SPECIAL REVIEW

CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION'S OFFICE OF INTERNAL AFFAIRS INFORMATION SECURITY

OFFICE OF THE INSPECTOR GENERAL

DAVID R. SHAW
INSPECTOR GENERAL

STATE OF CALIFORNIA

MAY 6, 2009

David R. Shaw, Inspector General

Office of the Inspector General

May 6, 2009

Matthew L, Cate, Secretary
California Department of Corrections and Rehabilitation
1515 S Street, Room 502 South
Sacramento, California 95814

Dear Mr. Cate:

Enclosed is the final report of a special review conducted by the Office of the Inspector General into the California Department of Corrections and Rehabilitation's information security over internal affairs investigations. Specifically, we assessed whether the department's Office of Internal Affairs (OIA) takes appropriate security measures to protect personal, confidential, and sensitive data from unauthorized access or use and whether OIA maintains proper accountability of its laptop computers.

The review found that OIA violated numerous state rules by not adequately protecting the personal, sensitive, and confidential data stored on its agents' laptop computers. In addition, OIA agents and managers are violating state requirements by sending emails with confidential material to unsecured email addresses. Moreover, OIA does not maintain adequate inventory control over its laptop computers and has had several laptops lost or stolen in 2008.

The report makes four recommendations to correct the problems and deficiencies found during the special review. Included as an attachment to the report, is the department's written response to the special review.

Thank you for the courtesy and cooperation extended to my staff during the course of this review. Please call Jerry Twomey, Chief Assistant Inspector General, at (916) 830-3600 if you have any questions.

Sincerely,

David R. Shaw
Inspector General

cc: David Grant, Assistant Secretary, Office of Internal Affairs
Kim Holt, External Audits Coordinator

Enclosure

Contents

Executive Summary

This report presents the results of a special review conducted by the Office of the Inspector General (OIG) into the security of the information systems maintained by the California Department of Corrections and Rehabilitation's (CDCR) Office of Internal Affairs (OIA). Specifically, we assessed whether OIA takes appropriate information security measures to protect personal, confidential, and sensitive data from unauthorized access or use and whether OIA maintains proper accountability of its laptop computers. We conducted this review under the authority of California Penal Code section 6126, which assigns the OIG responsibility for oversight of the California Department of Corrections and Rehabilitation.

Our review revealed the following inadequacies in OIA's information system security:

- **OIA violated numerous state rules by not encrypting the personal, sensitive, and confidential data stored on its agents' laptop computers, which could lead to the inadvertent release of confidential information.** OIA is responsible under state rules to protect any personal, sensitive, or confidential data stored on any electronic medium. This personal data includes social security numbers, home addresses, telephone numbers, and educational, financial, medical or employment history. Even though state rules require that this confidential data be maintained in a secure fashion, we found that OIA agents store personal, sensitive, and confidential data on computers not protected with encryption software. During our review of OIA laptop computers, we found that over 68 percent contained confidential case files, including names, addresses, photographs, and criminal allegations made against correctional staff members who are under investigation for misconduct. Unauthorized or unintended release of such information could potentially jeopardize the success of an investigation against departmental employees or result in damages against the state due to the release of confidential material. In fact, losing a laptop computer is not just a theoretical possibility at OIA, but rather, during the course of our review, OIA inventory records indicated that five laptop computers were reported as missing or stolen since February 2008. If the missing or stolen computers contained files similar to those that we identified in our review, it is likely that confidential data has already been compromised.

- **OIA agents and managers are violating state requirements by sending confidential emails to unsecured email addresses.** In spite of the requirement for OIA to protect any personal, sensitive, or confidential data stored on any electronic medium, we discovered that OIA agents and managers were emailing confidential electronic files over the internet, thereby subjecting the material to indiscriminate viewing. From our sample of OIA emails reviewed, we found that over five percent of the emails with attachments that were sent outside of the state's email system were stored on public servers and contained confidential

information, including names, addresses, audio recordings and criminal allegations made against correctional staff who were under investigation for misconduct. The material sent to servers outside of the state's control could be subject to public release and could constitute a breach of confidentiality and expose the state to lawsuits and potentially jeopardize an investigation against correctional staff.

