MARK J. WALSH
DIRECTOR

2615 PAULIN DRIVE
SANTA ROSA, CALIFORNIA
95403-2871
707.565.2911
FAX 707.565.3009

County of Sonoma

INFORMATION SYSTEMS

KEN HIGHTOWER
SYSTEMS & PROGRAMMING
JON PHILLIPS
TECHNICAL SERVICES
JOE GALVAN
WORKGROUP SUPPORT
CHRIS ANDEREGG
ADMINISTRATION

July 28, 2005

The Honorable Robert Boyd, Presiding Judge
Sonoma County Superior Court
600 Administration Drive
Santa Rosa, CA 95403

RE: Information Systems Response to 2004-2005 Sonoma County Grand Jury Report

Dear Honorable Judge Hardcastle:

We are in receipt of the report titled "Protecting the County's Assets," and respectfully submit the following response for the Information Systems Department. The letters and numbers make reference to the report. Italic formatting is used to indicate a direct quote from the report.

F1 (page 59): *ISD has an arrangement with a supplier with offices in San Mateo, whereby tape copies of major files are taken each day and stored at the supplier's location. This arrangement does not include files from the school data processing system, for which ISD only provides facilities management.*

RESPONSE: The respondent disagrees partially with the finding.

ISD uses a third party tape vaulting service to store backup tapes of all of the systems that County ISD has responsibility for. Backup tapes for the Sonoma County Office of Education (SCOE) are included in the ISD tape library for tracking purposes and are stored offsite under a separate contract that SCOE manages.

F2 (page 59): *Files for the schools' data processing system are backed up daily and stored at Sonoma County Office of Education.*

RESPONSE: The respondent agrees with the finding.

F3 (page 59): *The ISD network is well designed with very little "hardwiring." Thus, it is close to providing facilities whereby "anyone, with the right authority, and the right equipment, can get to any application or service." This flexibility should bode well in the disaster planning.*

RESPONSE: The respondent agrees with the finding.

F4 (page 59): *ISD is presently developing a plan to identify the critical points of failure in the data center and the county network, especially those points of failure that have no redundancy. Since this plan is in its early stages, the grand jury expects that any recommendations made in this report can be folded into the emerging plan*.

RESPONSE: The respondent disagrees partially with the finding.

The Information Systems Department is developing a plan for the continued delivery of technology services during a disaster. However, the plan initially focuses on reporting relationships and the conduct of a disaster needs assessment, rather than on identifying critical points of failure in the data center. In some instances, the technology team will "work around" the data center, rather than try to restore it.

The lack of redundancy in one type of technology is not necessarily a problem, as long as another communications method delivers the same result. Duplicating all technologies to prepare for unknown events is not efficient, and may not work.

During a disaster, the County's focus is on protection of its citizenry, and the focus of the technology becomes public safety response. The plan begins with a focus on reporting relationships, much like the SEMS structure requires. For technology issues, a team of radio, telephone, and network engineers report to the Division Director of Technical Services. They will perform an assessment, based on agreed upon priorities, and restore the most essential services.

F5 (page 59): *The recovery test that the jury participated in (as observers) was straightforward and the minimal numbers of users involved were able to log on to the "recovered" system. However, the validity of the test was somewhat undermined by using the incorrect tapes! The test facilitator was able to declare the test successful by taking account of the modified steps needed to utilize the recovered data.*

RESPONSE: The respondent disagrees partially with the finding.

The purpose of a remote disaster recovery exercise is to test several aspects of the disaster recovery process which includes: Testing the quality of recovery documentation, including the procedures to restore the system; testing the integrity of the backup tapes that are available at the remote location at the time of the declared disaster; testing the integrity of the systems being recovered through end user participation.

There is always uncertainty when a disaster strikes. Because all of the goals of this last exercise have been accomplished, we disagree with the finding that having an incorrect data set of some of our system tapes undermined the validity of the recovery exercise.

F6 (page 59): *ISD tried the conventional approach of attempting to get its major users to reach consensus on which applications would take priority in the event of a major and prolonged outage of the computer systems. Like many other ISD departments, they found the responses lackluster at bust.*

RESPONSE: The respondent disagrees partially with the finding.

In the process of revising the ISD Disaster Recovery Plan for the County, ISD sent out a questionnaire to all of the County departments seeking input on what each of the departments plans were in the event of a disaster, including input on the priority of system recovery. Some of the County departments did not respond to the questionnaire.

ISD is proceeding with its revision of the Countywide ISD Disaster Recovery Plan. ISD is working with General Services to insure that each of these plans is dovetailed in order to take into account facilities issues. Once the new plan becomes available, it will be sent out again to all of the County departments to solicit input.

F7 (page 60): *ISD is run on a full cost recovery basis, i.e., its expenditures are funded by charging user departments for their share of the computer usage, an equitable scheme. However there is no place in the cost recovery system to separately fund any unique expenditure for disaster recovery plans.*

RESPONSE: The respondent disagrees with the finding.

The technical infrastructure necessary for Disaster Recovery is a baseline expense that every County Department benefits from. ISD currently fully recovers the cost of Disaster Recovery in the same manner that it recovers all other baseline expenditures.

F8 (page 60): *Most of the computer applications used by the Tax Collection Department are developed by and purchased from a third party provider and are server-based. Sonoma County uses the same applications as Napa County and other counties within a reasonable distance. There is a valid assumption that in the event of a total system loss, the Tax Collection systems could be processed elsewhere, likely at the Napa County facility. The arrangement is reciprocal. It is not clear whether the Tax Collection Department would literally use the copy of the application that resides in Napa. It may be safer to make a copy of the application code in use in Sonoma County, and take it to Napa County when needed.*

RESPONSE: The respondent disagrees partially with the finding.

