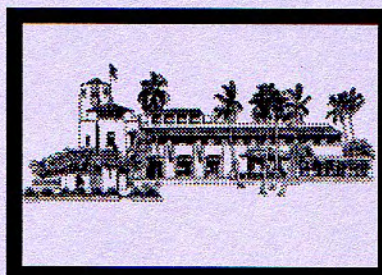


OFFICE OF THE CITY AUDITOR

City and County of Honolulu
State of Hawai'i

Audit of Selected City Information Technology Controls

A Report to the
Mayor
and the
City Council of
Honolulu

Report No. 06-01
January 2006

Audit of Selected City Information Technology Controls

A Report to the
Mayor
and the
City Council
of Honolulu

Submitted by

THE CITY AUDITOR
CITY AND COUNTY
OF HONOLULU
STATE OF HAWAI‘I

Report No. 06-01
January 2006

Foreword

This is the report of the audit conducted on selected information technology security controls applied by the Department of Information Technology. The city auditor initiated this audit pursuant to Section 3-502.1(c) of the Revised Charter of Honolulu and the Office of the City Auditor's Annual Work Plan for FY2005-06. The city auditor determined that a review of these information technology security controls was warranted due to the increasing reliance on information technology-based processes to support current government service initiatives to the public, along with increasing general concern among governments at all levels and the public over information security.

We wish to acknowledge the assistance and cooperation of the Department of Information Technology and others whom we contacted during this audit.

Leslie I. Tanaka, CPA
City Auditor

EXECUTIVE SUMMARY

Audit of Selected City Information Technology Controls

Report No. 06-01, January 2006

This audit was initiated by the Office of the City Auditor pursuant to Section 3-502.1(c) of the Revised Charter of Honolulu and the Office of the City Auditor's Annual Work Plan for FY2005-06. The city auditor selected this audit because of the increasing reliance on information technology-based processes to support current government service initiatives to the public, along with increasing general concern among governments at all levels and the public over information security. This report reviews and assesses the adequacy of selected general information security controls employed by the Department of Information Technology, such as backup and recovery, physical and environmental controls, and service continuity/contingency planning.

Background

Information is a key asset that has value to governmental organizations and requires to be appropriately protected. Information security controls preserve the confidentiality, integrity and availability of key information systems, programs, and data. Recent city and state information systems audits in other jurisdictions underscore the importance of effective information security controls. This is increasingly important as today's governments place greater reliance on information technology (IT) to support their service initiatives, and many have substituted IT-based processes to provide public information and services.

For a city of its size, Honolulu has been repeatedly recognized by the annual *Digital Cities Survey* for its service-oriented, business-driven, and cost-effective application of IT in city government. Although most of the governments surveyed provided a significant degree of IT-related public services and IT integration in their operations, the majority of cities surveyed had notable deficiencies with their security framework, including issues with the state of their security plans, standards and policies, annual audit requirements, currency of security policies and plans, and disaster recovery plans. With the current reliance on IT-based processes to provide public services and information, this underscores the growing importance of appropriate information security controls to protect critical and sensitive information systems, programs and data from threats to IT service continuity and availability, minimize

potential damage to key systems and data, and maximize the utility that these systems can provide to public services and governmental operations.

Summary of Findings

We found that Department of Information Technology's control framework is insufficient to ensure comprehensive and effective citywide IT security management, due to inadequate oversight and lack of sufficient authority. We also found physical and environmental controls are inadequate to effectively protect key city IT systems and resources, due to inadequately managed data center access practices and not addressing known physical and environmental control issues. We lastly found that while the department manages normal backup and recovery requirements, its disaster recovery planning and implementation is lacking to ensure service continuity in the event of a major disruption.

Finding 1: The Department of Information Technology's control framework is insufficient to ensure comprehensive and effective security management.

- DIT's oversight to ensure effective security management of the city's IT systems is inadequate.
  - Key planning documents, and other DIT policies have attempted to externalize certain aspects of oversight responsibility to the departments;
  - Key security management oversight functions such as monitoring effectiveness and assessing risks have not been implemented; and
  - The department has not developed an overall foundation that links together individual security guidance pieces into an effective citywide program of security planning and management.
- The department lacks sufficient authority to effectively implement and monitor a citywide IT security management system.
  - Current administrative guidance separates the policymaking responsibility from the monitoring and enforcement responsibility;

- The department relies on self compliance of the other departments and users as a technique to manage citywide IT security; and

- Though responsibility is delegated, DIT does not provide the sufficient training to these responsibilities and obligations that would justify the delegation.

Finding 2: Physical and environmental controls are inadequate to effectively protect key city IT systems and resources.

- Data center access practices are inadequately managed.

  - Almost every DIT employee is issued an access card, with minimal regard to his or her actual need for access into the data center;

  - With the exception of card issue and establishing initial privilege level, there is little management of the card system and its related rules; and

  - Logged activity is not monitored and reviewed on a regular basis.

- Physical and environmental control issues have not been effectively addressed.

  - The data center is subject to water intrusion;

  - Fire suppression may not be in working condition;

  - Air conditioning cooling failures are problematic;

  - There are a few entry points that appear insecure; and

  - Access and air conditioning issues related to the Kapolei Hale computer room.

- DIT has not proactively pursued durable resolutions to known physical and environmental concerns.

  - Disjointed departmental management responsibility contributes to lack of implementation of appropriate controls; and

- ➢ DIT has only sought temporary solutions to these known problems.

Finding 3: The department manages normal backup and recovery requirements adequately, but disaster recovery planning and implementation is lacking.

- The department uses reasonable management practices to manage its routine backup and recovery duties.
  - ➢ There are procedures and appropriate activity to regularly back up computer files and store backup copies securely at an off-site location;
  - ➢ There have been very few memorable user recoveries under the current system; and
  - ➢ There are a few issues with the current management of routine backup and recovery that require future management attention.
- The department has not effectively managed its responsibilities related to disaster recovery and contingency planning.
  - ➢ There are notable weaknesses related to the current state of disaster recovery;
  - ➢ Most functions in the plan are intended to be carried out by Honolulu Municipal Building-based personnel; and
  - ➢ Kapolei Hale site is not fully suited for recovery or command activities.
- Insufficient support exists to implement an effective disaster recovery program.
  - ➢ Previous administration was primarily concerned with higher profile and public relations type initiatives and accomplishments; and
  - ➢ Disaster recovery coordinator has responsibility but no authority to accomplish disaster recovery planning.

Recommendations and Response

We made a number of recommendations to resolve the issues and problems identified during this review. In summary, we recommended that the department should:

- Develop a comprehensive IT security plan that includes, but is not limited to the creation of a functional management plan, and an ongoing assessment process to ensure the evaluation of the plan;
- Seek funding to facilitate citywide risk assessment, including business impact and business continuity/resumption;
- Seek to clarify authority and lines of responsibility for citywide security management by appropriately revising key planning documents and policies, and working with the mayor and the departments to resolve coordination, management, and oversight issues;
- Improve security for the data center by seeking funding for improved physical and environmental controls, and manage data center access to more accurately reflect actual needs for access;
- Seek ways to further improve routine backup and recovery practices by acquiring funding for upgrading technology or media, and developing appropriate guidelines or other awareness programs to enhance backup and recovery effectiveness;
- Pursue an appropriate funding program to fund disaster recovery planning and required supporting elements, and provide an appropriate level of authority and priority to the disaster recovery function within the department; and
- Coordinate and seek agreements from external departments and agencies related to supporting elements and services related to physical controls and disaster recovery planning.

We also recommended that the mayor should ensure the department receives the appropriate budgeting consideration for physical and environmental controls priorities, improvements to backup and recovery, and disaster recovery. We further recommended that the mayor should facilitate and guide discussions between the department and other

departments to ensure proper coordination in support of physical and environmental controls and disaster recovery planning requirements.

In its response to our draft audit report, the Department of Information Technology expressed general agreement with most of the audit findings and recommendations.

The department acknowledged the need to improve security, backup, recovery, and disaster preparation, but noted the difficulty of working under funding constraints that have precluded compliance with many common security management practices. The department views this audit as an opportunity to educate the administration and city council, and indicated its commitment to timely meeting these challenges in a fiscally prudent manner. The department agreed with the security management issues related to citywide IT security oversight, authority, and enforcement; improving the access card system, the need to improve disaster recovery, the need to coordinate and fund improvements to known environmental control issues, and the need to fund supporting measures such as risk assessments, monitoring, and required technology and media upgrades. The department indicated narrow disagreement on the issue of its overall IT security responsibility, stating that agencies should be responsible for IT security much like they are responsible for the physical security of systems and resources.