- **OIA does not maintain adequate control over its inventory of laptop computers despite state requirements to do so.** OIA's system to track its inventory of laptop computers contained significant errors, limiting its ability to accurately account for all of its laptop computers. During our review of the laptop computer inventory at OIA, we found various errors and omissions on OIA's inventory tracking system, including 20 laptop computers that were assigned to the wrong user; 23 laptop computers that were not on the inventory tracking sheet, 16 of which did not have state required property identification tags; and 4 laptop computers that were reported as removed from service, yet were still in OIA's possession. These significant inventory tracking problems diminish OIA's ability to accurately monitor its inventory.

As a result of this special review, we made four recommendations to the assistant secretary for the Office of Internal Affairs. Specifically, the Office of the Inspector General recommends that OIA:

- Follow the State Administrative Manual requirements and obtain, install and use encryption software so that all personal, sensitive and confidential data stored on its laptop computers is protected.

- Develop and implement a policy that ensures that personal, sensitive, or confidential information attached to emails is protected. If necessary, OIA should restrict or prohibit personal, sensitive, or confidential attachments to emails sent outside of the OIA's email system.

- Develop and implement an accurate inventory tracking system and periodically audit its inventory to account for all of its laptop computers.

- Ensure that each laptop computer is fitted with a CDCR property tag and logged into the inventory system upon receipt to maintain adequate control over its information technology assets.

CDCR's Response

In its response, the CDCR agreed with the conclusions indentified in this report. Further, the CDCR states it is immediately addressing all identified deficiencies and that its corrective action will be reported to its Office of Audits and Compliance.

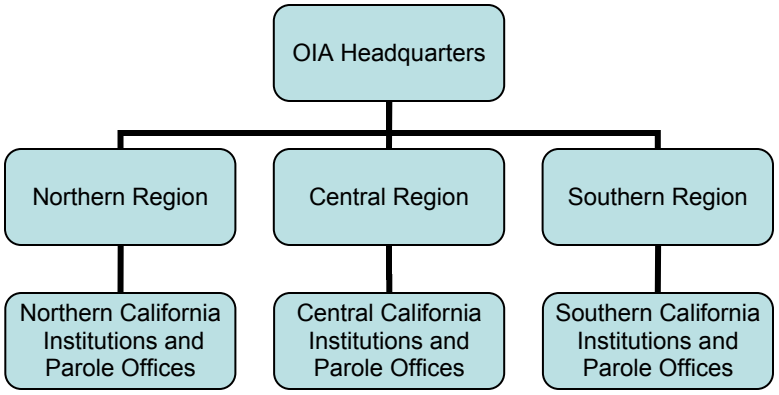
Introduction

Background

The Office of Internal Affairs (OIA) is responsible for providing comprehensive investigative services into allegations of employee misconduct at the California Department of Corrections and Rehabilitation (CDCR). Its agents are assigned to conduct investigations into allegations of misconduct by any employee of CDCR regardless of the employee's position or rank. Further, the OIA agents are responsible for conducting investigations in a manner that provides a complete and thorough presentation of all facts regarding the allegation, while refraining from conjecture or opinion.

The OIA is responsible for performing investigations of CDCR employees at adult institutions, fire camps, juvenile institutions, parole offices, as well as headquarters. To fulfill this mandate, the OIA maintains three regional offices throughout the state – the northern regional office in Sacramento, the central regional office in Bakersfield and the southern regional office located in Rancho Cucamonga. Each of these regional offices houses special agents who are responsible for investigations at the institutions and offices geographically located near the regional office, as shown in Figure 1 below.

Figure 1



In addition to the regional offices, OIA operates a headquarters office in Sacramento, which is responsible for processing the initial complaints of employee misconduct as well as conducting investigations where the regional offices might have a conflict of interest.

