6.0.1	19	23	4
Arcview	8.3	1	1	0
Avaya (nee Octel) Base System	Rel. 2 Ver. 3	65	100	35
Avaya Full implementation	Rel. 2 Ver. 3	250	250	0
Avaya Mailbox Manager	Rel. 2 Ver. 3	1	1	0
Avaya Octel Access Software	Rel. 2 Ver. 3	1	1	0
Avaya Octel Analog Networking	Rel. 2 Ver. 3	1	1	0
Blue Ocean Track-It Enterprise (35 Named Users including Agent, Receive, Sync modules)	5.0	41	41	0
Blue Ocean Track-It Enterprise PC Audits	5.0	Con-current	100	0
Blue Ocean Track-It Knowledgebase - 10, per year	5.0	0	10	10
Blue Ocean Track-It PC Audits 1500 add'l, per year	5.0	1542	1700	158
Blue Ocean Track-It Web 100, per year	5.0	Con-current	100	0
Cisco Ciscoworks LMS 2.0 upgrade	2.0		1	1
Cisco Network Management Assessment Tool - Pro Plus Edition		1	1	0
Cisco Security Scanner		1	1	0
Commview Remote sites config/setup (7 sites)		7	7	0

Publisher/Software Title	Version	Number of Installations (A)	Licenses Owned (B)	Reconciliation Number (B - A)
Corel Wordperfect	2002	4	4	0
Crosseyes	2.1	1	3	2
Crystal Reports for ESRI - Archview 8.1	8.0.1.0	1	1	0
Digital Secure Certificate	N/A			
Documents to Go Pro Edition (Handheld Version of Word/Excel)	4.0	17	10	(7)
Dragon Naturally Speaking	7	7	8	1
EDI Document Imaging Electronic		2	2	0
Encase	1.2	0	18	18
Encase	1.2	0	6	6
Encase	4.0	0	10	10
E-vantage Enterprise Viewer V2	2.0	313	380	67
E-vantage Host Access Server 2	2.0	1	1	0
E-vantage SNA Gateway 2.1 FUL	2.1	1	1	0
Exambuilder	4			
Microsoft Front Page 2K2 Eng Std	2002	104	80	(24)
FTP Control 4.0 Power Version	4.0	6	1	(5)
Hummingbird DOCS Open Transit Central EDM Server	3.9.6	1	1	0
Hummingbird DocsOpen Client	3.9.6	147	141	(6)
Hummingbird DocsOpen Server	3.9.6	1	1	0
Hummingbird Web Publishing Server	3.9.6	1	1	0
IC Verify Windows v 2.5 - Multi-user upgrade	2.5		1	
JSPELL Client Server Edition w/Source v.2.0	2.0	0	1	1
LawPack Family Maintenance Renewal	5.0	159	Unlimited site license	0

Publisher/Software Title	Version	Number of Installations (A)	Licenses Owned (B)	Reconciliation Number (B - A)
Lophtcrack Upgrade	2.1	1	1	0
Microsoft BackOffice Client Access Lic	2000	Access Rights only	1400	0
Microsoft Exchange 2000	2000	0	1	1
Microsoft Exchange Server 2000	2000	6	6	0
Microsoft Exchange Server Enterprise 2000	2000	8	8	0
Microsoft Office Professional English Upgrade Advantage	2002		1250	
Microsoft Project 2000 (License)	2000	33	40	7
Microsoft Project 2002 (License)	2002	18	19	1
Microsoft Visio STD 2002 WIN32	2002	178	38	(140)
Microsoft Windows 2000 Advanced Server - Core Implement Option for Media Agent	2000	3	3	0
Microsoft Windows 2000 Advanced Server- 1 silo support software for up to 32 slots	2000	3	3	0
Microsoft Windows 2000 Advanced Server I-data Agent	2000	10	10	0
Microsoft Windows 2000 Advanced Server Media Agent	2000	3	3	0
Microsoft Windows 2000 Professional Upgrade (95/98)	2000	1408	1306	(102)
Microsoft Windows Advanced Server 2000	2000	104	104	0
Microsoft Windows XP (2000/XP) Professional	XP	14	14	0
Monarch Version 5 Pro	5.0	24	27	3
Net Tracker Enterprise License	6.0	1	1	0

Publisher/Software Title	Version	Number of Installations (A)	Licenses Owned (B)	Reconciliation Number (B - A)
NetworkIT 2.0 Advanced Edition (NT/2000 Unlimited IP Devices Ld)	2000	0	1	1
NetworkIT 2.0 Advanced Edition System Agent for Client/Server	2000	0	70	70
Norton Systemworks 2001, 3.0 CD ROM, Pro 4.0	2000	0	1	1
Oracle - Admin Knowledge Xpert	5.0.7	3	3	0
Oracle - Application Server Enterprise Edition- Qty 1096 Power Units	9iAS		1	
Oracle - Forms Server Power Unit Intel Qty 1096 Power Units			1	
Oracle - Knowledge Xpert or PL/SQL Developer	5.0.7	5	5	0
Oracle - Reports Server Power Unit Intel Qty 1096 Power Units			1	
Oracle - SQL Impact Seat-single Server per seat	3.2.6	0	2	2
Oracle Financials annual maintenance renewal	11i		1	
Oracle License - 14 9iAS	9iAS	8	14	6
Oracle License - 2 9iAS Personalization Module	9iAS	0	2	2
Oracle License - 25 iDS Designer Web	9iAS	8	25	17
Revenue Collector/Cashiering For Windows Enterprise	2.5/4.0	17		
SAS Enterprise Package	8	1	4	3
SAS On-Line Tutor Software, Version 8	8	1	4	3
Second Wind Version 2	2	0	60	60
SPSS Maintenance (contract 100193045)	11.0	1	1	0