The department provided additional information clarifying aspects of the draft report, which as appropriate, were incorporated into the final report as additional information or stylistic changes.

Leslie I. Tanaka, CPA
City Auditor
City and County of Honolulu
State of Hawai'i

Office of the City Auditor
1000 Uluohia Street, Suite 120
Kapolei, Hawai'i 96707
(808) 692-5134
FAX (808) 692-5135
www.honolulu.gov/council/auditor

Table of Contents

List of Exhibits

List of Appendixes

Chapter 1
Introduction

This *Audit of Selected City Information Technology Controls* was conducted pursuant to the authority of the Office of the City Auditor (OCA) as provided in the Revised City Charter of Honolulu. The audit is consistent with OCA's Annual Audit Program established for FY2005-06, which was communicated to the mayor and the City Council on June 29, 2005.

Information is a key asset of governmental organizations and must be appropriately protected. Information security controls act to preserve the confidentiality, integrity, and availability of key information systems, programs, and data. The protection of information systems has become important as governments increasingly rely on them to support programs and provide the public with information and services. Recent information systems audits in other city and state jurisdictions have highlighted the importance of effective information security controls.

Background

For its size, Honolulu has been repeatedly recognized by the annual *Digital Cities Survey* for its service-oriented, business-driven, and cost-effective application of information technology (IT) in city government. The annual survey rates the integration of IT into key common county and city government operations and services. The 2004 survey reported that although most governments had integrated IT into their operations and public services to a significant degree, 42 percent had either none or only partially developed information security standards (such as security policies, standards and guidelines, annual audit requirements, and disaster recovery plans). Only 3 percent of cities and 4 percent of counties required information technology departments to have such security standards in place. Typically, good information security practice involves regular review and timely updates of information security standards; however, the survey noted that only 39 percent of cities with full standards had done this in the past 18 months.

These results further underscore the growing importance of information security controls to protect and minimize potential damage to critical and/or sensitive information systems, programs, and data from threats to service continuity and availability; and to maximize the utility these systems can provide to public services and governmental operations.

Organization

In the City and County of Honolulu, the Department of Information Technology (DIT) is responsible for the security of the city's information systems and key public safety-related telecommunications systems. DIT is not responsible for systems maintained by the Board of Water Supply, Honolulu Police Department, or other semi-autonomous agencies created by ordinance.

Statutory background

The Department of Information Technology was established pursuant to Section 6–1201, Revised Charter of Honolulu (RCH). Formerly known as the Department of Data Systems, the department was created as a part of the mayor's 1998 reorganization of city departments and functions. The department's primary functions, as described in Section 6–1202, RCH, are to operate the city's data processing system, provide technical expertise in data processing, assist the city's managing director with management information for decision support, and advise the mayor on data processing matters.

Responsibilities

The department's mission is to provide information technology products, services, guidance, and direction to enable city agencies to serve the public in a cost-effective and efficient manner. The department sees its primary responsibilities as: (a) increasing the efficiency of city workers; (b) maintaining, securing, and protecting the city's various communications networks in support of public safety, including but not limited to city emergency response functions; (c) providing the city with a stable and robust electronic working environment for all users, and (d) providing leading edge technological solutions to the city's business needs.

The department carries out its responsibilities by planning, directing, and coordinating the city's information technology systems and resources. It also sets and enforces citywide computer and data security, standards, and policies. In addition, the department provides the city with technical expertise in electronic data processing and assists the city's managing director and mayor in administering information technology and promoting a technology industry. A significant function of the department is its management of the city's computer network and central data processing operations center on a continuous basis — twenty-four hours a day, seven days a week.

Staffing

According to Department of Human Resources statistics, the department's overall staffing has followed a V-shaped growth trend over

the last twelve years (1993-2005). Between 1993-2000, the number of full time equivalent (FTE) employees fell steadily, from 118 in FY1992-93 to 96 in FY1999-2000. Since FY2000-01, however, the department has increased its staff each year and now retains 138.5 FTE employees.

Over the past five years, the department's divisional staffing has remained relatively stable. Most of the cumulative growth to the department has been in the Applications Division. Of interest in relation to this audit is the rather unchanged staffing level of the Operations Division, and the implications this poses regarding the department's ability to adequately manage its information security.

Funding

The department's funding has been fairly stable over the past five years. Exhibit 1.1 shows the department's funding sources from FY2001-02 through FY2005-06. Two substantial recent increases in funding were due primarily by the transfer of the Department of Design and Construction's telecommunications functions in 2003 and the continuing implementation of departmental IT centralization initiatives. Exhibits 1.2 and 1.3 illustrate expenditures by division and the character of expenditures during the period of FY2001-02 through FY2005-06, respectively.

Exhibit 1.1
Department of Information Technology, Funding Sources
FY2001-02 through FY2005-06

Fiscal Year	*General Fund*	*Sewer Fund*	*Liquor Commission Fund*	*Refuse General Operating Account (SWSF)*	*Federal Grants Fund*	*Housing & Community Development Section 8 Fund*	*TOTAL FUNDING*
FY2001-02	$7,844,765	$ 46,156	$16,443	$28,709	$0	$0	$ 7,936,073
FY2002-03	$8,472,141	$ 53,766	$39,696	$32,807	$ 65,735	$76,560	$8,740,705
FY2003-04	$8,471,921	$ 52,245	$36,388	$36,036	$ 70,166	$90,713	$ 8,757,469
FY2004-05*	$11,982,674	$ 54,516	$39,696	$36,036	$129,324	$129,056	$12,371,302
FY2005-06**	$13,189,832	$117,576	$43,152	$39,336	$154,930	$120,218	$13,665,044

*Appropriated, not actual, funding.
**Budgeted, not actual, funding.
Source: Department of Information Technology, 2002-2005

Exhibit 1.2
Department of Information Technology, Expenditures by Division
FY2001-02 through FY2005-06

Division	*Actual FY2001-02*	*Actual FY2002-03*	*Actual FY2003-04*	*Approved FY2004-05*	*Budgeted FY2005-06*
Administration and Planning	$3,138,825	$3,433,848	$3,234,823	$6,340,794	$6,852,422
Applications	$2,562,796	$2,769,577	$3,043,875	$3,280,598	$3,732,822
Operations	$1,073,413	$1,220,879	$1,284,128	$1,305,168	$1,430,088
Technical Support	$1,161,039	$1,316,401	$1,194,643	$1,444,742	$1,649,712
Totals	$7,936,073	$8,740,705	$8,757,469	$12,371,302	$13,665,044

Source: Department of Information Technology, 2002-2005

Exhibit 1.3
Department of Information Technology, Character of Expenditures
FY2001-02 through FY2005-06

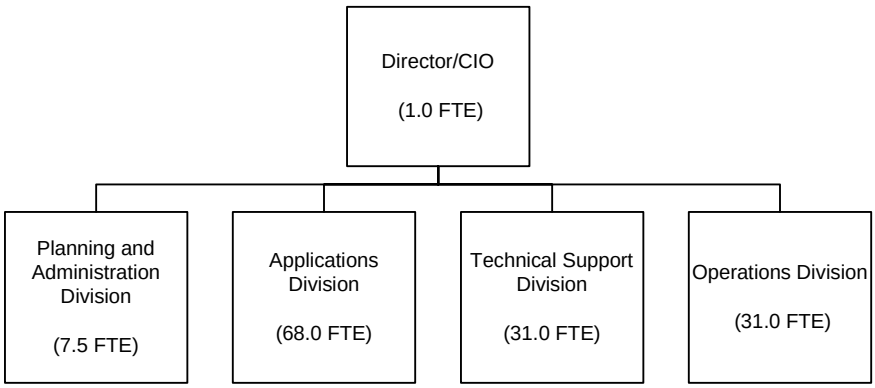
Fiscal Year	*Salaries*	*Current Expenses*	*Equipment*	*Totals*
FY2001-02	$5,295,124	$2,018,746	$622,203	$7,936,073
FY2002-03	$5,824,088	$2,072,509	$844,108	$8,740,705
FY2003-04	$5,976,021	$2,030,845	$750,603	$8,757,469
FY2004-05*	$6,471,326	$5,007,347	$892,629	$12,371,302
FY2005-06**	$7,271,750	$5,348,565	$1,044,729	$13,665,044

* Appropriated, not actual, expenditures
** Budgeted, not actual, expenditures
Source: Department of Information Technology, 2002-2005

The Department Has Four Functional Divisions

Currently, the department is organized into four divisions, each reflecting their intended function: Planning and Administration; Applications; Operations; and Technical Support. Exhibit 1.4 shows the department's organizational chart.