Because OIA is a law enforcement agency that routinely handles sensitive investigations, confidentiality of information is paramount to its operations. In fact, the OIA's operating procedures state that all investigative records of the OIA are confidential. The procedures further state that OIA investigators, OIA support staff and others involved in an investigation shall not discuss any aspect of any investigation with others, except department legal counsel and the OIG, without approval of OIA. Further, its operational procedures also require that all correspondence related to any OIA investigation be

clearly marked "confidential" and when using courier services, the procedures require that the material be sealed in such a way to prevent or reduce unauthorized access.

OIA further recognizes in its operating procedures that it has an ongoing responsibility to maintain the confidentiality of its investigative records, files and complaints. These procedures require that all reports, documents, evidence, and other materials or information relative to any investigation shall be processed and stored in a manner precluding unauthorized access or disclosure.

Objectives, Scope, and Methodology

The purpose of this review was to assess whether OIA adequately protects its data from unauthorized disclosure and its information systems from external threats and loss. Specifically, we assessed whether OIA takes appropriate information security measures to protect personal, confidential and sensitive data from unauthorized access or use, and whether OIA maintains proper accountability of its laptop computers. We focused on laptop computers during our inventory and file storage testing because the portable nature of laptop computers places them at a higher risk to be lost, stolen or accessed by unauthorized users.

In conducting this review, we performed the following procedures:

- Reviewed documents and interviewed staff members related to purchasing, tracking and assigning laptop computers to gain an understanding of OIA's operations and the nature and scope of its inventory system.

- Attempted to physically verify the location of each laptop computer at OIA to verify the accuracy of OIA's inventory records.

- Reviewed policies and procedures and interviewed key staff members to gain an understanding of OIA's information security protocols.

- Reviewed the data stored on a sample of laptop computers used by staff members and managers to determine whether OIA agents were storing personal, confidential or sensitive information on OIA laptop computers.

- Inspected the laptop computers and attempted to access the data on them to determine whether OIA computers contained encryption software.

- Collected and reviewed email messages for a sample of staff members and managers to determine whether OIA staff members were sending personal, confidential or sensitive information via email.

- Analyzed the data gathered in the above procedures to develop the information for this report

We conducted our fieldwork from December 2008 through January 2009 at OIA headquarters and each of the three regional offices.

Review Results

Finding 1

The Office of Internal Affairs violated numerous state rules by not encrypting the personal, sensitive, and confidential data stored on its agents' laptop computers, which could lead to the inadvertent release of confidential information.

Given the nature of its responsibilities, it is not unreasonable for personal, sensitive, or confidential data to be stored at least temporily on OIA's laptop computers. However, OIA is responsible under the State Administrative Manual (SAM) to protect this data. Even though the SAM requires that confidential data stored on any electronic medium be maintained in a secure fashion, we found that the personal, sensitive, and confidential data stored on the OIA computers we examined were not protected with encryption software. Furthermore, during our examination of the OIA laptop computers, we found that over 68 percent of them contained confidential case files on their hard drives, including names, addresses, photographs, and criminal allegations made against correctional staff members accused of misconduct who were under investigation. Unauthorized or unintended release of such information could potentially jeopardize the success of an investigation against departmental employees or result in damages against the state due to the release of confidential material.

OIA laptop computers frequently contained personal, sensitive, or confidential data

In order to identify the type of information that could be released publicly if an OIA agent or manager were to lose control of an OIA laptop computer, we reviewed the files that were contained on a sample of laptop computers. We reviewed laptop computers that were continuously assigned to a particular agent, as well as those laptop computers that OIA's information technology department checked out temporarily to an agent. In total, we reviewed 19 different laptop computers from all three regions and headquarters and found that 13 of them (68 percent) contained personal, confidential, or sensitive files.

