CITY OF PALO ALTO OFFICE OF THE CITY AUDITOR

March 26, 2012

The Honorable City Council
Palo Alto, California

Special Advisory Memorandum – Security Vulnerability in the City's SAP Enterprise Resource Planning System

This is an informational report and no action is required.

The Office of the City Auditor has prepared the attached Special Advisory Memorandum (SAM) for your review and consideration. For the development of this SAM, we worked closely with the Administrative Services Department, the City Attorney's Office, the Information Technology Department, and the City Manager's Office. Their input is reflected in this document.

The purpose of this SAM is to inform the City Council of the results of a review our office conducted to address an information security vulnerability we initially discussed in an email sent to the City Council on October 26, 2011. Specifically, we address:

- A significant SAP security vulnerability that allowed certain individuals with SAP access to view employee personal information they did not have a business need to know.
- Actions taken by the Administrative Services Department (ASD), the Information Technology Department (ITD), and the Office of the City Auditor (OCA) to address the security concerns.
- Recommendations to further improve SAP security.

I would like to thank the above mentioned departments for their time, consideration, and cooperation in the development of this SAM. Should you have any questions, please contact my office at your convenience.

Respectfully Submitted,

Jim Pelletier
City Auditor

ATTACHMENTS:

- Attachment A: Special Advisory Memorandum - Security Vulnerability in the City's SAP Enterprise Resource Planning System(PDF)

Department Head: Jim Pelletier, City Auditor

Office of the City Auditor
SPECIAL ADVISORY MEMORANDUM

Security Vulnerability Exposes Employee Personal Data in the City's SAP Enterprise Resource Planning System

The Honorable City Council
Palo Alto, California

The purpose of this special advisory memo is to inform the City Council of the results of a review our office conducted to address an information system security vulnerability we initially discussed in an email sent to the City Council on October 26, 2011. Specifically, this memo discusses:

- A significant SAP security vulnerability that allowed certain individuals with SAP access to view employee personal information they did not have a business need to know.
- Actions taken by the Administrative Services Department (ASD), the Information Technology Department (ITD), and the Office of the City Auditor (OCA) to address the security concerns.
- Recommendations to improve SAP security.

BACKGROUND & SCOPE

In October 2011, the OCA issued the SAP Security Audit, which discussed significant security vulnerabilities in the City's SAP Enterprise Resource Planning system (SAP) and recommended additional measures to effectively secure SAP. After completion of the audit, a City employee informed our office of concerns that some City staff may have access in SAP to employee personal information, such as employee names, birth dates, and social security numbers.

About SAM's

The Office of the City Auditor issues Special Advisory Memos (SAM's) to provide important information to the City Council and City Management in a quick and flexible manner. SAM's are prepared in coordination with relevant City Departments and are utilized for timely communication of limited reviews or evaluations.

City Auditor
Jim Pelletier, CIA

Senior Performance Auditor
Houman Boussina

As of January 25, 2011, an SAP system report listed a total of 1,503 SAP user accounts, including approximately 1,400 employee users. Staff reported that as of November 3, 2011, the SAP system contained records for 3,261 employees, including non-active (former) employees.

Under state law, the combination of name and social security number is "personal information." Agencies must notify individuals if their personal information is acquired by an unauthorized person in a way that amounts to a security breach under the law. Based on representations made by City staff, the City Attorney's Office determined there has not been a security breach under state law.

We notified the City Manager's Office, ASD, and City Council of the security concerns, and have concluded a limited scope review to determine:

- The extent of the security vulnerability and its cause.
- If staff has secured SAP to protect employee personal information.
- If the City has a legal responsibility to notify individuals of the security vulnerability and exposure of personal information.

This was a limited scope review not conducted in accordance with generally accepted government auditing standards; the information presented in this memo is based on staff representations that were not independently validated. The information provided in this memo supplements the SAP Security Audit, and provides additional recommendations that are based on industry standards for ensuring the security of information systems.

RESULTS

Staff reported that an unplanned change in the configuration of an SAP search function gave nearly 300 users of the City's SAP system, who were designated as "time keepers" and/or "time card

CITY OF PALO ALTO

Office of the City Auditor
SPECIAL ADVISORY MEMORANDUM

approvers," access to personal information of current and former employees in their departments if the search function was used. There is no business need to provide users access to this personal information, which includes social security numbers and birth dates, through the search function. Staff stated time keepers and time card approvers are employees designated by department heads or management to approve time records, including designation of time off.