Exhibit 1.4
Department of Information Technology Organization Chart



Source: Department of Information Technology, 2005
FTE: Full time equivalent

The department is headed by a director who is also the chief information officer for the City and County of Honolulu. The department is further divided into four functional divisions, each with a division chief as its lead administrator. Although not formally depicted on the chart, each division also oversees specific information technology services.

Planning and Administration Division

The Planning and Administration Division administers and directs the department's administrative policies, procedures, and plans. The division also supports the information technology requirements of the department by providing strategic planning, capital budget planning, IT master planning, and project management. It also plans and executes the department's ongoing reorganization to incorporate the Department of Design and Construction's former telecommunications functions.

Applications Division

The Applications Division analyzes the business functions of city divisions and makes recommendations on how to improve services by developing

and implementing software applications. This division provides support for major software applications such as those used for finance, land management, the city geographical information systems, public safety, and management services. The division also provides each city agency with direct technical support from computer service representatives.

Operations Division

The Operations Division manages the city's mainframe computer system and assists city personnel in their use of mainframe services. The division provides central help desk support for all city mainframe users as well as processing for all mainframe applications. Its data center operates as a nerve center for the city's IT infrastructure, and it monitors equipment to ensure continuous availability of IT services. The division is also responsible for disaster recovery planning for service continuity.

Technical Support Division

The Technical Support Division provides technical assistance to all city divisions in evaluating, planning, and using information technology. Its mission is accomplished by implementing and maintaining desktop computer systems and networks, providing city-wide computer training and user assistance, and maintaining city web servers to assist agencies in providing information via the Internet. The division also oversees the security of the city's data network and mainframe system, and recommends, maintains, and implements established city security policies.

Audit Objectives

1. Review and assess the adequacy of selected general information security controls employed by the Department of Information Technology such as backup and recovery, physical and environmental controls, and service continuity/contingency planning.

2. Make recommendations as appropriate.

Scope and Methodology

Our audit reviewed a selection of general information security controls as applied and managed by the Department of Information Technology (DIT), including backup and recovery procedures for key systems, physical and environmental controls, and service continuity/contingency plans. The review covered legal requirements and internal policies, procedures, and verbal or written administrative guidance related to such controls and activities. We assessed the impact of these controls on

operations and the ability to meet departmental and other relevant city security objectives. Some autonomous agencies such as the Board of Water Supply and Honolulu Police Department are not included in the review.

The audit focused primarily on general information controls applied over departmental operations and resources. The controls under audit included the physical and environmental controls applied at the department's data center in the Honolulu Municipal Building and Kapolei Hale disaster recovery site. We also reviewed physical access controls at both locations. The audit did not cover other access controls such as logical or software controls applied by the department, physical and environmental controls related to telecommunications facilities managed by the department, or controls applied by other departments to facilities or resources the department may provide services to.

We reviewed backup and recovery procedures for selected key systems located in the data center and supplemental activities related to this objective at Kapolei Hale. The audit did not include backup and recovery procedures implemented at any of the other city departments, or those applied to systems outside the control of the data center.

We also reviewed and assessed the city's disaster recovery plans for service continuity, which are also managed by the department's operations division. The audit did not cover client/server recovery or other operational level maintenance related to recovering individual resources applied by the department.

The audit reviewed the adequacy of the department's security framework to protect the city's critical information systems and data by comparing it to commonly used industry security standards for relevant controls, data management, and service continuity. We reviewed the high level management role in coordinating and integrating the current applied information security framework. We also reviewed previous assessments of departmental information security to determine whether the department has addressed previously identified issues and problems.

We reviewed applicable charter provisions, ordinances, laws, rules and regulations, departmental policies and procedures, annual reports, budgets, financial documents, plans, and other documentation related to the department's capabilities to fulfill its mission and purposes related to security controls and service continuity.

We conducted interviews with department management, operations division supervisors and staff, and other departmental staff whose primary function relates to the administration of security controls and disaster recovery to determine past and current practices. We also interviewed selected personnel from other agencies related to the department's management of disaster recovery coordination and provision of physical controls.

We conducted visual observation and reviews of operations at the department's data center and Kapolei Hale recovery site, focusing on the physical, environmental, and access controls employed, backup and recovery practices, and other related operational activities.

We also researched and reviewed selected Internet, literature, and technology information resources to identify commonly utilized information security frameworks, controls and practices used by government and industry.

As the audit concerned physical controls, activities of personnel, and management of security, we did not assess the reliability of computer systems themselves or computer-processed data.

The audit was conducted in accordance with generally accepted government auditing standards (GAGAS).

Chapter 2

The Department of Information Technology Does Not Provide Sufficient Oversight and Planning to Effectively Protect and Secure the City's Key Information Technology Resources and Systems

In the City and County of Honolulu, the Department of Information Technology (DIT) is responsible for the overall management of the city's critical information technology (IT) resources and systems, including providing security of key systems and resources. The department has admirably managed the technical aspects of the city's information technology system, despite the age of certain key systems and funding constraints.

However, the department has been unable provide sufficient oversight in its overall security management due to a lack of authority in current administrative guidance and because it has delegated key monitoring and enforcement responsibilities to departments and users. Though most critical resources and systems are kept in-house at the Honolulu Municipal Building basement's data center, the department has not appropriately managed access to the center or remedied known physical and environmental risks. The department reasonably manages routine daily backup and recovery, but has not adequately managed the planning required for disaster recovery of citywide information systems and resources. This report examines the department's effectiveness in meeting its responsibilities for the selected information security control areas.

Summary of Findings

1. The Department of Information Technology's control framework does not provide sufficient oversight to ensure comprehensive and effective security management of the city's information technology systems. The department lacks sufficient authority to successfully control citywide information technology security; and has not developed a foundation that links individual security guidelines to an effective program of citywide security planning and management. Key oversight functions, such as monitoring and risk assessment, have been delegated to departments and users; yet the department

does not provide sufficient training to justify delegating these responsibilities and obligations.

2. We found that some physical and environmental controls are inadequate to effectively protect key city information technology systems and resources. For instance, data center access cards are issued without regard to actual access requirements and key management practices such as actively managing the access control system or reviewing logged access activity are not evident. Known physical and environmental control issues are evident, but the department has not actively pursued durable solutions to these concerns.

3. While the department effectively manages normal backup and recovery requirements, disaster recovery planning and implementation is lacking. There are a few issues with the current management of routine backup and recovery that require management attention. The department has not effectively managed its disaster recovery and contingency planning responsibilities: there are notable weaknesses with current disaster recovery plans and insufficient support for implementing an effective recovery program.

The Department of Information Technology's Control Framework Is Insufficient to Ensure Comprehensive and Effective Citywide IT Security Management

Administrative guidance tasks the department with issuing general security guidance and administering technical security solutions. The department has been largely successful in applying technical solutions to defend the city's IT resources and systems. However, apart from technical controls managed by the department, key elements of overall security management have been left to departments and users largely because the department has no explicit enforcement or oversight authority despite its overall management responsibility.

Departments have been left to assess their own security needs, authorize users, create additional policies, and enforce all levels of IT policies. A great deal of risk management in the city's security framework relies on the concept of the "good city user", where individual user compliance is required to maximize security of city systems and resources. Despite having citywide responsibility for its effective management and control, the information technology department is authorized to provide only technical advice for most departmental and user security issues.

The department's oversight of city IT systems security is inadequate

In accordance with Mayor's Directive 99-1, the department was given overall responsibility for managing the city's IT resources and services. The impetus for the directive was to consolidate and centralize management of the city's IT systems with the department.

However, the department has not demonstrated oversight or guidance proportional to its responsibility for the overall management of the city's IT security. The department has emphasized its technical and production functions at the expense of overall citywide IT system management, often delegating its authority in security matters to the departments and users.

