Perris Union High School District

Management Review

July 18, 2007

Joel D. Montero
Chief Executive Officer

FCMAT
FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM
CSIS California School Information Services

July 18, 2007

Jonathan L. Greenberg, Ed. D., Superintendent
Perris Union High School District
155 East Fourth Street
Perris, CA 92570

Dear Superintendent Greenberg:

In December 2006, the Perris Union High School District contacted the Fiscal Crisis and Management Assistance Team (FCMAT) to request a management review. The subsequent study agreement specified that FCMAT would perform the following:

1. Conduct a review of the district's administrative and instructional systems, applications, processes, infrastructure and emerging technologies and make recommendations for improvement.

2. Conduct a review of the district's technology organizational structure and staffing allocations and make recommendations for improvement.

3. Conduct a security and configuration review of the district's network resources and make recommendations for improvement.

A FCMAT study team visited the district on June 1-2, 2007 to conduct interviews, review data and collect information. This report is the result. of that effort.

We appreciate the opportunity to serve you, and we extend our thanks to all the staff of the Perris Union High School District.

Sincerely,

Joel D. Montero
Chief Executive Officer

Table of Contents

Foreword

FCMAT Background

The Fiscal Crisis and Management Assistance Team (FCMAT) was created by legislation in accordance with Assembly Bill 1200 in 1992 as a service to assist local educational agencies in complying with fiscal accountability standards.

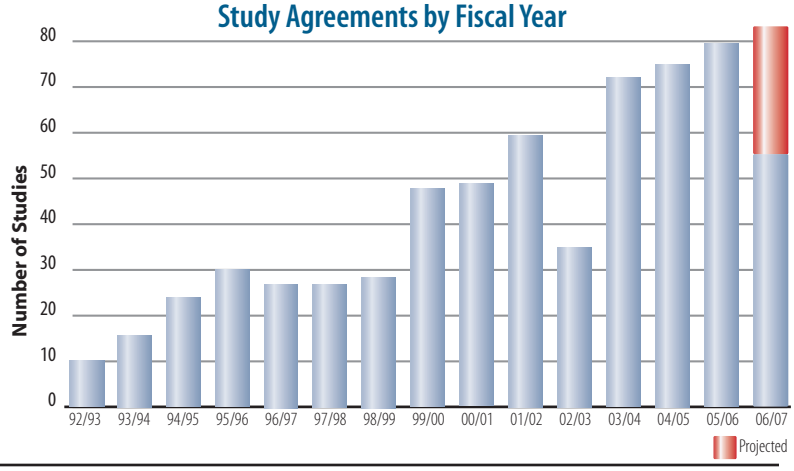
AB 1200 was established from a need to ensure that local educational agencies throughout California were adequately prepared to meet and sustain their financial obligations. AB 1200 is also a statewide plan for county offices of education and school districts to work together on a local level to improve fiscal procedures and accountability standards. The legislation expanded the role of the county office in monitoring school districts under certain fiscal constraints to ensure these districts could meet their financial commitments on a multiyear basis. AB 2756 provides specific responsibilities to FCMAT with regard to districts that have received emergency state loans. These include comprehensive assessments in five major operational areas and periodic reports that identify the district's progress on the improvement plans

Since 1992, FCMAT has been engaged to perform more than 600 reviews for local educational agencies, including school districts, county offices of education, charter schools and community colleges. Services range from fiscal crisis intervention to management review and assistance. FCMAT also provides professional development training. The Kern County Superintendent of Schools is the administrative agent for FCMAT. The agency is guided under the leadership of Joel D. Montero, Chief Executive Officer, with funding derived through appropriations in the state budget and a modest fee schedule for charges to requesting agencies.

Total Number of Studies..... 637
Total Number of Districts in CA..... 982

- Management Assistance..... 603 (94.66%)
- Fiscal Crisis/Emergency 34 (5.34%)

Note: Some districts had multiple studies.
Districts (7) that have received emergency loans from the state.
(Rev. 4/3/07)



Introduction

Background

Located in Riverside County south of San Bernardino, the Perris Union High School District serves approximately 9,000 secondary and middle school students who live in Perris Valley. The district encompasses approximately 184 square miles and has more than 500 employees.

With more than 1,500 computers in its schools, the district's investment in technology is extensive. One of the district's charter schools functions completely online, and the other is a military academy.

In January 2007, the district entered into an agreement with the Fiscal Crisis and Management Assistance Team (FCMAT) for a management study to perform the following:

1. Conduct a review of the district's administrative and instructional systems, applications, processes, infrastructure and emerging technologies and make recommendations for improvement.

2. Conduct a review of the district's technology organizational structure and staffing allocations and make recommendations for improvement.

3. Conduct a security and configuration review of the district's network resources and make recommendations for improvement.

Study Team

The study team was composed of the following members:

Andrew Prestage
FCMAT Management Analyst
Bakersfield, CA
School District

Leonel Martínez
FCMAT Public Information Specialist
Bakersfield, CA

Warren Williams*
Director of Special Projects
Grossmont Union High

La Mesa, CA

Bradley L. White
Senior Network Engineer
Arrival Communications
Bakersfield, CA

*As a member of this study team, this consultant was not representing his respective employer but was working solely as an independent contractor for FCMAT.