We informed ASD of the security vulnerability on October 7, 2011, and in response to our request for further details, staff provided the following information:

- By default, the SAP system provides time keepers and time card approvers with access to employee personal information through a standard "search help" function that helps users find relevant data in SAP. If the search help function is not restricted by the organization running SAP, users designated as time keepers and time card approvers can display a list of all possible input values for a screen field, including birth dates and social security numbers.
- During the initial implementation of SAP in the City in 2003, SAP was configured to prevent access to employee personal information through the search help function; however, the configuration was reset during implementation of an SAP support pack on December 9, 2008, allowing time keepers and time card approvers to access, through the search help function, birth dates and social security numbers of current and former employees within their department.
- As of October 7, 2011, there were 299 SAP users who were designated as either time keepers or time card approvers. Staff confirmed access was limited to personal information for current and former staff in each time keeper or time card approver's department. As of November 3, 2011, the SAP system contained records for 3,261 employees, including non-active (former) employees. ASD staff informed us that many of the 299 SAP users classified as time keepers and time card approvers had access to personal employee information through other means in following established business processes that are currently under review.

From December 9, 2008 through October 7, 2011, the City's SAP system allowed time keepers and time card approvers access through the SAP search help function to the following personal information of current and former employees in their departments:

- First and Last Name
- Birth date
- Social Security Number

Staff is not aware of any instance or allegation of misuse of any employee personal information.

Staff does not have information regarding whether or how often employee personal information was accessed by time keepers or time card approvers, and is not aware of any instances or allegations of misuse of any employee personal information. We did not conduct additional audit procedures as part of this limited scope review to determine if employee personal information was accessed or misused.

ACTION TAKEN

Staff reports steps have been taken to address the immediate security concerns. Staff secured access to employee personal information through the SAP search help function on October 7, 2011, and subsequently took additional measures to secure SAP. We conducted limited testing and verified staff appears to have secured access to employee personal information through the SAP search help function.

The City Attorney's Office determined that notification requirements do not apply. We met with the City Attorney's Office to discuss the SAP security vulnerability and requested the City Attorney's Office provide guidance regarding any notification requirements under California law. Based on information gathered from staff, the City Attorney's

CITY OF PALO ALTO

Office of the City Auditor
SPECIAL ADVISORY MEMORANDUM

Office determined that there has not been a security breach under state law and therefore state law reporting requirements do not apply.

ASD has improved its incident response process. Although the security vulnerability discussed in this memorandum raises concerns regarding the overall security of the City's information systems and the City's ability to timely detect vulnerabilities, ASD demonstrated improvement in its ability to take corrective action subsequent to notification by our office. ASD staff provided a written report of their response to the security vulnerability and our inquiries. The ASD report demonstrates staff formally documented the security vulnerability and took appropriate remedial action including:

- Identifying key aspects of the vulnerability, including the cause and duration.
- Documenting corrective action taken and preventive measures implemented.
- Apprising management and the City's CFO of the security concerns.
- Documenting the CFO's sign-off on the incident report.

NEXT STEPS

ASD and ITD staff reports that efforts are well underway for improving information security in the City. ASD staff stated that policies and procedures will be developed to safeguard employee personal information, and that as part of the IT Strategic Plan, the new Chief Information Officer will undertake a comprehensive security evaluation for all information systems in addition to assessing resource requirements.

Staff also reports steps have been added to the checklist used to test SAP subsequent to updates, to include review of the SAP search help function.

Additional measures should be implemented to secure the City's information systems. ASD staff reported the City has not formally defined or cataloged all sensitive information in the City's information systems. ASD staff stated guidance has been requested from the OCA in this area. We have provided staff with guidelines on information system security and will follow up in future audits to assess security.

We recommend the ITD, in coordination with City management and the City Attorney's Office, develop and implement policies and procedures to identify and address security of personal information in all of the City's information systems, including any legacy information systems.

We also presented this information to the City's Chief Information Officer (CIO) for his consideration. The CIO stated that in recognition of the need to make information security a top priority, the City, upon his recommendation, is submitting a request for a full-time Information Security Manager. The CIO stated that the manager, who will report to the CIO, will be an experienced and skilled security professional who will quickly assess the City's security needs, prioritize them, and then provide leadership in implementation.

The CIO also reported ITD will be designing and implementing a more rigorous change management process in order to minimize the likelihood of similar issues in the future and that staff is now fully utilizing a tool called the SAP Security Optimizer. This tool is assisting with pre-empting issues by identifying security risks in SAP and making recommendations to remediate.

Respectfully submitted,

Jim Pelletier
City Auditor

cc: James Keene, City Manager
Molly Stump, City Attorney
Lalo Perez, Director of Administrative Services
Jonathan Reichental, Chief Information Officer