Key planning documents and other departmental policies have attempted to delegate some oversight responsibility to the departments

As noted above, mayoral Directive 99-1 was intended to centralize the management of the city's IT resources and systems. However, other administrative guidance, including from the department itself, acts to diffuse the department's overall responsibility without the proper coordination, reporting or oversight mechanisms needed for the department to retain appropriate management control.

For instance, prior to the mayor's 1999 directive, the department created the city's *Information Technology Master Plan* in 1998. The plan, which has never been revised and is therefore still operative today, was intended to provide high-level strategic direction and a unifying vision for the management of information technology in city government.

Under 'Security Standards', the plan indicates that each agency should designate someone to be responsible for IT security, including performing a risk classification for all applications and documents of importance to the agency. The classification should assess the agency's risk of exposure or harm should data or programs be destroyed, altered or stolen.

However, since Directive 99-1 was issued, there has been no indication as to whether the department has adopted this risk assessment responsibility or agencies are still expected to perform their own assessments and coordinate them with the department to assist with its overall management of citywide IT security.

Furthermore, the 2003 citywide security policy created by the department indicates that each department must conduct business impact analyses of their own critical information systems. To date, no agencies

have performed such an analysis, and the department is now seeking funds for a citywide business impact analysis.

Thus, through its administrative guidance to agencies, the department has delegated the risk assessment and business impact analysis aspects of its security management responsibility. By not collecting and coordinating such information, the department loses key information relevant to security management and planning for which it has overall responsibility.

Although the department created the current security policy, it did not devise an oversight role for itself to ensure effectiveness of the policy for agencies and end users. Instead, responsibility for security is dispersed and there is no coordinated oversight or management. Part of this division may be due to the treatment of policymaking as separate from enforcement in Directive 99-1. Nevertheless, it seems inappropriate for the department to perpetuate such a disjointed approach to IT security by assigning away its management responsibility without ensuring uniform reporting or coordination (apart from incident handling).

The mayor's 99-1 directive defined the department's security function as having citywide implications but failed to provide adequate oversight authority to implement this responsibility. We are aware of a suggestion within the department that it be allowed to oversee the effectiveness of the citywide security framework; however, unless the current administrative guidance is revised, no such authority exists even if the role were taken on.

Key security management oversight functions such as monitoring effectiveness and assessing risks have not been implemented

Despite its responsibility for both management and technical aspects of citywide IT security, under the current city security policy the department has retained its technical functions but delegated much of its management role. While the department continues to implement technical security solutions, manage network security, provide perimeter control, and protect against malicious events, agencies are left to conduct their own monitoring.

We found that the only coordination between the department and city agencies is for security violations and incident handling, and the support provided by the department is technical rather than managerial. This suggests a reactive rather than monitored or managed approach to IT security. When we inquired whether anyone ensures that responsibilities given to agencies or users are complied with, we found there is no official

monitoring of compliance. The department characterizes its computer service representatives as "its eyes and ears", but noted the representatives are not officially tasked with monitoring compliance. As a result, effectiveness of the security policies and guidelines largely relies on agency and user compliance.

We acknowledge that the department has been successful in protecting the network systems under its control and has reported no substantiated unauthorized access. However, the department is lacking an effective way to enforce the citywide security policy at the agency level, as it cannot monitor or enforce all guidelines remotely. This also means the policy cannot be assessed for its effectiveness.

The department's monitoring activities are triggered only by alleged violations of the security policy. In addition, they appear to be focused solely on email security. Given the department's responsibility for overall IT security, this degree of monitoring is very narrow. The department does, however, maintain logs that could be used to promote accountability. But given the size of the logs, the department considers regular review as impractical; consequently there is no active monitoring except when required for investigative purposes. However, the department does check the intrusion detection system logs on a daily basis.

The facts above indicate the department takes a reactive rather than planned approach to managing citywide IT security risks. A more proactive approach would involve the use of risk assessments.

Risk assessments can be a key tool in assisting management with security planning by identifying the types of information handled and security required to protect it. Risk assessments normally consider data sensitivity, the need for data integrity, and the range of risks to systems and data. Risk assessments can help organizations to develop appropriate security plans to manage their risks. Best practice dictates that a comprehensive high-level risk assessment should be the starting point for developing or modifying any security policy or plan. Risk assessments should also be performed and documented on a regular basis or whenever systems, facilities, or conditions change.

The department does not have a comprehensive risk assessment for the city's IT resources and systems. It has not effectively used risk assessments to help identify the types of information it handles or the security required to protect it. Although the department's IT security

was assessed by both the 1989 Sungard Business Impact Analysis and the 2000 Lucent High Level Assessment, neither assessment focused on data sensitivity, the need for integrity, or the range of risks to its systems and data. The Lucent assessment looked at selected high-level issues of the city's information technology resources and system while the Sungard analysis presented an early version of the current disaster recovery plan.

As noted earlier, under the city's 1998 information technology master plan, each agency was required to perform its own risk classification to grade applications and documents by their importance to the agency, assess the potential harm if data or programs were destroyed, altered or stolen, and assess the agency's degree of exposure should it lose its valuable information.

When the plan was created, the IT security model used by the city was essentially decentralized. The 1999 mayor's directive then consolidated responsibility for all IT resource management to the department, thereby centralizing it. However, the practice of delegating risk assessments to agencies has persisted into the 2003 citywide security policy despite the department's supposed centralized management. This has created an inherently disjointed management situation.

Since an agency does not manage the technical function, it is exposed primarily to operational risks such as non-compliance with the security policy, rather than actual physical risks to the system. These risks are managed by the department, which has centralized technical and physical control of nearly all primary resources relied on by the agencies. Although it may be instructive for the department to know about operational risks faced by agencies, the ultimate risk to the city is on the systems and resources that support agency operations. Agencies have no control over these risks, and they have not been assessed by the department.

The department has not linked individual security guidance pieces into an effective citywide security planning and management program

Although a variety of IT security framework documents exist, there is no overall framework linking them into a single citywide program of security planning and management. Most of the security documents are stand-alone and do not relate to other guidelines.

The department does not have a comprehensive plan that describes its overall security program for the city. It does, however, have a citywide

security policy (rather than plan) and an issue-specific Internet usage policy. We acknowledge that the security policy effectively delineates generalized responsibilities and expected behaviors. However, neither policy specifically identifies a) the major systems and facilities it covers; b) who is responsible for their security management; or c) who owns, uses, or relies on particular resources and systems.

Other assessments have made similar findings. The 2000 Lucent assessment found that the city did not have a security plan and that foundation planning for the city's IT security framework was patchwork. Without updated planning, Lucent said there was a danger that policies created by the department will continue to reflect their particular (technical) focuses, causing general, non-technical, responsibilities to be deferred to departments and users who lack the appropriate guidance as to how to fulfill those responsibilities. These criticisms are still relevant today.

Lucent's finding was based on the idea that every organization should have an overall security plan so that individual policies can be consistent under a single framework. The security plan should flow from the city's strategic business plan and provide the foundation for citywide security policies and procedures. The plan should be a comprehensive document at a level higher than specific policies, such as Internet usage.

Under Mayor's Directive 99-1, the responsibility for such a plan is held by the city's chief information officer (CIO) who is the department's director. The CIO is also responsible for developing security management goals and objectives; identifying metrics to measure progress; and ensuring all IT plans are consistent with the business needs of the city.

As for foundational planning, we found that the IT master plan has not been updated since 1998 and probably reflects a decentralized IT management style no longer employed by the city. In addition, the city's strategic IT plan was last updated in 2004 and makes no mention of security; and as discussed above, there is no security plan. Therefore, the foundation from which to build security policies, procedures, standards, guidelines, and regulations is inadequate because of lack of updates and focus.

Unguided by measurement criteria or planning guidelines, it is unclear how the department can evaluate management results versus city business needs and purposes. It would be difficult, if not impossible, to

evaluate the current effectiveness of the security program. Without a security plan linked to other foundational documents, there is no way to ensure that any given security implementation is aligned with the city's overall IT security strategy.

The department lacks sufficient authority to effectively manage a citywide IT security system

The department was designed under the city charter to fulfill a technical and expert role in operating most of the city's IT systems and resources. Mayor's Directive 99-1 clarified this general role by assigning to the department the overall management of citywide IT systems and services, including planning and measuring IT achievement and implementing a security system with procedures.