For example, on one computer, we found several files that contained pictures that appeared to have been taken as part of an investigation. These pictures include graphic photographs of injured inmates. This same computer contained files with a surveillance video that appears to have been taken from a video camera on a prison yard. The video documents a fight between inmates and shows correctional officers using force to quell the fight. This computer also contained files of audio recordings of interviews with both subjects and witnesses in an investigation. Another laptop contained a wide variety of files that contained documents including a personnel file of a CDCR employee as well as a case summary that included names and addresses of individuals who were part of an investigation. Each of the 13 laptop computers contained information that was personal, sensitive, or confidential.

SAM requires security measures for personal, sensitive, or confidential data

Specifically, SAM section 5335.2 requires that "files containing confidential or sensitive data should not be stored on personal computer systems unless the agency can demonstrate…that security measures have been implemented to provide adequate protection." The SAM further requires in section 5345.2 that "encryption, or equally effective measures, is required for all personal, sensitive, or confidential information that is stored on…portable computing devices (including but not limited to laptop and notebook computers)."

Encryption software electronically transforms computer code into a non-readable format. The user of the encrypted text uses an electronic key that decrypts the message and returns it to its original plain text format. Essentially, if anyone were to obtain the encrypted data without the electronic key, it would be unreadable.

The SAM sections referenced above require each state agency that stores personal, sensitive or confidential data to take precautions to ensure the security of the data. As a law enforcement agency, the OIA conducts confidential investigations of employees of the CDCR, and because such investigations would frequently include personal, sensitive, or confidential information, these SAM sections clearly apply. As such, we expected to find encryption software, or equally effective measures on each of the laptop computers we reviewed. However, our inspection of a sample of OIA laptop computers found no encryption in place. In fact, using readily available software, we easily gained access to the data contained on the computers' hard drives.

Although encryption software is available at a relatively low cost, OIA did not purchase or install encryption software

Encryption software is available under the state contracting processes and can be obtained at a low per user cost. For example, the OIG's information technology (IT) manager provided us with a copy of the most recent purchase order that showed that the OIG obtained compliant encryption software for approximately $43 per computer and an annual fee of approximately $8 per user for technical support and maintenance. According to the manufacturer of this particular software, it provides full disk encryption and the encryption software is activated before the computer boots up. The manufacturer also claims that this system will protect the operating system from all known attack methods.

Using these costs, OIA could purchase encryption software for its 126 laptop computers for approximately $5,500, plus annual maintenance costs of approximately $1,000.

When we discussed this finding with the IT manager and executive management at OIA, they told us that they did not have any encryption software installed on any of their laptop computers. Not only is this lack of encryption not in compliance with the SAM, but more importantly, by not encrypting the data on its laptop computers, OIA could potentially compromise its investigations. If the contents of an investigator's computer were to be

shared with a subject of an investigation or potential witnesses, the department could lose its ability to discipline the employee. Moreover, if the state allows disclosure of personal information such as social security numbers, home addresses, telephone numbers, financial matters, education, and medical or employment history that would link the information to an individual, then the state may be liable for damages and attorney fees in accordance with the California Civil Code section 1798, et seq.

Losing a laptop computer is not just a theoretical possibility at OIA, but rather, during the course of our review, OIA inventory records indicate that five laptop computers were reported missing or stolen since February 2008. If the missing or stolen computers contained files similar to those that we identified in our review, it is likely that confidential data has already been compromised.

Recommendation

The Office of the Inspector General recommends that OIA follow the SAM requirements and obtain, install and use encryption software so that all personal, sensitive and confidential data stored on its laptop computers is protected.

Finding 2

The Office of Internal Affairs agents and managers violated state rules by sending confidential emails to unsecured email addresses

OIA has a responsibility under the SAM to protect any personal, sensitive, or confidential data stored on any electronic medium. In spite of this requirement, we discovered that OIA agents and managers were emailing confidential electronic files over the public internet, thereby subjecting the material to indiscriminate viewing. From our sample of OIA emails reviewed, we found that over five percent of the emails with attachments were sent outside of the state's email system and were stored on public servers, such as those owned by Google, Inc. The e-mails contained confidential information, including names, addresses, audio recordings and criminal allegations made against correctional staff who were under investigation for misconduct. The material stored on public servers could be subject to public release and could constitute a breach of confidentiality and expose the state to lawsuits and potentially jeopardize the investigation against correctional staff.