Study Guidelines

FCMAT visited the district March 1-2, 2007 to interview employees, collect data and review information. This report is the result of that effort and is divided into the following sections:

I. Executive Summary
II. Staffing and Organizational Structure
III. Administrative and Instructional Systems
IV. Network Resources

Executive Summary

The Perris Unified School District is in a good position to create a sustainable technology implementation program that will benefit students and teachers while performing the administrative functions of the district.

Effective strategies and processes are needed to make optimal use of the district's current assets and provide long-term support for the staff and students. The district's Technology Department needs to be reorganized to take advantage of the skills of its current employees. The director needs to be provided with the flexibility to make significant technical changes in current network topology. The district should engage in a collaborative process to establish priorities for projects in production. In addition, a strategic plan must be developed that provides future direction for technology.

The district is at risk in the use of its critical applications. The student information system does not comply with the district's educational plans, and the data it contains is suspect. There is concern that students have been provided access to other students' information via teacher workstations. This practice needs to be discontinued immediately. Business Services has made accommodations to acquire a new, modern student system. This project should begin immediately.

The business and human resources software, Galaxy, is adequate and full-featured. A concerted effort should be made to purge extraneous programs that are used for business and human resources purposes. Galaxy should be used to accomplish these tasks.

Much of the district's educational computer inventory is obsolete. Parts from some computers have been used to repair other computers. This outdated inventory has created the potential for poor inventory control, potential theft and an impression that the student-to-computer ratio is higher than it is. A complete replacement policy would alleviate most of these problems. This should become one of the first priorities for a district technology committee to address.

Findings and Recommendations

Staffing and Organizational Structure

Technology Department Organization

The Director of Technology Services reports to the Assistant Superintendent of Business Services, but is not a cabinet-level position. Communication between technology services and the three district divisions (Human Resources, Business, and Educational Services) is adequate, but improving it would improve department effectiveness.

Many district staff members commented that the district's work order system is ineffective and cumbersome. Some technology support staff members do not routinely check in with site personnel before leaving a campus after a repair is completed. The district lacks an effective system for maintaining hardware inventory information and tracking installation of new equipment.

Job descriptions for computer technicians do not accurately reflect the duties and functions performed by the staff members who fill these positions. Position titles such as Network engineer and Database Administrator are not included in the Technology Department's staffing allocations. Formal certifications are not required for any technology support position. The Technology Department had a vacant position titled Senior Clerk, but that position was recently filled. The department lacks a help desk position to provide timely resolution of user requests for support. In the absence of a formal help desk position, telephone-based user support requests are currently fielded by department technicians who rotate in and out of the position.

The allocation of technology support staff members to sites is not effective. For example, the high school sites do not have an assigned technology staff member. On July 1, 2007, the Technology Department assumed responsibility for supporting the district's telephone systems. The Senior Clerk is handling the additional workload associated with telephone support. Technology department staff members do not regularly seek professional development through attendance at conferences, workshops, and in-service trainings. The department has established informal procedures for repair, replacement, and installation of computer equipment, but because these procedures are not published, users are largely unaware of them. Information on standard hardware for purchasing is posted on the district's Web page. However, some users commented that they are unaware of the existence of published hardware purchasing guidelines.

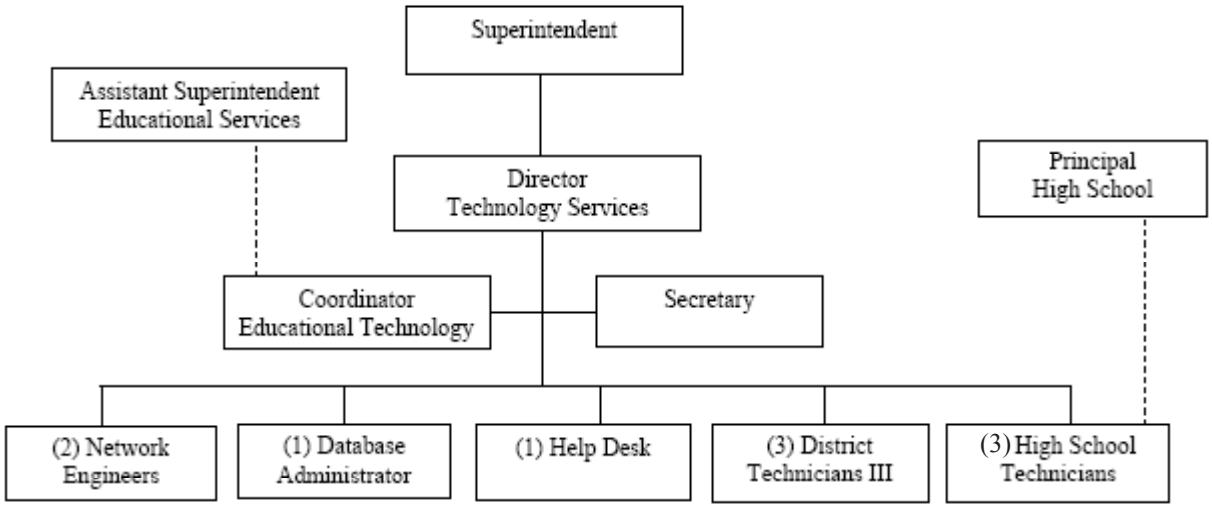
Some district staff members believe that the technology support staff does not understand the importance of good service orientation. Other staff members commented that the technology support staff sometimes starts work on a new project or repair ticket before finishing the last one.