However, the directive also effectively divided the policymaking and technical monitoring responsibilities from the enforcement responsibility. While this reinforces the charter's vision of the department as a technical support agency, it does not provide the department with the authority necessary to manage its overall responsibility as assigned in the 1999 directive. Furthermore, the citywide security policy created by the department in 2003 confirms this division but does not establish authority to comprehensively oversee the effectiveness of the city's IT security management program.

Current administrative guidance divides policymaking from monitoring and enforcement responsibilities

Under Mayor's Directive 99-1, overall management responsibility of the city's IT systems, resources, and data belongs to the department. The department also has the primary policymaking responsibility. Agencies are responsible for developing and implementing adequate security procedures consistent with overall city security policies. Agencies are also responsible for enforcing overall policies at their local sites. The heads of non-city organizations are responsible for ensuring their own compliance.

The department has complied with the 1999 directive by setting up a framework to manage the city's IT services and creating security policies and procedures to be enforced by the agencies. However, under this system, the department is only responsible for creating a framework of documented policies but not for overseeing or enforcing that system. There is no oversight other than what agencies may self-impose.

Because it has limited ability to enforce its policies, the department's power to fulfill its mandate is limited by the level of compliance of

individual end user agencies. In addition, the bulk of responsibility for implementing the security framework falls on agencies rather than the department. Though it has overall management responsibility, the department plays only a supporting role rather than an enforcement or oversight role. This situation of responsibility without authority is primarily due to the division of policymaking from monitoring and enforcement roles created under administrative guidance.

The department relies on agency and user compliance to manage citywide IT security

Under current policy, agencies play the most significant role in monitoring and enforcing the citywide security policy. They must ensure compliance and enforce the policy and guidelines, including disciplining violators. They must also develop their own guidelines and procedures, which they must submit to the department for review. However, there is no guidance regarding regular monitoring or how to manage this responsibility.

An important omission in the current security policy relates to the coordination of management between the department and agencies. The current approach relies on self-monitoring to ensure compliance. Agencies must monitor themselves for compliance with security policies; however, the department's Help Desk has never received any security violation reports from them. Feedback on how to improve the policy is provided on a voluntary basis. At the time of our audit, none of the departments had developed their own policies or guidelines for the department to review.

Under such a self-monitoring regime, a key to effectiveness would be to provide agencies with administrative guidance and training on responsibilities and obligations. Without this, agencies are left to their own discretion in enforcing and monitoring compliance. Such discretion precludes uniform management of security policies and promotes variance between agencies. As agencies must currently assess their own security policy compliance and management but need not report these results to anyone, the department does not know how effectively the policy is being managed by each agency.

Within agencies, security liaisons are the interface between the department and the agency for the current security policy. Liaisons are to report attempted, actual, or suspected violations of the security policy to the departmental Help Desk. Liaisons are also to disseminate IT security related information to their agency users. Although they are to

report violations, there is no role for regular monitoring by agency liaisons. As a result, reporting occurs only when liaisons become aware of violations. No security violations have been reported to the Help Desk by liaisons under the current policy.

As with the agencies themselves, the key to effectiveness with this type of liaison system is to make sure officers are aware of their responsibilities and obligations by providing adequate training. Without such, liaisons are free to report what they like and must rely on the good faith reporting of end users to accomplish their responsibilities.

Finally, agency users are expected to monitor themselves with respect to compliance with security policies and their use of authorized software. Users play a supportive role in reporting security policy violations to their security liaisons. As identified above regarding both agencies and liaisons, the key to effective monitoring by users is administrative guidance and training related to responsibilities and obligations. Without this, users are similarly left to their own discretion and good faith to comply with security policies.

The department does not provide sufficient training on responsibilities and obligations to justify their delegation

There is no training program on responsibilities and obligations under the current security policy for agencies, security liaisons, or end users.

Although the role seems very important, there is no formal training for departmental security liaisons. Similarly, no training is provided for agencies. Agencies were given an informational presentation on their responsibilities when the policy was first implemented.

For end users, there is likewise no formal orientation or training. There is, however, a short video for users regarding the security policy located on the city's CityFYI web pages. We tried to access this video but were unable to because our standard configuration for Windows Media Player lacked the necessary technical software compatibility to play it, it is likely others experience difficulty accessing the video, too.

We also noted from CityFYI that users are backed into acknowledging reading the security policy and complying with certain security policy rules as part of the terms of use of the city's web-based electronic mail. Relying on user compliance is inadequate as a primary security strategy. Altogether, we believe the department does not provide sufficient training

to justify delegating external security responsibilities to agencies and end users.

Physical and Environmental Controls Are Inadequate to Effectively Protect Key City IT Systems and Resources

Most critical city IT systems and resources are located at the data center in the Honolulu Municipal Building, where important functions such as city check production occur at various times. We noted that the department has known of significant physical and environmental control issues that can impact IT systems and resources. However, apart from seeking temporary maintenance, the department has not sought nor coordinated solutions with other departments who resolve those issues. The department has also shown a relaxed attitude regarding data center access practices and entry monitoring.

Data center access practices are inadequately managed

The department believes there have been no adverse physical access events and that only people with legitimate business purposes access the center. Given the importance of the room as a site of key IT resources and systems as well as check production, current management of the access control system and review of access logs is very relaxed. Card issue is nearly universal within the department, is not in relation to actual access needs, and there are notable issues related to safekeeping the cards.

Almost every departmental employee is issued an access card, with minimal regard to actual need

Virtually all staff are issued card keys to the data center, even if they rarely need to enter it. A list of departmental employees showed that of 137 staff members, 128 have been issued access cards. Of these, 25 employees have access to the front door of the data center (green); 67 have access to the front door and the computer/control room doors (blue); and 35 can access all controlled doors in the data center (red).

There are also eight visitor passes, seven of which have blue level access and one of which has red level access. According to the department, the red access visitor card was needed by a maintenance person during a project, but was not returned to its original blue level access, after the project's completion. The department has since re-programmed the maintenance worker's security access.

We conducted a survey to gain an understanding of users' perceptions and experiences of the department's data center access control card

system. The survey also tested the validity of internal control rules and the accuracy of internal control logs related to the system.

We surveyed departmental users of the data center to determine:

- How widespread issuing of access control cards is;
- Whether users knew of control information that could help validate internal control rules and logged information;
- Whether users knew what conceptual and/or actual access they had to the data center;
- Their experiences with using a card system regarding possession, safekeeping, lending, loss, and replacement; and
- Frequency of user access to the data center.

We also attempted to determine whether:

- Logged information relating to users is maintained;
- Access rules are followed in issuing access;
- Access rules are followed for managing access;
- Rules have been updated and revised to reflect personnel or organizational changes;
- Rules have effectively managed certain aspects of user experience; and
- Access system rules or practices make sense in light of the number of users granted access.

We sent a survey to all 135 employees on the current departmental roster. A sample of the survey and our covering email message is provided in Appendix A. We received 114 responses. The completed surveys were compared with departmental control logs and rules to assess whether there is general compliance with existing guidelines and

procedures, and to assess user perceptions and experiences related to the issues above.

Survey responses showed that 54 employees access the data center at least once a week, while 52 access the center only monthly or less. This division in access patterns could easily serve as a guideline when issuing access cards in future. Operations staff who work in the data center and a small proportion of other staff that have regular service or maintenance duties require cards to access the data room. Remaining cardholders should have their access levels re-evaluated.

We concluded from this survey that the prevalence of issuing cards does not appropriately reflect the levels of access or frequency of use required by users throughout the department, and therefore incurs unnecessary exposure to security risks. Access guidelines and management practices should be revised to focus on actual requirements in order to maintain data center security.

Except for card issue and establishment of initial privilege level, there is little management of the card system and its related rules

Our survey also showed that the security access card database appears to be well-maintained and highly accurate with respect to employee information, card numbers, and privilege levels. Of the two instances where the system log showed inaccuracies, one was an employee whose access was recorded but not his card number; the other was an employee who had started work in May 2005 and whose name and card number had not been logged as of July 2005. The log's general accuracy was also confirmed by the fact that of 13 survey respondents who had their cards replaced due to loss, all 13 replacement card numbers were confirmed on the log.