Confidential material was found in emails sent to public servers

In order to determine whether email messages were stored in a secure manner, we randomly selected 33 OIA staff email boxes for review. We focused primarily on the emails that were sent by OIA staff that included attachments, such as word processor documents, photographs, and audio recordings. We identified 1,861 messages in our sample of email files that contained attachments. Of these messages, we focused on those emails sent to addresses outside of state government, where messages would no longer be subject to state network security protocols. Therefore, we searched for only those messages with attachments that were sent to a .net or a .com address. We found that 109 of the 1,861 messages with attachments (5.9 percent) were sent to .com or .net addresses, however, the vast majority of these messages did not appear to contain confidential information. For example, one user forwarded messages such as jokes or information about political candidates[1]. Nevertheless, 6 of these 109 messages with attachments sent to .com or .net addresses contained confidential information.

We identified three users who sent confidential attachments over the email system. User One sent two confidential messages. The first file, sent in February 2008 contained the text of an internal affairs investigation report that included allegations that the peace officer participated in a "Code of Silence" by not reporting a use of force against an inmate. The report included summaries of interviews with staff as well as an inmate. The second file, sent in June 2007 included an audio recording of an interview with the subject of an investigation.

For User Two, we identified one confidential message sent in October 2008 regarding a case of misconduct involving two peace officers. The report alleges over familiarity with

[1] While incidental sending of these types of emails may not be in violation of state rules, the use of the state's email systems for personal use should be limited.

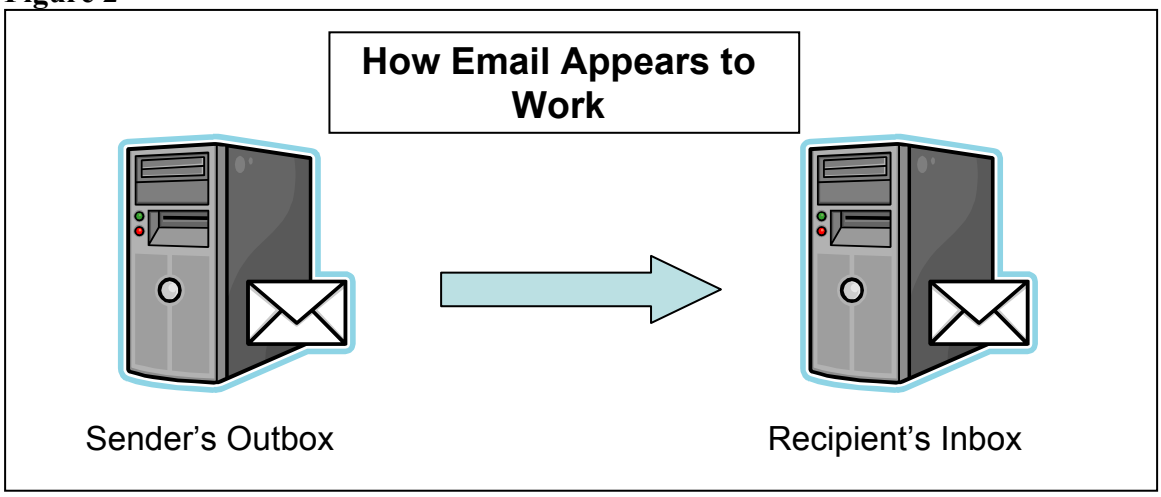
an inmate by these two employees and the report includes specific information about both employees and their families as well as detailed information about an inmate.

Lastly, User Three sent three confidential messages. One of these messages was sent to a gmail.com address and appears to be an investigative report written by an agent regarding an allegation of misconduct by an employee of an institution. This report contains specific documents from a local police department documenting criminal acts committed by the employee. This police report includes the home address of the employee as well as his alleged victim. The other two messages were notices to subjects of investigations to appear for interviews. These messages included the email address of the subject as well as the specific allegations that were under investigation.