Recommendations

The district should:

1. Assign the Director of Technology to report directly to the Superintendent as shown in the following organizational chart. It is important for the director to have regular access to the cabinet. To maintain a balance of service to the three divisions, Human Resources, Business and Educational Services, the director should meet frequently with each Assistant Superintendent and frequently be included in divisional meetings.

Recommended Technology Department Organizational Chart



2. Consider alternatives to the current work-order system, which is not designed for workflow in a Technology Department. The alternatives to be considered should help the director more effectively communicate with end users, assign staff members and track interventions. End users should be notified when repairs are to occur, and technicians should report to site personnel before leaving a campus or department after a repair is completed. The district should work with the Purchasing Department to establish a better method to inventory and track the installation of new equipment.

3. Consider reclassifying the technicians' job description to recognize the variety of work this position is asked to perform. The current job description does not reflect positions in modern educational technology operations. The Technician III classification should be separated into four separate job descriptions with a level of compensation commensurate with the responsibilities: Network Engineer, Database Administrator, District Technician and Site Technician. A sample organization chart and job descriptions are attached as appendices to this report. Current technicians should be considered for reclassification, if permitted by the district's personnel policies, to these job categories. Each position should have a certification requirement, and current technicians should be provided with a grace period to achieve these certifications.

4. Allocate a technician to each comprehensive high school. These positions should report to the Director of Technology, but have an indirect reporting line to the site administration.

5. Assign the Technology Department staff to participate in regular staff development. Members should be encouraged to attend conferences and workshops to advance their skills.

6. Increase awareness of the Technology Department's existing guidelines for standard hardware purchasing alternatives, operations and technical procedures. End users should be aware that this documentation is available for review on the district's Web site.

7. Encourage the Technology Department to develop a customer service orientation for end-users. An in-service training session with frequent refresher sessions is needed to instill the importance of end-user satisfaction with departmental services. Feedback from site and district personnel should be incorporated into every service call, and biannual surveys should be solicited from all user groups.

8. Complete service calls and repair jobs before a new job is initiated except during emergencies.

Educational Technology Coordinator

No single position in the district has full responsibility for educational technology measures. As a result, instruction and learning do not benefit from an organized approach to technology implementations. Teachers and site administrators cite the need for instructional technology leadership and participation in decision making.

The district lacks a standing a district technology committee. The sites were not involved in the decision on how to disburse funds from the Microsoft settlement. No standard has been established for the minimum technology to be used in every classroom.

Teachers lack sufficient training for new systems, and they were not involved in the decision to make the district a "PC only" district. E-Chalk has not been completely implemented or supported. Network, computer and software changes are frequently arranged with little or no teacher notification or input. Teachers also have little input in establishing technology standards. Many teachers are unable to upgrade computer software because the Technology Department has them "locked down." During interviews, the technology director acknowledged the advantages of allowing site users to have full administrative access to their computers, but explained that this level of access increases the demand for support due to unlicensed software installation, incompatibility among applications, and increased rates of virus infection. There is no linkage between Program Improvement schools and their uses of technology. Many instructional technology decisions are made in the central office with little or no input from Educational Services. Teachers and site administrators frequently purchase instructional software with no input from the Technology Department.

Many classroom computers are not used because they need to be repaired or upgraded. As a result, students are denied the benefit of technology because of computer downtime or lack of appropriate instructional software. Educational technology programs are sometimes unused for months.

The Technology Department filters educational content, and teachers are unable to access appropriate educational Web resources.

The Technology Department also has no planned staff development days or regularly scheduled sessions for educational technology initiatives.

Recommendations

The district should:

1. Establish in the Technology Department a certificated Educational Technology Coordinator position that works closely with the Assistant Superintendent of Educational Services. The Director of Technology will coordinate the workflow of the position with the department's activities. The coordinator's duties should include the following:

- Providing technology support for classroom instruction, staff development, educational software evaluation and implementation, working on CTAP, and library technology and overseeing Internet filtering. This position should collaborate with teachers to establish appropriate Web sites for student and faculty use.

- Functioning as the primary point of contact for schools considering educational software or equipment acquisitions.

- Frequently attending Educational Services meetings.

- Chairing a district technology committee that meets regularly and is composed of selected teachers from each school.

- Representing schools, teachers and students in Technology Department meetings.

Administrative and Instructional Systems

Student Information System

Teachers indicate that there are frequent errors in the Schools Administrative Student Information Software (SASI) attendance reporting, and site administrators report attendance and master schedule problems. Students are reported to be taking attendance and entering grades for some teachers. The lack of adequate security in the system permits teachers to access the database where records can be altered or deleted. Teachers and SASI support personnel also lack sufficient formal training on the use of the system.