However, we did note some problems with the card system's internal management controls. The department's *Security Card Access Guideline* outlines criteria for determining staff access levels. The guideline does not state who is to make this determination, but we wanted to find out if users knew what level of access they should have. Most staff did not know, including prominent departmental managers. We discovered that when employees are issued cards, they are verbally informed of their privilege level. Since nearly all employees surveyed were able to correctly identify the doors their cards could open, it appears that the practice of verbally informing employees which doors their cards can open is more meaningful than the system of color-coding access privileges.

There were also significant problems with logged access conforming to access rules. For instance, there are notable gaps in access guidelines, such as how to determine privilege levels for those in Planning and Administration or the Directorship. We found several instances of employees holding cards that do not conform to existing guidelines. These generally related to inconsistencies such as employees who transferred internally but did not have their cards changed to the appropriate privilege level; and recently re-organized sections/branches like the Systems and Database Administration Section, which did not have its staff's privileges changed (or the rules were not changed to accommodate their need for access).

Although the guideline provides criteria for granting access, it does not specify who makes the determination, who manages or maintains the system after issue to ensure appropriate access levels are assigned, or who updates the guidelines to ensure access levels reflect current organizational needs. We understand that control of the access system has fallen to the Operations Division by default because it is located in the data center. However, there are no directives to help the division in managing the system.

Other aspects of the system that were problematic related to the safekeeping of cards. First, we are not aware of any current management or direction regarding protection of cards. Previously, employees were asked to sign an acknowledgement form to document that a card had been issued, but this practice has been discontinued.

Second, there are no guidelines regarding where cards should be kept, whether and how to secure them, or whether employees are allowed to lend or share their cards. It is left to the employee's discretion in each of these areas as to how they secure the card.

Third, there are no formal loss or replacement policies. Employees who lose cards are simply issued with new ones and the lost cards are deactivated. There are no criteria governing whether lost cards should be replaced. The effectiveness of this system relies on employees being aware of having lost their cards and making a timely report to the proper person so they can receive a replacement and have the lost one deactivated.

Of 106 employees surveyed, 15 had lost their cards. The Operations Division has lost more cards than the other divisions combined. This may be because management of the system is located in the Operations

Division and therefore knowledge about replacement cards is more widespread. Or it may indicate a level of abuse of the system, because employees are aware of how easily lost cards can be replaced. We noted that two lost cards have not been replaced; the Operations Division employee in charge of the system has stopped issuing replacements until the results of this audit are released.

Although virtually every employee we surveyed who had been issued a card reported that they actually possessed the card, there may have been occasions when employees were aware of losing their cards but because they did not need to access the data center did not inform anyone of this. Some survey respondents commented that they know they can enter the center without using a card and therefore store their cards elsewhere. In the absence of guidance on how employees should secure their cards, we found that cards are kept in various ways and in a wide variety of locations.

The security implications of employees using and storing cards at their discretion are significant. Cards could remain unaccounted for for a significant period of time and potentially be used to gain unauthorized entry to the data center. In addition, access card issuance may need to be reassessed if employees are not finding it worthwhile to use their assigned cards to access the center. Given the importance of resources secured at the data center, the potential for access cards to be left in unattended locations such as at home, in unlocked desks, or in unattended personal effects like bags or in cars could be serious.

Furthermore, there is no guideline prohibiting employees from lending their cards to others. Survey results showed that only 5 of 106 employees allowed someone else to borrow their cards. However, two of those five had residual red (high level) access remaining from inter-office transfers.

The Department of Facility Maintenance manages the Kapolei Hale facility. However, the Department of Information Technology has not established access control rules for this room, as it has shared control over the facility. In addition to information technology personnel, Department of Facility Maintenance staff and security personnel also have access to the keys to the data center.

In addition to being a disaster recovery and information technology support facility, the data center room houses telecommunications facilities and other cable-related facilities for Kapolei Hale. Vendors for these

facilities can gain access to the room either by being escorted by departmental personnel or Department of Facility Maintenance security staff. Given the multiple uses of the Kapolei facility, there is a risk that the information technology department would not be made quickly aware of non-departmentally escorted entries into the facility or harmful activities at the site.

Logged activity is not regularly monitored or reviewed

No adverse access incidents concerning the data center have been reported by the department. However, this may reflect the current relaxed attitude regarding the review and monitoring of access logs. We found that access entry logs created by the system are not monitored or reviewed on a regular basis. Inspection of the logs only occurred after something happened to warrant such review. Visitor logs are collected, but only held for two to three months.

Management believes that most employees do not exceed their privileges or abuse the system. We were told there is an informal system such that if an employee is discovered using keycards or accessing something inappropriately, the person in charge of the card access system will discuss it with the offending employee and escalate the action taken as necessary with a supervisor or division chief. Occurrence of this was characterized as rare.

The Kapolei Hale facility is managed by the Department of Facility Maintenance which contracts with a private security company. The telecommunications room is within the vicinity of business hours security patrols, but these patrols are designed to patrol the area in general and are not tailored to look for specific activities that may jeopardize information and technology department assets within the room.

The private security company keeps logs of its patrols. The manager for security told us he could not recall any instances where suspicious activity had occurred related to the data center. The information and technology department does not coordinate with security to be informed of suspicious activities.

Physical and environmental control issues have not been effectively addressed

The data center faces known physical and environmental control issues that may jeopardize its IT resources and systems. The center's location in the basement of the Honolulu Municipal Building makes it subject to water intrusion. There are known problems with environmental control measures related to fire suppression and cooling. The data center has

few physical security measures beyond its access card system, and key access points are not physically secure or monitored by security cameras.

The data center is subject to water intrusion

The data center is located in the basement of the Honolulu Municipal Building. Several of the employees we interviewed noted the data center has historically experienced water intrusion whenever there are heavy rains or the landscape above is over-watered. There are a number of points where water intrudes into the data center and the department has resorted to measures such as an indoor rain gutter and protective tarps to prevent water damage to resources.

Some building occupants suspect that when the offices on the first floor breezeway were enclosed some of the drains were covered up, causing water to intrude unpredictably into the basement. Some leaks are predictable, such as the area where an indoor rain gutter has been installed and a sealed crack in an area where critical resources are located (known as the dark room). Exhibit 2.1 is a photograph of the indoor rain gutter.

Exhibit 2.1
Photo of Indoor Rain Gutter in Data Center

This indoor rain gutter was installed in the dark room to catch water that seeps in from between the ceiling and wall.

At another known point of leakage, a rudimentary water detection system has been developed by inserting paper towels between the wall and the roof. Exhibit 2.2 shows the paper towels stuck in the ceiling.

Exhibit 2.2
Photo of Paper Towel Water Detection System

Paper towels placed between the ceiling and wall in the dark room are used to indicate when water is seeping in.

Employees monitor the dampness of the paper towels and report any wetness to the Department of Facility Maintenance. In a memorable instance several years ago, water dripped onto some disk control units and the mainframe, causing damage to the disk controller and loss of space on the disk due to acid in the water. The tenant next door, Oahu Civil Defense Agency, has experienced similar water intrusion and equipment damage.

The department has discussed this situation with the Department of Facility Maintenance; when called, maintenance staff tries to seal the leaks. Currently there are no maintenance employees dedicated to the Honolulu Municipal Building, making timely remediation of leaks or applying preventive maintenance more difficult. Since the data center

runs 24 hours a day, seven days a week, center personnel are asked to check for water intrusion on a daily basis.

Fire suppression may not be in working condition

There are five gas-based fire extinguishers in the data center. There are eight sprinkler discharge points in the computer room, seven in the dark room, and two in other areas of the center. The system is activated by smoke or heat and is maintained by a vendor contracted by the Department of Facility Maintenance. The system is inspected by the vendor twice a year. Initially there were also four handheld extinguishers, but one is currently missing.

The Honolulu Fire Department inspected the data center recently and cited the department for the front tank extinguisher because it lacked a service tag. As the vendor for the tanks had just recently made its own inspection, the department inquired about the missing tag. The vendor revealed the department had not passed its inspection either, but failed to communicate this at the time. The vendor promised to return and correct the deficiencies.

A fire occurred recently because a faulty air conditioning heating element caused the floor to smoke. The fire suppression did not work to put out the fire, but luckily there was no resulting damage.

Air conditioning failures are problematic

The Department of Facility Maintenance maintains the data center's air conditioning units, which have experienced problems in the last year due to their age. The facility maintenance department has advised the information technology department that most of the recent repairs are merely temporary solutions and replacement would be a better course.

