EXECUTIVE OFFICE OF THE BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES

VIOLET VARONA-LUKENS
Executive Officer

May 31, 2005

To: Supervisor Gloria Molina, Chair
Supervisor Yvonne B. Burke
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: Violet Varona-Lukens vvl
Executive Officer

SUBJECT: RESPONSE TO REVIEW AND ASSESSMENT OF THE BOARD OF SUPERVISORS' INFORMATION TECHNOLOGY NETWORK SYSTEMS

On October 19, 2004, on motion of Supervisor Knabe, the Board instructed the Auditor-Controller to contract with an independent consultant to review the Board of Supervisors' computer and network systems, and report back to the Board with a corrective action plan to ensure the stability and high reliability of the Board's information technology (IT) system.

On May 13, 2005, the Auditor-Controller transmitted to the Board the consultant's (VeriSign, Inc.) final report, *Business Continuity and Security Assessment*, which contained their findings and recommendations concerning the Board's information technology (IT) system. Overall, the Executive Office's Information Resource Management (IRM) IT infrastructure is technically appropriate and consistent with the requirements and critical business processes identified to meet the needs of the Board offices. Since April 2004, IRM has made many changes that resulted in dramatic improvements in the stability and availability of the Board's IT environment. However, VeriSign, Inc. identified nine critical findings and recommendations to further improve the security and reliability of the Board's IT system. In addition, VeriSign, Inc. provided detailed recommendations to solve each of these critical findings.

Attached is our response to each of the nine critical findings and recommendations. We support VeriSign, Inc.'s recommended solutions to improve service reliability, performance and management oversight of the Board's IT infrastructure, and have already implemented several of the recommendations.

As identified in the attached chart, several of the critical findings require the purchase of equipment and software, as well as IRM staff augmentation, to implement the recommendations. While we have estimated the costs of implementing these recommendations, they are not included in the Department's 2005-06 Proposed Budget. Therefore, under separate cover, we will be submitting to the Board a request to fund 2005-06 unmet needs for consideration during the Board's budget deliberations for the adoption of the 2005-06 County budget.

We would like to express our appreciation to the Auditor-Controller, his staff and VeriSign, Inc. for their assistance in identifying improvements to the Department's IT system. Please call me if you have any questions, or your staff may contact Charlene Abe, Chief Deputy Executive Officer at (213) 974-1410 or Gary Sysock, Deputy Executive Officer at (213) 974-1646.

VVL
CHA:ca

Attachment

c: Chief Administrative Office
Auditor-Controller
Internal Services Department

verisign audit memo

BOARD OF SUPERVISORS BUSINESS CONTINUITY AND SECURITY ASSESSMENT
CRITICAL FINDINGS AND RECOMMENDATIONS

FINDING/RECOMMENDATION	ESTIMATED COST	ESTIMATED IMPLEMENTATION DATE	COMMENTS
1. **Finding:** There are four, single points of failure still existing in the Boards IT infrastructure. These points of failure support external email, internal disk storage, Blackberry wireless email and network fax service, which in turn supports many other critical business processes. IRM is preparing to correct these vulnerabilities sometime in the second quarter of 2005. These changes will provide the redundancy and resiliency needed to ensure that all upstream processes will be unaffected in the event of a system failure in any of these four areas. **Recommendation:** Provide emphasis and funding to ensure the implementation of mechanisms to eliminate these four single points of failure in the second quarter of 2005. If this recommendation is not implemented, a higher risk of service interruption is likely in the event that any of these systems fail.	One time $248,000 Annual $120,000	External email June 2005 Blackberry wireless email September 2005 Network fax service September 2005 Internal disk storage December 2005	Concur with recommendation; in process of being implemented. ***External email:*** A separate Exchange server will be reconfigured as a second SMTP Gateway for external email, and provide backup for the primary server. ***Blackberry wireless email:*** The Blackberry Enterprise Server software will be installed on a second server to provide backup for the primary server. Both servers will be configured with mirrored disk drives and dual power supplies to prevent common problems from affecting the system. ***Network fax service:*** Currently this service is in limited production, a secondary server will be configured for backup during a severe outage. Both servers will be configured with mirrored disk drives, dual power supplies, and dual interface boards and Telco lines. ***Internal disk storage:*** A second disk storage unit will be used to duplicate data on the existing SAN and will be the base for the department's business recovery site.