SASI lacks the functionality of a modern student information system. District resources may be affected because of system attendance inaccuracies. The system does not comply with an Education Code requirement to inform teachers of dangerous students in their classrooms. Parents are often not informed of boundary changes until they arrive at the wrong school at the beginning of the school year. Demographic software, used in conjunction with an improved student information system, could eliminate this problem. SASI and other district software programs do not share information, causing double entry and the lack of integrated data. The district has a SASI user group, but not all departments are represented or involved.

System data should be thoroughly reviewed to ensure that it accurately reflects the student census and enrollment data before any change is made to any new system. Some site staff members commented that students have occasionally accessed the student information system. This type of access should never be allowed.

The district's acceptable usage policy (AUP) needs to be updated and signed by all district staff members.

District personnel indicated that there are no "job-alike" meetings among personnel with similar job functions to encourage communication regarding system functionality. For example, a bimonthly meeting among all data attendance clerks would promote communication and increase understanding of the student information system.

A teacher on special assignment currently provides student system user support and handles requests for student data from the district's student information system. Four staff members in the Technology Department are certified to provide technical support for the student information system, with an additional staffer dedicated to SIS database support and administration. Despite this, many requests for technical and database support on the SIS have been handled by the teacher on special assignment rather than by appropriately trained technology department staff members.

The district lacks a data warehouse to assist with aggregation of disparate data from sources such as student, financial, and academic performance systems.

Recommendations

The district should:

1. Immediately draft a comprehensive request for proposals (RFP) as the first step in acquiring a new student information system. External assistance should be obtained for a project of this complexity. Precautions should be taken to ensure that no required or desired functionality is missing from the new system. Technical and legal support should accompany implementation. Every affected party should be consulted regarding the acquisition, and each should have significant input on drafting specifications.

2. Take immediate steps to cease the current system's security breaches. Students should never have access to staff computers. Advise all administrators, counselors, and teachers that providing access to the student information by unauthorized personnel or by student assistants is strictly forbidden. Allowing unauthorized personnel to record grades and review student programs, census and custodial information is contrary to district policy. This issue should be covered in a signed AUP that details outcomes for violation. The AUP should be renewed and re-signed each year by all district employees.

3. Perform a comprehensive audit, and correct erroneous or missing student census and enrollment data before a new student system is adopted. Temporary data entry personnel should be used to assist in this operation.

4. Encourage the formation of user groups composed of employees with similar positions. For example, all attendance clerks should meet regularly to receive training and compare best practices. This process will be essential when a new system is adopted.

5. Develop permanent expertise and technology support for the student system. The district should consider eliminating the TOSA support position for SASI and assigning this function to the Technology Department.

6. Consider collecting data from throughout the district in one location. To maintain long-term compatibility among disparate databases, technology support staff should continue to design data collection procedures in a manner that is compatible with the School Interoperability Framework (SIF). As a result, users should eventually be able to access and/or provide reports to all district departments with relative ease.

Educational and Business Systems

Educational and business systems are adopted without a consistent method for ensuring compatibility with existing systems, determining ongoing personnel and financial support requirements, and developing a collaborative implementation process. In many cases, systems are acquired with little or no end-user input.

Many Human Resources functions are handled manually such as determining seniority hours, payroll calculations and leave balances. Valuable teacher and classified employee information is maintained separately from the Galaxy business and human resources system, necessitating double entry of data and increasing the likelihood of error.

Employees in Human Resources and Business Services are not cross-trained in system functions. Credential information is accessible by only one person from one computer. Valuable data maintained on some of these computers is not protected by back ups. Human Resources is compartmentalized, and information is not integrated. The GALAXY system is underutilized to store district information. Site administrators do not have access to real time budget or human resources information.

There are no system controls to ensure that budget overruns do not occur. Staff members in the Business Services and Human Resources divisions are not cross-trained on the functions performed in these two divisions. Attendance accounting procedures may need to be reviewed to ensure that attendance data is reported accurately. During interviews, staff members commented that the pupil custodian warning flag in the student information system has been disabled. This could allow noncustodial parents to gain illegal access to a student.

Recommendations

The district should:

1. Implement only systems that can be supported or maintained with district resources and staff. The district should ensure that any system to be considered includes the resources necessary to accomplish the task. The impact on the current staff and financial resources should be considered. E-Chalk is an example of an exemplary program that is underutilized because of lack of support.

2. Conduct an analysis of the various functions that are being performed separately from the Galaxy business and human resources system to determine if these tasks could be performed online rather than manually. Any identified Galaxy problems should be addressed so that all information processing tasks can be performed online rather than manually. This will help to ensure the integrity of credential, payroll and purchasing information.

3. Discontinue the practice of maintaining separate databases since this can lead to incorrect information being reported to the state, jeopardizing district revenues. The spreadsheets and databases contain data that should be entered into the Galaxy system. Data from adjunct systems for seniority hours, payroll calculations, teacher credential information and leave balances should be entered and reconciled in the Galaxy system, and the use of the external programs should be terminated as soon as possible.