The data center is served by two air conditioning chillers in the basement. In the event of a basement failure, chillers on top of the building can be used as backup for the basement units. Problems with the air conditioning system are known and not unusual. Even during our site visit, one portion of the data center was noticeably warm; we later discovered the system had required maintenance for three days including the day of our visit. The department is under the impression that the facilities maintenance department is planning to replace the entire building's air conditioning system. As a stopgap measure until that happens, the department has purchased four cooling fans, which appear to be effective when used during air conditioning failures.

The center's informal protocol is that whenever the temperature in the dark room reaches 85 degrees or more, IT systems are powered down. The last time this occurred was in February 2005 (six months prior to our audit work).

On one occasion before the heavy duty cooling fans were purchased, the department had to purchase household-grade fans and borrow fans from employee work spaces following a late-night air conditioning failure. As a result of that failure, rising temperatures forced the department to shut down non-critical servers. Some hard drives and memory have failed as a result of such cooling failures. However, to date, the department has not had to shut down any major or critical resources due to cooling failures.

Some entry points appear insecure

As noted above, most of the significant access points to the data center are controlled by card key. However, there are a few vulnerable locations. For instance, in the visitor entry area there is an open space about waist high through which an adult could easily gain entrance to the operators' area. This opening was a remnant from plans to provide a handicap access ramp that was never built. Exhibit 2.3 shows this opening in the visitor entry area.

Exhibit 2.3
Photo of Opening in Visitor Control Area

There is also a sliding metal partition used to close off the security window area entirely, from roof to floor. This partition covers the open space noted above. However, we heard conflicting reports as to when the pull down partition is used. Employees variously reported the partition is used rarely; during weekends or late at night; or whenever city checks (including general, payroll, and Section 8 checks) are being produced.

The data center delivery door opens onto a shared hallway in the basement. After entering Honolulu Municipal Building, there is no significant barrier to access to the basement level and this hallway. The delivery door is an older double door with glass window panels (taped to obscure the room) that is kept locked at all times and secured by a card swipe access point. There is a noticeable gap between the doors where the locking mechanism could be forced, and some employees are concerned it is not secure.

There is also a service elevator to the basement. The entire basement is shared by the information technology department, the Honolulu Fire Department call center, and Civil Defense. The information technology department was provided with only two elevator keys, which are generally used for vendor deliveries. Occasionally, vendors and others are escorted down the elevator unbeknownst to the department. This could be problematic, as the hallway from the elevator passes the center's delivery door noted above.

The center itself has only one security camera for the visitor area. There are plans to install more cameras at access points in the center itself and at the delivery door. However, employees noted that existing building security cameras are currently not monitored; nor are the environmental sensors for building air quality.

Further issues related to the Kapolei computer room

In addition to the security issues regarding the multi-purpose character of the Kapolei Hale room, there have been load failures (when the two chillers run simultaneously) that have prompted alternate operation of each chiller individually. In the event that the operating chiller shuts down, an alarm is triggered. However, the alarm sounds only within the room; because the room is mostly unattended, there is a risk that climate control problems could remain unidentified for a significant period of time.

This system relies on passing Department of Facility Maintenance personnel to detect the sounding alarm and take appropriate action to activate the other chiller. Instructions for this process are on a crude handwritten sign on the door. Consequently, there is no fail-safe method of activating the backup chiller should a failure occur.

In addition, there is also no uninterruptible power source for the room. This creates a power management issue for the room's equipment. There is a current project to install an uninterruptible power supply, which is scheduled to be completed before the end of 2005.

The department has not proactively pursued durable solutions to known physical and environmental concerns

There are two factors delaying the department's resolution of known physical and environmental concerns. One is control of design and maintenance; the other is the department's lack of initiative in solving the problems in-house or coordinating with other departments to ensure permanent solutions to these issues.

Disjointed responsibility contributes to a lack of implementation of appropriate controls

The department's systems and resources are housed in facilities controlled by other departments, notably the Department of Design and Construction and the Department of Facility Maintenance. As such, the design of improved access and other physical controls is not directly under the department's control; nor generally is the maintenance of existing facilities. Although the department has consulted with the above departments about improvements to physical controls such as the access control system and air conditioning, their implementation is not under the department's power. However, the department recently indicated that the Department of Facility Maintenance has delegated the review of certain citywide physical control project proposals to it.

The department has sought only temporary solutions to known problems

Lacking control over the design or implementation of improved access and physical controls, it is understandable that the department uses existing means to secure maintenance to its physical and environmental controls. However, it is problematic that solutions to known recurring environmental control issues such as water intrusion and the air conditioning have not been either meaningfully coordinated with controlling departments or resolved in-house through budgetary or negotiated service measures.

The Department Manages Normal Backup and Recovery Requirements Adequately But Disaster Recovery Planning and Implementation Is Lacking

The department effectively manages routine backup and recovery requirements according to its defined policies and related activities. In most instances, the current system appears effective. However, there are notable issues related to disaster recovery planning and implementation that may jeopardize service continuity and availability for the citywide system.

The department manages its routine backup and recovery duties reasonably

Procedures and related regular activities are in place for backing up servers, mainframes, and databases. A program exists to regularly back up city computer files and store copies securely at an off-site location to minimize service disruption. The current program is successful in effectively backing up and recovering data for routine business needs; and this is due, in part, to automated scheduled backups of mainframe and Windows servers to electronic vaults.

Computer files are regularly backed up and stored at a secure off-site location

Procedures are in place for regularly backing up servers, mainframes, and databases. Backup files are created on a daily and weekly basis. Most network backups and the mainframe backup are automatically stored in tape vaults in the data center and at the offsite Kapolei location on a daily and weekly basis.

Daily tapes used to be stored offsite but are currently being stored in the Civic Center parking garage. Previously, daily tapes were taken each morning to the Honolulu Police Department at Alapai Street, where they were stored in a minicomputer room secured by an access control card key. The card, however, recently expired and has not been renewed because the police department is reviewing continuing authorization. Weekly tapes are taken offsite to the Kapolei storage facility every Tuesday.

This system ensures that most disruptions are correctable from daily tapes, although the weekly set is occasionally retrieved from Kapolei. The staggered approach to backups means there are usually several

incremental daily backups available prior to a full week's backup. Weekly sets are available in turn prior to monthly backups.

Physical protection of backup copies is also an issue. Previously, daily tapes were stored about half a mile away from the center at the police department. This distance facilitated tape drops but was not so near as to be affected by an event specific to the Honolulu Municipal Building. However, it would be affected by any citywide power outage or common natural disaster such as an island-wide storm.

The current daily tape storage location, in the municipal building's parking garage, does not offer this protection. Although it is a dedicated storage space for the department and is located adjacent to the municipal building, it is near enough to be affected by any building-specific event. It would also be affected by a local power outage or other disaster such as a storm.

In the event Honolulu Police Department storage room access is not renewed, the department will need to find another viable daily storage site because the parking garage location is not far enough away from the data center to protect against loss caused by the same event. The department has been warned in a previous review that its practice of storing tapes in the municipal building parking garage is not distant enough to protect against impairment.

The weekly tape storage site at the city's Kapolei Hale office complex is located 21 miles away from the data center. This is far enough to not be affected by a building-specific event or by a city-wide power outage. The site would still be likely affected by an island-wide disaster event, however.

There have been very few memorable user recoveries under the current system

Contact personnel for key servers reported no problems with the current backup and recovery system. Most indicated they are not involved in the backup process itself; they primarily coordinate backup and restoration issues for users. They reported that restoration of data is usually accomplished without incident; on rare occasions a recovery has to be made from Operations Division tapes or from tapes retrieved from Kapolei.

It appears that the centralized responsibility for backup and recovery, supplemented by automated scheduled backups, is efficient and effective for meeting current business needs.

Some aspects of routine backup and recovery require future management attention

As noted above, the daily tape drop site is probably too near to Honolulu Municipal Building to be used as a permanent site for daily backup storage. If the Honolulu Police Department site cannot be reauthorized, another location should be chosen.

Another issue relates to mainframe backups. At present, the department is able to recover mainframe data, but it takes 48 hours to return to useful processing again. More equipment, including updated communication, storage, and mainframe equipment could make this process more efficient, so that the department could lose only 3 to 4 hours instead of 48. Pending budgetary approval, the department plans to acquire the necessary equipment within the next 8 to 12 months.