Emails sent to public servers are not subject to the same security measures as those sent to state networks

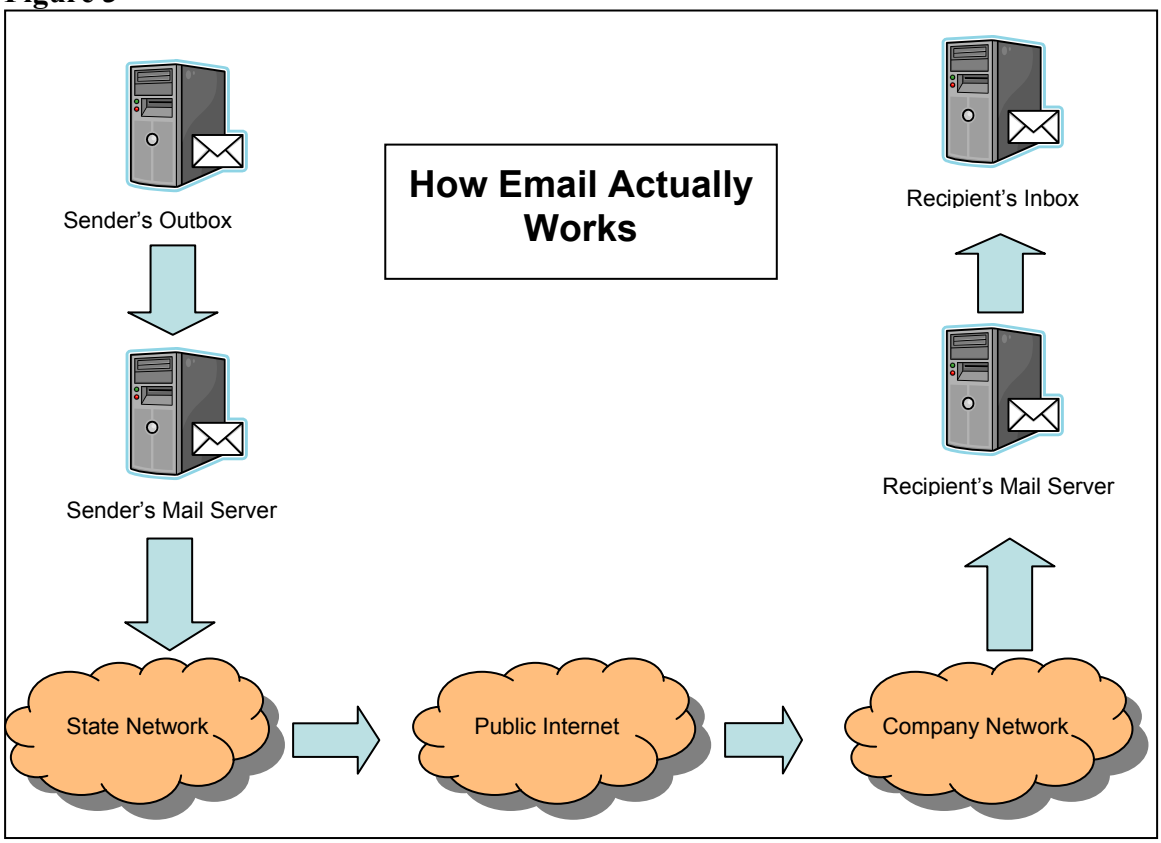
Emails, particularly emails sent to non-state agencies, are not subject to the same level of controls and security measures as those messages sent within the state network. To users of email, it may appear that the messages sent via email leave the sender's outbox and are instantly transported to the recipient's inbox as depicted in Figure 2 below.

Figure 2



However, email messages move through a series of servers on their way to the final destination. A simple, yet more accurate depiction of the lifecycle of an email can be seen in Figure 3 below.

Figure 3



Once the message leaves the sender's mail server as shown above, it is no longer in control of the sender. Therefore, these personal, sensitive or confidential reports and audio recordings that we discovered during our review, are available to users outside of the OIA.