Publisher/Software Title	Version	Number of Installations (A)	Licenses Owned (B)	Reconciliation Number (B - A)
Summation	2.5.2	3	3	0
Sun Solaris 8 - Client License	8		1	1
Sun Solaris OS	2.8	1	1	1
Symantex Ghost 7.0 Corp (plus 20 media)	7.0	2	10	8
TeamMate 2000 software (Market Conduct Exam Software)	2000	31	66	35
Technet Plus Starter Kit	N/A	4	4	0
TN3270 Emulation software		1	1	0
TOAD DBA Module	7.4.0	3	3	0
Toad Pro edition including PL Formater	7.4.0	7	7	0
TOAD SQL Impact	7.4.0	2	2	0
Toad Std edition including PL Formater	7.4.0	4	8	4
Toad Xpert edition includes Debugger Xpert, PL Formater	7.4.0	4	4	0
TrendMicro Neatsuite for NT			1400	
VRS (Voice Response Software)		1	1	0
Websense Enterprise - PIX			2500	
Webtrends Web Analysis Tool Enterprise Suite Essential Care		1	1	0
Win Fax Professional 9.0	9.0	4	1	(3)
WinZip 8.0 Site License	8.0		73	
WRQ Reflection for HP Terminal Emulation	9.x	0	1	1
Patchlink	5.0	1780	1814	34
I-Notes (Domino Web Access)	6.5	13	13	0
DreamWeaver MX	6.0	6	6	0

APPENDIX B – SECURE REPOSITORY INVENTORY

Application Development and Management (ADAM) Secure Repository Plan
Repository Inventory List (as of September 2003)

The Sacramento Application Development and Maintenance Repository contains the following software:

Vendor Name	Software Name	License	Quantity	Version	On Network Drive (Y or N)
Oracle	Internet Developer Suite-Named User Perpetual includes: • Oracle Warehouse Builder • Oracle 8i Quick Suite Install • Discoverer Desktop • Discover Administration • 8i Enterprise Edition – Server • Oracle Designer 6I & Repository 6I • Oracle Designer Upgrade 1.3.2 to 6i • Oracle Forms & Reports 6i • Oracle Forms & Reports - Patch 4A • Oracle Forms & Reports 6i - Demo • Oracle Jdeveloper • Oracle Tutor Start-Up • Oracle OLAP Client • Oracle 8i lite (forms interface)	Y	25	1.0.2.4.1 CD Pack	Designer & Repository; Forms & Reports and all associated patches on network drive
Oracle	Internet Application Server Enterprise Edition – Processor Perpetual	Y	2	9ias	N
Oracle	Internet Application Server Enterprise Edition – Processor Perpetual	Y	12	9ias	N
Oracle	Personalization – Processor Perpetual	Y	2	9ias	N
Oracle	Financials	Y	16	10.5/ 11i	
Sun	Solaris Operating System	Y	1	2.8	N
MacroMedia	DreamWeaver MX	Y	6	6.0	N
Quest	Standard Edition Includes PL Formatter	Y	6	7.4.0.1	Y
Quest	TOAD Professional Edition Includes PL Formatter & Debugger	Y	7	7.4.0.1	Y
Quest	TOAD Expert Edition Includes PL Formatter & Debugger and DBA Module	Y	5	7.4.0	Y
Quest	Knowledge Xpert for PL/SQL	Y	6	5.0.7	Y

	Development				
Quest	Knowledge Xpert for Oracle Administration	Y	3	5.0.7	Y
Quest	SQL Impact Seat-Single Server Per Seat	Y	1	3.2.6	Y
Quest	SQL Lab Expert-TOAD Add on	Y	5	34.3.0.2.0	Y

The following image is maintained by ADAM in Sacramento and contains the following software:

The Los Angeles Repository contains the following software

[1]FIDB Image

1. Windows NT Service Pack 2 Version 5,0 Build 2195
2. Oracle Designer 6i 6.5.88.4.0 Production
3. PL/SQL Release 8.1.7.3.0
4. (Oracle Forms 6.0.8.19.2(Patch 10
5. Oracle Reports 6.0.8.19.0(Patch 10)
6. Internet Explorer ver: 5.51.4807.2300
7. Winzip ver 8.1
8. TOAD ver 7.3.0.0
9. Visio Professional ver 5.0c
10. Acrobat 5.0.5 full version
11. ODBC 8.1.7.5
12. FTP ver 3.0.0.117
13. TNVT plus ver 3.0.0.117