FINDING/RECOMMENDATION	ESTIMATED COST	ESTIMATED IMPLEMENTATION DATE	COMMENTS
2. **Finding:** The communications/data network deployed by the Internal Services Department (ISD) in support of the Board is **not** managed or maintained by IRM. The network and its infrastructure, which provides connectivity to the Hall of Administration (HOA) Board offices, the Board field offices and Internet access, are managed exclusively by ISD, with no oversight by IRM. **Recommendation:** Provide funding and staff augmentation authority to acquire staff skills and head count to implement a monitoring and oversight program of ISD-provided Board network services. Even though ISD does not currently provide Service Level Agreements with its internal customers, VeriSign recommends that IRM negotiate a Service level Agreement with ISD and use IRM staff to monitor ISD's compliance with it. If this recommendation is not implemented, IRM will be unable to ensure Board network needs are communicated effectively or are consistently met by ISD, as well as lengthen IRM problem resolution times in the event of a network-based problem.	One time $100,000 Annual $0	To be determined	Concur with recommendation. The Executive Office is evaluating various tools that will assist in monitoring the ISD-provided network services for the Board. The Executive Office will meet with ISD to discuss implementation of Service Level Agreements.
3. **Finding:** The Board, and rightly so, has very high expectations for the level of service provided by IRM. While IRM works very hard to meet this demand, it has insufficient staffing levels, a lack of some skills and the need for additional support tools to meet the Board's support expectations. **Recommendation:** Provide funding and staff augmentation authority to implement the recommended staffing plan. While the existing IRM staff is capable and competent, critical skill sets such as network engineering, information security, Business Continuity, Disaster Recovery, network and application monitoring are not present in existing skill sets and if present could not be supported at current staffing levels. These staff shortcomings make it very difficult to provide effective oversight of ISD's stewardship of the Board's network services, timely and consistent help desk and user support, network and application monitoring and still maintain the security and confidentiality of the Board's electronic data and communications.	One time $90,000 Annual $528,000	To be determined; pending discussions with CAO and DHR	Concur with recommended organizational staffing plan. The Executive Office will work with the Chief Administrative Office (CAO) and the Department of Human Resources (DHR) to implement this recommendation.

FINDING/RECOMMENDATION	ESTIMATED COST	ESTIMATED IMPLEMENTATION DATE	COMMENTS
4. **Finding:** Board communications and IT assets are at risk for compromise (eavesdropping and or modification) and unauthorized access. The Board servers and desktop systems are exposed to access from anywhere in the LA County network. This presents a considerable risk to the Board's operations through shared and/or cascading risk. Cascading risk is defined as when one party knowingly or unknowingly incurs additional risk due to the acceptance of risk or the failure to control risk of another party. The Board shares or incurs the risk knowing or unknowingly accepted by other County departments. This is the result of ISD adopting an "any-to-any" model within the county network, similar to what a telephone company provides, without advising client County departments that their internal security, *vis-à-vis* the rest of the County, is an individual department responsibility. For the Board and other County departments, this creates a threat environment that is broader and more difficult to manage and directly threatens the confidentially, integrity and availability of Board critical business processes. **Recommendation:** Provide funding and authority needed to coordinate with ISD to initiate a design/build program to implement additional security infrastructure for the Board. This architectural concept is designed to provide for the confidentially and integrity of Board communications and assets in transit and at rest. If this recommendation is not implemented, it will leave Board communications and IT assets exposed to potential compromise and/or unauthorized access from within and from outside the County network, of which the Board IT assets are a part.	One time $120,000 Annual Included in Recommen-dation No. 1	To be determined; pending discussions with ISD	Concur with recommendation. The Executive Office will work with ISD to design and build a more secure network architecture within the County's enterprise network. Immediate steps have been taken to implement a firewall in the department's computer room.
5. **Finding:** VeriSign has identified high risk vulnerabilities during its automated and manual scan of Board IT assets. **Recommendation:** Provide funding and authority needed by IRM to correct the existing high risk vulnerabilities as defined in VeriSign's report. If this recommendation is not implemented, it will leave the IT assets vulnerable to compromise, unauthorized access and increased risk of interruption of service.	One time Included in Recommen-dation Nos. 1 and 4 Annual Included in Recommen-dation No. 1	To be determined	Many of the vulnerabilities mentioned in the security audit were related to servers that were in the process of being removed from the system. These servers have been replaced with new servers. The Executive Office will evaluate the effect of implementing the recommended changes, as some of the recommendations may affect the day-to-day IT operations.