Because these six messages we identified were sent to personal email addresses and stored on personal computers in a non-encrypted fashion, the senders exposed the confidential information to individuals and companies who should not have access to such confidential information. For example, one user sent a message to a gmail.com address. Google, the company that owns gmail.com has a published practice of retaining all documents sent through its email system. Therefore, this confidential document is likely stored on an email server maintained by Google, which is outside the control of the state. In fact, Google's privacy report found on its website states:

> *There are issues with email privacy, and most of these issues are common to all email providers. The main issue is that the contents of your messages are stored on mail servers for some period of time; there is always a danger that these messages can be obtained and used for purposes that may harm you.*

Although the SAM does not specifically prohibit the sending of confidential material via the internet, it states very clearly that personal, sensitive or confidential information must be protected. SAM Section 5345.2 reads:

> *Encryption, or equally effective measures, is required for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers).*

SAM section 5335.2 further requires that:

> *Information maintained in a personal computer system, including laptop computers and mobile devices, must be subjected to the same degree of management control and verification of accuracy that is provided for information that is maintained in other automated files. Files containing confidential or sensitive data (as defined in SAM Section 5320.5) should not be stored in personal computer systems unless the agency can demonstrate that doing so is in the best interest of the state and that security measures have been implemented to provide adequate protection.*

These SAM requirements exist to protect the state's information assets from unauthorized disclosure. However, once this information leaves the state networks, it is no longer subject to the same level of security controls and thus security could be compromised.

In addition to the SAM requirements for protecting confidential information, sending investigative data to an agent's home computer may open that computer to discovery. Discovery is the right of a party to a lawsuit to obtain information before trial, such as demanding the production of documents. Thus, when an agent sends investigative material to his or her personal computer, all personal data stored on that computer may be subject to unwanted viewing by plaintiff's or defendant's attorneys.

Recommendation

The Office of the Inspector General recommends that OIA develop and implement a policy that ensures that personal, sensitive, or confidential information that is attached to emails is protected. If necessary, OIA should restrict or prohibit personal, sensitive, or confidential attachments to emails sent outside of OIA's email system.

Finding 3

The Office of Internal Affairs does not maintain adequate control over its inventory of laptop computers despite state requirements to do so

OIA's system to track its inventory of laptop computers contained significant errors, limiting OIA's ability to accurately account for all of its laptop computers. During our review of the laptop computer inventory at OIA, we found various errors and omissions on OIA's inventory tracking system, including: 20 laptop computers that were assigned incorrectly; 23 computers that were not on the inventory tracking sheet; 16 of which did not have state required property identification tags; and 4 computers that were reported as removed from service, yet were still in OIA's possession. OIA's significant problems with its inventory tracking system diminish its ability to accurately monitor inventory.

The inventory listing did not accurately reflect all laptop computers maintained by OIA

In order to determine whether OIA had accounted for each of its laptop computers, we attempted to reconcile each entry on the inventory tracking system with a laptop computer in service. During this review, we discovered 23 computers that were not on the inventory tracking sheet. According to the IT manager at OIA, 7 of these computers were older laptop computers that became part of OIA's inventory when the California Youth Authority and California Department of Corrections became one department in 2005. However, 16 of the 23 computers were new and still in the factory sealed cartons. These computers were originally delivered to OIA in October 2007, but as recently as January 2009 had not even been removed from their original packaging. Consequently, OIA is wasting money, as well as its rapidly expiring computer resources. Further, these 16 laptop computers had not been identified as property of the state of California as required under SAM section 8651, which requires that,

> *All state property will be tagged after acquisition. The purpose of tagging assets is to designate the assets as belonging to the State. Tags will be placed so that they are in plain sight and easy to read.*

Not only did OIA violate the SAM requirement to tag these computers with state identification, OIA also placed these state assets at risk. Since OIA did not inventory or tag these laptop computers, if a computer was lost or stolen, OIA would have no record of its existence and possibly no awareness of its disappearance, nor would the asset have any identifying characteristics that it is state property.