4. Develop a consistent backup process for all critical applications.

5. Provide immediate training for those assigned to system operation and support for end users who frequently don't know how to operate systems. All major systems lack sufficient support. The personnel in charge of these systems also lack sufficient training to maintain them at optimal and secure levels.

6. Immediately implement procedures to ensure that budget overruns do not occur.

7. Provide cross-training for the Business Services and Human Resources divisions so that operations will not be hindered when employees take vacations, retire or take sick leave.

8. Evaluate attendance accounting procedures to ensure that information is reported correctly to the state.

9. Immediately reinstitute the pupil custodian warning flag so that noncustodial parents cannot gain illegal access to a student.

Technology Plan

The district technology plan is consultant-oriented and has little teacher and administrative input. The document lacks a collaborative strategic plan and does not reflect the district culture. Site personnel indicated that technology planning is frequently driven by the central office.

There is no process to resolve disagreements between Educational Services and Business Services on educational technology projects. Programs like E-Chalk are often initiated without consideration of the strategic plan, support structure or technological capacity.

In some instances, computers are purchased without consideration of long-term plans. There is no district technology committee to deliberate and determine policies and priorities. Principals are not included in central office discussions regarding technology decisions.

Recommendations

The district should:

1. Re-establish the district technology committee and provide it with the responsibility to develop a strategic technology plan. Participation should include classified, certificated and management personnel, parents, community members and student representatives. A list of committee responsibilities should be developed to include: reviewing site technology plans, reviewing the goals and objectives of the Technology Department, exploring available educational systems, and submitting a proposed technology plan and budget to the governing board for consideration.

2. Update the board regularly about district technology plans and programs. Provide a yearly in-service of current trends in technology.

3. Include technology as a regular discussion item in Superintendent's Cabinet and at Principal's Council.

4. Provide a mechanism for the Director of Technology to stay updated on new regulations, laws and technology practices.

5. Ensure that the district takes full advantage of all sources for technology funding including E-rate,K-12 vouchers, CTAP and categorical funding, when appropriate.

6. Devise a plan to ensure consistent and long-term management of the Technology Department.

Communication

There is a perception that most decisions regarding technology systems are made at the administrative level without the opportunity for adequate feedback from the rest of the staff. End users perceive that they are not involved with technology acquisition and support. Users commented that in the past, technology staff members have made changes to major software systems without appropriate notification or instructions.

The Technology Department is not oriented toward its clients. The district lacks published policies on the process to engage the services of the Technology Department. The technology staff frequently appears on a school site, completes repairs and leaves without notifying site personnel of the work's status.

The current work order system does not provide for adequate communication to end users. As a result, users are unaware of the status of work requests and receive no feedback after a work order has been completed. Technicians are not informed of end-user evaluation of their performance. Schools are modernized without the consistent input of the Technology Department**.** Parents complain about the difficulty of making telephone contact with a person instead of a recording when calling the district.

Recommendations

The district should:

1. Ensure that end-user groups are frequently consulted and surveyed about support services.

2. Incorporate full end-user participation into the acquisition of any system.

3. Provide for end-user representation at all levels of the organization. The district should include feedback and suggestions at department meetings and develop a method to report these discussions to the cabinet.

4. Assess communication services currently provided to parents and community members and consider ways to increase communication and district support.

Operating Procedures

The Technology Department's operating procedures are not recorded, nor do they provide for efficient overall organizational operations. There is no policy manual or documentation of processes for operational practices. The new director is developing a formal disaster recovery plan to ensure system operations continuity in the event of a catastrophe. The district has also begun to document password policies and other security protocols.

Before the arrival of the current Technology Director, site administrators expressed frustration that technology staff members were not assigned to provide site support on any expected or planned basis. The new director implemented a new staff allocation plan that ensures that all sites receive support on a rotational basis. The director also implemented a new help desk system that allows staff members to prioritize support tasks based on department and site priorities. Although the new system is an improvement, further efforts are needed to make it fully effective. The department could further benefit by increasing efforts to make site administrators aware of when technology support staff will be on site to address support issues. The site support assignments should be interrupted only for emergency cause.

Definition of Web filtering policies did not include the input of the various stakeholder groups affected by the policy itself. A more collaborative process that invites input from various constituents and stakeholder groups would increase understanding and acceptance of the district's Web filtering policy among all users.

There is no defined classroom technology hardware and software configuration, and standards have not been established for minimum levels of classroom technology.

Information on network changes and system upgrades is not communicated effectively to sites before the changes occur. During interviews, site adminstrators expressed frustration that they do not have access to certain rooms that contain network communications equipment on their campus. Teachers, staff and students are not required to sign a yearly AUP.

Employees are permitted to develop and maintain databases separate from the central systems acquired by the district. Illegal software is loaded on many computers, putting the district at risk of a substantial fine.

Recommendations

The district should:

1. Implement a written and proven back-up and disaster recovery plan. The disaster recovery plan should include provisions for a "hot site" to ensure business continuity in the event of a catastrophe.