The tax collection application is developed and purchased by a third party vendor, and is used by other California counties. The counties do help each other in event of a disaster. Whether and to what extent Napa County would be in a position to help may depend on their situation status. The County is continuing discussions with the vendor to determine the safest method for restoring the application.

During a declared disaster, personnel in both the Information Systems and the Tax Collection departments report to the Incident Commander in the Emergency Operations Center, and carry out assigned duties. It is not likely that a needs assessment conducted during a major disaster would focus on restoring the tax collection activities. However, as personnel are not needed to restore the highest priority services, and become available, the Information Systems Department and customers will work to restore day-to-day business applications, such as the tax collection system.

F23 (page 61): *As well as the Dispatch Center, the Sheriff's Department has other technology bases that are critical to its operation (or will increasingly be so). The "A Disaster Waiting to Happen" report noted that the current radio network design had a good level of redundancy and more was in the planning stage. The report also noted that the Sonoma County Law Enforcement Consortium (SCLEC) was housed on a single computer system that was a single point of failure, and a plan is needed to reduce that exposure.*

RESPONSE: The respondent disagrees partially with the finding.

The first finding about the current radio network design is correct, and describes a desirable characteristic of an efficient public safety radio system. Additionally, upon impairment of part of the radio system, it is possible to broadcast radio signals directly from individual radio sites.

The second finding is incorrect. The Sonoma County Law Enforcement Consortium computer system design has been built using redundant computer servers for each of its core applications. If a system failure occurs at any given time, there is a backup server in operation that will, in most cases, automatically switch to primary and begin performing transactions without service interruption occurring.

R1 (page 63):*Complete its initial disaster recovery plan by December 2005, and request the funding it calls for in time for the 2006-2007 budget cycle. This request should include a change in the manner by which such expenditures are funded, separately from recovery of ongoing ISD running costs.*

RESPONSE: The recommendation has not yet been implemented, but will be implemented in the future.

The Information Systems Department will complete the disaster recovery plan by December 2005. Whether and to what extent the plan will require new funding will be known at that time. Financial recommendations will be based on the magnitude of potential system disruption, the probability of the disruption actually occurring, and the required expenditure to insure the disruption does not happen. Identifying every possible "single point of failure" and building a redundant system for it is not an efficient use of funds. The manner in which costs are allocated follow State and Federal rules, and is not a significant factor with respect to disaster recovery.

R2 (page 63): *Involve the major users more closely in the design of the new disaster recovery plan. This may need senior management directives to the major users.*

RESPONSE: The recommendation has been partially implemented.

The Information Systems Department will continue to involve customer departments in the prioritization of systems with respect to disaster recovery. The department will also coordinate with others in the preparation of the plan, especially the Emergency Services Department.

R3 (page 63): *Ensure that the new disaster plan under development includes specific recommendations on:*

- *The need for user consensus on the system and application priorities, both for protection against failure and sequence of recovery in the event that not all facilities can be restored immediately after a catastrophic outage.*

RESPONSE: The recommendation will be implemented in the future.

The Information Systems Department works with customers in prioritizing systems, and will incorporate those priorities into the plan. Sequence of recovery will be a part of that process. The overall situation assessment, as conducted at the EOC, or other facility, will be a factor in the prioritization, and the Incident Commander may change priorities per SEMS.

- *The value of distributing some of the servers (presently clustered) and the use of storage area networks – a "let's not put all of our eggs in one basket" strategy.*

RESPONSE: The recommendation requires further analysis.

The value of "clustered" servers and secondary locations is acknowledged, and the benefits will be weighed against costs.

- *A "non-stop" solution for the Sonoma County Law Enforcement Consortium (SCLEC) system such that an outage of the main system is instantly switched to a standby, such standby preferably located at a site some distance from the primary location. There are numerous hardware, network, and software solutions available to achieve this.*

RESPONSE: The recommendation has been partially implemented, the remainder of which will require further analysis.

The current system design includes a failover redundant server approach. If any of the primary application servers were to fail, a backup system is in place to provide immediate failover.

A "non-stop" solution can be made, if a re-architecture of the entire system were to occur at a significant expense and if permission is granted from the State of California to install a second data-line connection to the designated new remote data center location. In addition to a second secure connection with the State of California, this solution would also require new connections between each agency and our designated remote data center location, as well as a real time transfer of information between each of these data center locations. There are many different network designs that could be deployed, but there are not "many" solutions for this that is financially feasible. The Department will evaluate remote site backup solutions and related costs with the consortium partners as part of the SCLEC program planning process that occurs annually.

- *Identify every single point of failure in the data center, including network terminators and cabling ducts, and determine the investment value of providing redundancy.*

RESPONSE: The recommendation has been partially implemented.

As part of the process to revise our existing Disaster Recovery Plan, evaluation of our current systems, including the identification of critical systems and their relevant single points of failure will be included. We currently adhere to the use of a best practices approach for all of our system designs, including the use of system and component level redundancy within our technology acquisitions.

Identification of every single point of failure in the data center, including network terminators and cabling ducts in order to determine the investment value of providing complete redundancy will not be implemented because it is not warranted for all systems that currently reside in the data center. The identification phase of every possible "single point of failure" would require a significant opportunity cost and would not be an efficient use of funds or provide meaningful benefit.

My staff and I appreciate the opportunity to respond to these findings and recommendations. Please call me or Jon Phillips if there is any other information we can provide.

Sincerely,

Mark J. Walsh
Director

cc: Judge Allan Hardcastle
Board of Supervisors
Court Executive Officer
County Clerk