In addition to these 23 computers that did not appear on the inventory listing, during our physical inspection we also found 4 laptop computers that were reported as removed from service. Generally, when an asset, such as a computer, exceeds its useful life, state agencies will remove these assets from service. During our review, we noted on the inventory sheet numerous computers that OIA had marked as removed from service. However, during our physical inspection of OIA laptop computers, we found that four of

these computers were actually still in service. Therefore, either OIA is not following appropriate procedures to remove old equipment from service or it has mislabeled equipment that is still functional. Once again, if one of these computers were lost or stolen, OIA would have difficulty detecting its loss through its inventory system.

OIA inventory list did not accurately reflect the employees who were assigned laptop computers

We also found problems with the accuracy of the inventory tracking system when reporting the assigned user of each laptop computer. For 20 of the 126 laptop computers reported on the inventory sheet by OIA, or nearly 16 percent, we found that the inventory sheet listed a user that was different from the staff person or location where we actually found the computer. For example, we found one laptop computer that was assigned to a staff person who had not been employed with OIA for well over 6 months. It is important for OIA to track the users of the laptop computers accurately because if one is ever lost or stolen, OIA is required to report information regarding the lost or stolen asset to the California Highway Patrol. If the inventory tracking system identifies the wrong user, OIA may inadvertently report the wrong computer stolen. Further, if a laptop computer is ever lost or stolen, the data contained on the computer may be compromised. As such, the OIA should accurately track the users assigned to each laptop computer in order to better assess the risks associated with the data lost on a particular computer. This risk is exacerbated by the facts as reported in finding 1, that OIA does not encrypt the data stored on its laptop computers; therefore, assessing the risks caused by a lost or stolen computer becomes even more critical.

Recommendations

The Office of the Inspector General recommends that OIA:

- Develop and implement an accurate inventory tracking system and periodically audit its inventory to account for all of its laptop computers; and

- Ensure that each laptop computer is fitted with a CDCR property tag and logged into the inventory system upon receipt to maintain adequate control over its information technology assets.

California Department of Corrections and Rehabilitation's Response

OFFICE OF THE SECRETARY
P.O. Box 942883
Sacramento, CA 94283-0001

April 29, 2009

Mr. David R. Shaw
Inspector General
Office of the Inspector General
P.O. Box 348780
Sacramento, CA 95834-8780

Dear Mr. Shaw:

This letter is being submitted in response to the Office of Inspector General's (OIG) report titled ***Special Review: California Department of Corrections and Rehabilitation's Office of Internal Affairs Information Security,*** dated April 2009. In this special review, you identified three issues related to the Office of Internal Affair's (OIA) security measures to protect personal, confidential, and sensitive data from unauthorized access or use, and the inadequate control of our computer laptop inventory. We agree with your conclusions and recognize the immediate need to address the deficiencies.

Specifically, in your report you identified unencrypted, confidential information on OIA laptops, which is a violation of State rules. Given the confidential work in which OIA is engaged, we are taking this opportunity to update and secure our data systems accordingly and encrypt all laptops in use by OIA. You also report that several e-mails containing confidential information had been sent across insecure networks. While the State Administrative Manual does not specifically prohibit the sending of confidential material via the internet, we are aware that personal, sensitive or confidential information must be protected. Specific direction has been provided to all staff, reiterating the need to secure confidential data as required by policy. Finally, your report discovered that the OIA laptop inventory was not accurate and up-to-date. To mitigate the risk of both property and data loss, OIA has reconciled the inventory to ensure each laptop has correct property tags and the inventory listing is updated appropriately.

All deficiencies identified are being immediately addressed and will be reported to California Department of Corrections and Rehabilitation's Office of Audits and Compliance in a corrective action plan for monitoring and follow up. We would like to thank the OIG for allowing us the opportunity to provide comment on the deficiencies identified in your preliminary report. We appreciate your continued professionalism and guidance in our efforts to improve our operations. If you should have any questions or concerns, please call my office at (916) 323-6001.

Sincerely,

LEE E. SEALE
Deputy Chief of Staff