2. Continue efforts to implement and document password and security protocols.

3. Increase efforts to communicate with site administrators regarding information on site visitation assignments for technology support delivery.

4. Develop an appropriate process for Web filtering and assign the task to a group made up of teachers and administrators rather than technology technicians.

5. Establish appropriate hardware and software standards in collaboration with the school site personnel.

6. Notify schools well in advance of any changes to network designs, system upgrades, and new implementations. Systems for communicating with teachers should be developed.

7. Provide school site administrators with keys to main distribution frames (MDFs) and intermediate distribution frames (IDFs).

8. Ensure that every employee in the district signs and AUP annual. The signed AUP should be maintained by the Human Resources Department.

9. Immediately develop a policy to detect and eliminate pirated or illegal software from computers, and acquire a software license tracking program such as Altiris or LANDesk. The district is at serious financial risk if an audit were to be conducted.

10. Continue efforts to improve the effectiveness of the new help desk system

Network Resources

FCMAT reviewed network infrastructure elements at the following sites:

- District Network Operations Center
- The district office
- Perris High School
- Paloma Valley High School
- Perris Lake High School
- Community Day School
- The A Street location

The district's IP address space was reviewed as well as elements contained in the network documentation that the district staff provided to FCMAT. Additional elements exist within the district that were not documented for FCMAT. The recommendations in this report should be applied to all network elements, including those that were not specifically reviewed.

The district's network documentation appears to be incomplete. FCMAT consultants did not receive any network diagrams or IP address space deployment documentation.

Administrative networks are not adequately separated from educational networks. Many network elements have either surpassed or are nearing an age in which the vendor will no longer support them. Many elements are also running outdated firmware versions, some of which are no longer supported.

The SNMP community strings on many network elements are using the default community strings of "public" for read-only access and "private" for read-write access. These strings are well known and could be used to make unauthorized configuration changes to the network elements. SNMP management of most network elements is not protected from unauthorized access through the use of an IP access list. Because of this, most network elements are vulnerable to unauthorized configuration changes. Some network elements do not have SNMP management enabled.

Several network elements have the built-in HTTP management server enabled, but access to this interface is not protected by an IP access list. A small number of network elements are not configured to prompt for a password on the console and/or auxiliary ports, and most of the network elements are not configured to time out connections on these same ports.

Telnet access to the VTY ports of the network elements is not protected by an IP access list. This allows any node on the network to connect to the network elements and attempt to log in to them. AAA (log in authentication, command authorization, and session accounting) is not enabled on any of the network elements. Remote log collection of the network elements is not enabled, and most devices do not perform any sort of log buffering.

"System up time" is used to time-stamp network element logs on most network elements. The correct time zone is not configured, and the Network Time Protocol (NTP) service is not enabled on many elements. Most elements also have the password-encryption service disabled. Some elements also have both an "enable secret" password and an "enable" password.

Network routers contain several IP access lists in their configurations that are not applied to any interfaces on the routers. Many of the IP access lists in use appear to allow more access than is actually desired. Several IP access lists contain "deny" lines that are not configured to log instances when these "deny" lines are triggered by unwanted traffic.

The network elements are configured either with log-in banners that do not contain the proper legal verbiage, or are not configured to use log-in banners at all. The use of MAC address learning and restriction is not uniformly configured on the network's Ethernet switches, and the elements do not use 802.1x to restrict access to them to authorized nodes only.

A small number of computers on the internal district network are configured in the firewall to allow remote log-in/terminal/control sessions from any IP address on the public Internet. Further, the network is not monitored by any sort of central network management system.

Recommendations

The district should:

1. Develop a complete set of network documentation. This documentation should at a minimum include the following:

    - A set of network diagrams that shows how all network elements are physically connected. One diagram should document the WAN, and the remaining LANs should be documented in individual diagrams.

    - A document that contains the IP address deployment scheme for the WAN and each individual LAN in the network.

    - A list of all network elements that are used to provide service in the district network. For each network element, this includes the IP address, the vendor and model, the serial number, the operating firmware revision, and the location.

    This documentation should be reviewed at least quarterly for accuracy, and management of this documentation should be assigned to a specific employee at the district.

2. Review the administrative network traffic flows and the educational network traffic flows. The traffic from these two networks is allowed to commingle. This must be resolved to prevent systems with student access from being used to intercept administrative network traffic, and/or access to administrative systems by nodes on the educational network. The use of properly configured IP access lists can be used to accomplish this.

3. Review all network elements to identify those that have reached or will soon reach end-of-life status with the hardware vendor. The district network appears to be entirely based on Cisco Systems equipment, and the status of each network element can be determined at the Cisco Web site. Network elements that have reached end-of-life status should be scheduled for replacement with a currently supported product from the district's preferred hardware vendor. Operating a production network on unsupported equipment is not recommended.

4. Review all firmware versions running on the network elements to identify firmware revisions that are no longer supported by the hardware vendor. A review of vendor security bulletins relating to any installed firmware revisions should also be undertaken. The district network elements reviewed are all manufactured by Cisco Systems, and the status of firmware versions in addition to security bulletins can be obtained at the Cisco Systems Web site. Operating a production network on unsupported firmware or using firmware that contains severe security related bugs is not recommended.