FINDING/RECOMMENDATION	ESTIMATED COST	ESTIMATED IMPLEMENTATION DATE	COMMENTS
6. **Finding:** A Microsoft Windows provided password protection system called SYSKEY is not being used, making it possible to attack and potentially crack both user and Administrator passwords. **Recommendation:** Implement the password protection scheme called SYSKEY. Failure to implement this Microsoft provided password protection scheme will leave Board passwords vulnerable to compromise, potentially leading to system wide compromise. If this recommendation is not implemented, Board passwords will remain vulnerable to interception and compromise leaving Board IT assets subject to unauthorized access and compromise.	One time $0 Annual $0	Implemented	Concur with recommendation. SYSKEY passwords have been installed on all the department's servers.
7. **Finding:** The vulnerability assessment results indicate that IRM managed servers should have the benefit of improved security configuration settings. **Recommendation:** Implement the security recommendations found in VeriSign's report. If this recommendation is not implemented, it will leave the Board servers vulnerable to an attack that may interrupt service and/or compromise the servers.	One time $0 Annual $0	September 2005	Many of the security issues were related to servers that were in the process of being removed from the system. These servers have been replaced with new servers. The Executive Office will work with the vendor that supports the new servers to review their security associated with the servers, and evaluate the effect of implementing the remaining recommended changes.
8. **Finding:** The IPTV server and its support systems are used to broadcast the Board's weekly meetings for viewing within the County. Due to its age and unpatched condition, these IT assets represent the highest level of risk in the overall Board network security profile with 6% of the total high risk vulnerabilities. **Recommendation:** Remove or upgrade these servers as soon as possible. If the IPTV server and associated systems are not replaced, the Board's weekly meeting broadcasts are subject to interruption as well as putting the rest of the network at risk.	One time Unknown; to be determined Annual Unknown; to be determined	To be determined; pending completion of testing new system	The support systems used to broadcast the Board's weekly meetings is being reviewed and upgraded by the ISD and Chief Information Office (CIO). The current IP server supports the building's multicast board meeting broadcast. Upon ISD's and CIO's completion of testing the new equipment and system, the new server will replace the existing server.

FINDING/RECOMMENDATION	ESTIMATED COST	ESTIMATED IMPLEMENTATION DATE	COMMENTS
9. **Finding:** IRM system administrators are using their personal user accounts to perform Administrative functions. Since the Administrators personal access credentials are used more widely, it increases the potential of domain-wide compromise if an Administrator's personal UserID/Password combination is compromised. It can also result in the administrator inadvertently executing a function or procedure under their personal user account (thinking that it will only apply locally) that could adversely affect the entire domain. **Recommendation:** VeriSign advises IRM system administrative personnel to remove their personal accounts from any but their local domain group. Then issue a unique domain administrative account name and password (different from their personal accounts) for each administrator. If this recommendation is not implemented Board systems may be subject to unintentional service interruptions and compromise.	One time $0 Annual $0	Implemented	Concur with the recommendation. All passwords have been changed.
TOTAL	**One Time** **$558,000** **Annual** **$648,000** **Total** **$1,206,000**		

verisign audit (05/31/05)