Statewide Network Support (SNS) Secure Repository Plan

Repository Inventory List as of December 2003

The Statewide Network Support Repository contains the following software in Sacramento, Los Angeles or
San Francisco:

Vendor Name (See inventory list)	Software Name	License (See inventory list)	Quantity (See inventory list)	Location
ACL	ACL for Windows			Sacramento
Adobe	Adobe Suite includes: • Acrobat 6.0 • After Effects 5.5 • Illustrator 9.0 • Pagemaker 7.0 • Photoshop 7.0 • Premiere			Sacramento
Attachmate	Attachmate E-vantage Enterprise Viewer V2			Sacramento
Avaya	Avaya Suite includes: • Base system • Full implementation • Mailbox Manager • Octel Access Software • Octel Analog networking			Sacramento
	BackOffice Client Access			Sacramento
	CardScan Executive v6			Sacramento
Cisco	Ciscoworks LMS 2.0			Sacramento
Crystal Decisions	Crystal Reports for ESRI Archview 8.1			Downloaded
	Cyberforensic Pro 3000			Sacramento IA
VeriSign	Digital Secure certificate			Sacramento
	Diskeeper 7.0 server			Sacramento
Dataviz	Documents to Go Pro Edition			Sacramento
Dragon	Dragon Naturally Speaking			Sacramento
	Established Position Record Cards			Sacramento
Attachmate	E-vantage includes: • Host Access Server 2 • SNA Gateway 2.1 FUL			Sacramento
Microsoft	Exchange includes: • Exchange 2000 • Exchanger Server 2000 • Server Enterprise 2000			Sacramento

Vendor Name (See inventory list)	Software Name	License (See inventory list)	Quantity (See inventory list)	Location
	Forensic Recovery of Device Senior			Sacramento
	Fastbloc IDE			Sacramento
	Forensic Utility Suite includes: • TCP/IP client • Console • IPX/SPX client • Recover NT Express • Recover98 Express			Sacramento
Microsoft	Frontpage 2002			Sacramento
BMTMicro	FTP Control 4.0 Power Version			Sacramento
	GFI Languard Network Security Scanner			Sacramento
Hummingbird	Hummingbird Suite includes: CyberDocs DOCS Open Client DocsOpen Client Docs Open Server Fusion Server Web Publishing Server			Sacramento
	IC Verify Windows v.2.5 – multi-user upgrade			Sacramento
	Informatics-WASP Barcode Nest Suite CCD Ba edition			Sacramento
Hummingbird	LawPack includes: • Family Maintenance Renewal • Users			Sacramento
	LinkScan Server 11.0			Sacramento
	LophtCrack LC4 and upgrade			Sacramento IA
	MI USB Security Key			Sacramento
Datawatch	Monarch Pro v5			Sacramento
Marketware	Microsoft Suite includes: • Microsoft Software for Windows Servers • Office Family • Applications Training and Learning • Server Applications			Sacramento
	Neatsuite for NT			Sacramento
	Network suite includes: • Management Assessment Tool –Pro Plus Edition			Sacramento

Vendor Name (See inventory list)	Software Name	License (See inventory list)	Quantity (See inventory list)	Location
	• IT 2.0 Advanced edition • IT 2.0 Advanced edition system agent for client/server			
	Partition Magic 8.0			Sacramento
	Procomm Plus for Windows (200, XP, NT)			Sacramento
	Programming F4OGS for ICOM			Downloaded
	Revenue Collector Maintenance			Sacramento
SAS	SAS Enterprise, renewal and tutor			Sacramento
	SCIF			On-line
	Security scanner			Sacramento
	Sniffer DSPro 4 and Pro Lan Perpetual			Sacramento
	Solaris 420R and 8			Sacramento
	SPSS Maintenance			Downloaded
	Symantex Ghost 7.0			Sacramento
	TeamMate 2000			Sacramento
	Technet Plus Starter Kit			Sacramento
Intuit	Track-It! Enterprise, knowledgebase, web			Sacramento
	Ultimate System Management Toolkit			Sacramento IA
	USPS Rates			Sacramento
VeriSign	VeriSign Secure Site Certificate			San Francisco
	VRS (voice response software)			Sacramento
Websense	Websense for 1500 users			Sacramento
Webtrends	Webtrends web analysis tool enterprise suite			Sacramento
	Win Fax Pro 9.0			DownLoaded
	Windows 2000 Advanced, professional, server			Sacramento
	XIOX software (phones)			Sacramento
Corel	WordPerfect Office 11			Sacramento

APPENDIX C – SOFTWARE MEDIA CHECK-OUT LOG

REQUESTOR	AUTHORIZED BY	PRODUCT CHECKOUT DATE	SOFTWARE PRODUCT NAME, VERSION	REASON FOR REQUEST: 1.INSTALL 2.DISPOSE 3.TRANSFER	WHERE WILL S/W BE USED DESKTOP ID	DATE PRODUCT RETURNED (**NO MORE THAN 3 DAYS**)