5. Ensure that SNMP community strings do not use the default "public" and "private" values. These SNMP community strings should be changed to randomly generated character strings of at least eight characters in length. Unique community strings should be employed on all network elements, and the use of read-write community strings should be disabled where possible.

6. Ensure that all SNMP community strings are protected by an IP access list. The access list should allow access only from a central network management server and possibly from a small number of network workstations that are operated by the district network staff. Access attempts by unauthorized workstations should be logged.

7. Configure SNMP community strings on all network elements to enable the use of a central network management system.

8. Use an IP access list to protect network elements that have built-in, HTTP-based management interfaces from unauthorized access. The access list should allow access only from a central network management server and possibly from a small number of network workstations that are operated by district network staff. Access attempts by unauthorized workstations should be logged.

9. Configure and require log-ins on all network element console and auxiliary ports. These ports should be configured to time out management sessions after a certain amount of idle time. This idle time out is left to the discretion of district staff.

10. Protect telnet access to all network elements with an IP access list. The access list should allow access only from a central network management server and possibly from a small number of network workstations that are operated by district network staff. Access attempts by unauthorized workstations should be logged.

11. Configure AAA (log-in authentication, command authorization, and session accounting) on all network elements that support this service. AAA uses either TACACS+ or RADIUS to provide centralized control of log-ins, restrict the commands specific users can run , and provide session accounting of the commands entered and the individuals who entered them. AAA facilitates log-in management of all network elements and permits the collection of detailed audit logs in the event that a network security incident occurs involving the unauthorized access of a network element. TACACS+ or RADIUS can also be run on a Linux server.

12. Configure all network elements to send debug level syslogs to a remote syslog server. This can be the same Linux server used to provide the TACACS+ or RADIUS services discussed in recommendation 11. Network element logs that are collected on a central server can be automatically analyzed by a number of freely available tools and used to alert network engineers of potential performance and security issues as they occur in the district network. This allows for a more proactive management of network performance and network security. Remote collection of logs can also help law enforcement investigate a network security incident.

13. Configure these elements to use the local time provided via the NTP (Network Time Protocol) service running on each element to time stamp logs.

14. Configure the elements for the correct time zone. This is required to time logs accurately.

15. Configure the elements to synchronize their system clocks via NTP (Network Time Protocol) to a central NTP server. The server used for recommendation 11 and 12 can run the NTP server process required to provide this service.

16. Configure all Cisco Systems network elements to use the password-encryption service. Although the encryption used by this service is reversible, it provides an additional layer of security for passwords contained in the network elements' configuration files.

17. Configure all Cisco Systems network elements to use only the "enable secret" command for setting the enable password on each network element. The encryption used by this command is not reversible, and is much more secure than the reversible encryption used by the "enable password" command. Alternatively, the enable password for all elements can be set at the TACACS+ or RADIUS server.

18. Thoroughly review all IP access lists on all network elements. Any unused access lists should be removed from the network element configuration files. Any "deny" lines in an IP access list should be logged, and all access lists should be verified for proper filtering. These access lists should be reviewed periodically to ensure the proper level of filtering is taking place.

19. Implement a more thorough log-in banner. Properly worded log-in banners are essential to the successful prosecution of a legal case involving unauthorized access. A sample log-in banner is attached as an appendix to this report. This log-in banner should be reviewed by the district's legal counsel before it is implemented. The banner should be installed on all network elements that support the use of log in-banners.

20. Configure all Ethernet switches to use MAC address security. This will prevent a "rogue node" from being allowed to connect to the network and gain access to unauthorized traffic or systems. The specific configuration of MAC address security may need to be adjusted for users that have mobile computers such as laptops that do not always connect to the same switch port.

21. Consider using the 802.1x protocol to authenticate all nodes attempting to connect to the district network. This protocol allows for the roaming of mobile computers such as laptops, and greatly enhances the security of any network by allowing only authorized nodes to gain access. A full implementation of 802.1x networkwide will require significant monetary and network engineering resources.

22. Block inappropriate access to servers. At present, servers on the district's internal network permit connections from any IP address to services that allow remote log-in or remote control of these servers. If access to these services is required, the access should be restricted to a specific set of external IP addresses, and access should be temporary. If permanent access to these services is required, any remote log-in or remote control services should be accessible only via a strongly encrypted IPSEC VPN connection.

23. Implement a centralized network management system. This type of system can greatly enhance network performance and utilization. A network management system typically performs SNMP trap collection from all network elements, utilization graphing of important interfaces on the network elements, and automatic alerting of district staff upon the reception of SNMP traps, indicating a network problem or important performance threshold exception. This system can be implemented on the same system referenced in recommendation 11, or a commercial product such as Castle Rock SNMPc can be used if desired.

24. Take proper security measures regarding the configuration of wireless access points (WAPs) on the district network. All WAPs connected to the district network should support the 802.11i security standard, and any WAP that does not meet this requirement should not be connected to the network. 802.11i includes WPA2(Wi-Fi Protected Access), the use of the AES encryption algorithm, as well as the 802.1x access control protocol. All these should be required of any node desiring to connect to the district network via a WAP. Any WAP installed by the district should also be configured so that it does not broadcast the wireless SSID of the WAP.

Appendices

A. Sample Log-In Bannder
B. Study Agreement

Appendix A: Sample Log-In Banner

****

NOTICE TO USERS

This is a (Your org here) computer system and is the property of (Your org here). It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, (Your org here), and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or (Your org here) personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

****

FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM
STUDY AGREEMENT
January 4, 2007

The FISCAL CRISIS AND MANAGEMENT ASSISTANCE TEAM (FCMAT), hereinafter referred to as the Team, and the Perris Union High School District, hereinafter referred to as the District, mutually agree as follows:

1. BASIS OF AGREEMENT

The Team provides a variety of services to school districts and county offices of education upon request. The District has requested that the Team provide for the assignment of professionals to study specific aspects of the Perris Union High School District operations. These professionals may include staff of the Team, County Offices of Education, the California State Department of Education, school districts, or private contractors. All work shall be performed in accordance with the terms and conditions of this Agreement.

2. SCOPE OF THE WORK

A. Scope and Objectives of the Study

The scope and objectives of this study are to:

1) Conduct a review of the district's administrative and instructional systems, applications, processes, infrastructure and emerging technologies and make recommendations for improvement.
2) Conduct a review of the district's technology organizational structure and staffing allocations and make recommendations for improvement.
3) Conduct a security and configuration review of the district's network resources and make recommendations for improvement.

B. Services and Products to be Provided

1) Orientation Meeting - The Team will conduct an orientation session at the District to brief District management and supervisory personnel on the procedures of the Team and on the purpose and schedule of the study.

2) On-site Review - The Team will conduct an on-site review at the District office and at school sites if necessary.

3) Progress Reports - The Team will hold an exit meeting at the conclusion of the on-site review to inform the District of significant findings and recommendations to that point.

4) Exit Letter - The Team will issue an exit letter approximately 10 days after the exit meeting detailing significant findings and recommendations to date and memorializing the topics discussed in the exit meeting.

5) Draft Reports - Sufficient copies of a preliminary draft report will be delivered to the District administration for review and comment.

6) Final Report - Sufficient copies of the final study report will be delivered to the District following completion of the review.

3. PROJECT PERSONNEL

The study team will be supervised by Anthony L. Bridges, Deputy Executive Officer, Fiscal Crisis and Management Assistance Team, Kern County Superintendent of Schools Office. The study team may also include:

A. Andrew Prestage, FCMAT Management Analyst
B. Two FCMAT Technology Consultants

Other equally qualified consultants will be substituted in the event one of the above noted individuals is unable to participate in the study.

4. PROJECT COSTS

The cost for studies requested pursuant to E.C. 42127.8(d)(1) shall be:

A. $500.00 per day for each Team Member while on site, conducting fieldwork at other locations, preparing and presenting reports, or participating in meetings.

B. All out-of-pocket expenses, including travel, meals, lodging, etc. Based on the elements noted in section 2 A, the total cost of the study is estimated at $6,500. The District will be invoiced at actual costs, with 50% of the estimated cost due following the completion of the on-site review and the remaining amount due upon acceptance of the final report by the District

C. Any change to the scope will affect the estimate of total cost.

Payments for FCMAT services are payable to Kern County Superintendent of Schools-Administrative Agent.

5. RESPONSIBILITIES OF THE DISTRICT

A. The District will provide office and conference room space while on-site reviews are in progress.
B. The District will provide the following (if requested):

1) A map of the local area
2) Existing policies, regulations and prior reports addressing the study request
3) Current organizational charts
4) Current and four (4) prior year's audit reports
5) Any documents requested on a supplemental listing

C. The District Administration will review a preliminary draft copy of the study. Any comments regarding the accuracy of the data presented in the report or the practicability of the recommendations will be reviewed with the Team prior to completion of the final report.

Pursuant to EC 45125.1(c), representatives of FCMAT will have limited contact with District pupils. The District shall take appropriate steps to comply with EC 45125.1(c).

6. PROJECT SCHEDULE

The following schedule outlines the planned completion dates for key study milestones:

Orientation:	To be Determined
Staff Interviews:	To be Determined
Exit Interviews:	To be Determined
Preliminary Report Submitted	Six weeks following date of Exit Interview
Final Report Submitted	To be Determined
Board Presentation	To be Determined

7. CONTACT PERSON

Please print name of contact person: Chuck Dinsfriend, Director of Technology

Telephone 951 943 2760, ext 2200 FAX 951 940-4241

Internet Address cdinsfriend@puhsd.org

Dennis D. Murray 1-18-07

Dennis D. Murray, Superintendent Date
Perris Union High School District

Barbara Dean 2-1-07

Barbara Dean, Deputy Administrative Officer Date
Fiscal Crisis and Management Assistance Team

In keeping with the provisions of AB1200, the County Superintendent will be notified of this agreement between the District and FCMAT and will receive a copy of the final report.