Similarly, the age of some equipment was also cited as a barrier to upgrading to more effective technology. The reliance on out-of-date hardware or software, which is no longer supported by vendors, is a related problem that creates maintenance and efficiency issues in this area. Some interviewees voiced concerns that the limited problems experienced with backups and recovery were caused by bad tapes, recovery time required not timely meeting business productivity needs, or other problems with current technology applied.

Finally, we were made aware of a growing backup window which is the time required to complete a backup on the server side. Some of this may be attributed to unnecessary back ups, in which case guidelines could be improved to help determine what should be backed up, what should be kept current, and what should be archived. Likewise, increasing user awareness of how their file maintenance affects backups could improve the efficiency of backup and recovery operations.

The department has not effectively managed its disaster recovery and contingency planning responsibilities

The department has a comprehensive contingency plan for citywide IT systems and resources, known as the disaster recovery plan. This plan focuses primarily on mainframe and critical applications recovery. Under the existing plan, there is no client server recovery strategy; however, one is being drafted.

Mainframe recovery testing has also been successful. The department is fairly confident it can meet its internal requirement that mainframe data be recoverable within two days. Critical servers have been tested successfully by the department's Applications and Technical Support Divisions for setting up a base system. However, we did note several problematic issues in this area.

Notable weaknesses related to the current state of disaster recovery planning exist

The department's disaster recovery plan is founded on a business impact analysis conducted in 1989. In the intervening years, responsibility has been passed to city agencies to conduct their own business impact analyses and risk assessments. To date, neither the department nor agencies have conducted a risk or impact analysis that would align with current conditions. Furthermore, the prevalence of client server/local area networks in use warrant assessment as to their risk, business impact and continuity, and incorporation into the city's disaster recovery contingency plan.

There currently is no operative strategy for testing client server/local area network resources, which may total as much as half of the city's IT systems and resources. In this respect, current service continuity and disaster recovery plans are blindly facing uncontrolled risk exposure to these resources.

During the most recent mainframe database recovery testing period, tests were performed within a modified 48 hour (the two day requirement) timeframe to accommodate a standard work day, and did not incur staff overtime. However, the department's testing report summary notes that an actual 48 hour test should be performed in the future to simulate disaster conditions.

We noted that the modified 48 hour time frame actually covered six working days. There were also instances of human error which, while unavoidable, has a foreseeable impact and may be magnified under the pressure of a real-time test.

Furthermore, off-island technical support that was unavailable during the test period is problematic. Aspects of the disaster recovery plan that require after-hours support should be reviewed and documented beforehand to mitigate delays in a test or actual disaster scenario. Also, since the department manages a few resources used by other counties and the state government, testing, maintenance, reconciliation, and

coordination should be made mandatory since one county recently opted out of a testing exercise.

Priority of recovery is another important issue. We were provided with a list indicating the order of emergency processing priorities among city entities. These priorities, however, have not been coordinated with agencies. The department's director acknowledged this gap, noting the department does not know agencies' own priorities in the event of loss and there are no criteria on which the department can judge its service and support to agencies. The department believes full mainframe recovery is achievable in the event of a loss, but except for one server there is no way to reconcile whether this has occurred under the current plan.

Space and travel time were not considered in the recent testing. The testing summary acknowledged some recovery functions and testing were done remotely; however, during an actual disaster, it is anticipated that recovery and command center space would be required. The summary mentions that the department has requested space at Kapolei from the Department of Facility Maintenance, but no decision has been rendered on the request.

The support site issue is problematic. The department plans to use sites at the police department on Alapai Street or at Kapolei Hale to support disaster recovery command or recovery. However, the department has not been in contact with the police in a few years to confirm its availability as a command center. The current disaster plan approaches this issue as an as-needed rather than a supported contingency. The Kapolei site also faces support site issues described more fully below.

Most functions in the plan are meant to be carried out by Honolulu Municipal Building-based personnel

Most duties and functions under the current recovery plan are intended to be carried out by Honolulu Municipal Building-based personnel. In the unlikely event that the Honolulu Municipal Building is destroyed during business hours, there would be very few employees remaining to implement the plan. This is a key vulnerability as there is no currently-staffed second site.

Furthermore, there is also a concern about employees' awareness of their functions. The plan provides general rather than specific duties, so it cannot be used as a checklist regarding key duties. We noted that during the testing one staff member could not fulfill his planned function

because he was not involved in the daily process related to those systems and did not know how to carry out the specific tasks required of him. This impacted the test results. Although there were no other such instances during the testing, it raises a concern that staff must be not only physically available but appropriately trained for and aware of their responsibilities.

Kapolei site is not fully suited for recovery or command activities

The Kapolei site is not adequately suited to serve as a recovery or command center in the event of a disaster. For instance, it does not have an uninterruptible power supply; and there are connectivity issues that make it unsuitable for some required activities in the plan. Its biggest issue is that it lacks appropriate space to conduct command and recovery functions. As there is no official agreement between the information technology department and the Department of Facility Maintenance on this subject, there is no guarantee more space or other availability issues will be addressed.

Insufficient support exists to implement an effective disaster recovery program

The disaster recovery coordinator indicated to us that to date, disaster recovery has been paid *lip service* only; and that the coordinator's position is one of responsibility without authority. Previous disaster planning initiatives have been under funded, and disaster planning is treated as secondary to daily production work.

Two primary issues have emerged regarding support for disaster planning. First, the previous administration was primarily concerned with higher profile and public relations type initiatives and accomplishments rather than disaster planning. Second, previous management and some members of current management have been unsupportive of current disaster planning efforts.

Previous administration was primarily concerned with high profile and public relations activities

Previous management was quite critical of the disaster planning program, and though the program was given priority in reports and budgets, in practice it was subordinated to other more visible projects. Not all previous management believed in the philosophy of disaster recovery and this has been reflected in budget cuts and a lack of funding and overall support. Previous departmental leadership was primarily concerned with high profile and public relations type initiatives and accomplishments and actively redirected and reprimanded staff who worked on disaster

recovery initiatives. There were also conflicting directives, as the same leaders told disaster recovery staff they would be personally liable for any recovery failures. However, the current department director appears supportive of disaster recovery planning and initiatives.

Disaster recovery coordinator has responsibility but no authority to accomplish disaster recovery planning

The department's disaster recovery coordinator has the responsibility to set up and execute a disaster plan, but not the authority to enforce compliance with planning objectives. The coordinator's position within the Operations Division means that division chiefs can effectively ignore requests for information and support. Some division chiefs have avoided participating in disaster planning by delegating this duty to subordinates; the chiefs then pleaded ignorance of the plan or planning process while criticizing the final planning document. Some key management personnel are allegedly not only vocally unsupportive, but actively work to undermine disaster recovery activities.

We noted that the disaster recovery coordinator position has been moved several times within the department's divisions. Following a recent reorganization, the coordinator is no longer included in operation division supervisor meetings or executive management chief meetings.

Disaster planning initiatives have also been under-funded. This is due in part to lack of management support as discussed above. The coordinator has had to resort to requesting funding for minimal but important initiatives such as more backup drives, additional firewalls, and additional servers. The coordinator has also requested and been refused training for several years, resulting in personal maintenance of her relevant certifications, and was not reimbursed for keeping her certifications current.

Disaster recovery planning has not been awarded the appropriate level of internal departmental priority. Meetings are scheduled on an as-needed basis. Even when scheduled, meetings are often cancelled because attendees' priorities are to attend to daily work rather than planning meetings. Disaster planning work is treated as secondary to daily production work. As a result, the coordinator has "worked around management" and "worked directly with staff" to achieve planning objectives.

Despite these challenges, the disaster recovery coordinator has been effective in producing a fully updated and comprehensive disaster

recovery plan regarding mainframe resources; overseen the successful recent mainframe testing; successfully coordinated with two of three neighbor island counties to move towards statewide testing; and obtained commitment and funding to plan client/server environment recovery protocols.

Conclusion

The Department of Information Technology is responsible for managing the city's information technology systems and services. This includes ensuring proper security over systems and resources and providing for the availability of key resources, systems, and data for city business needs. We acknowledge the technical successes of the department in maintaining and effectively operating its aging systems and resources, and providing effective technical security and substantial support to government services countywide and in some instances, statewide.

Our review of selected information technology control issues focused on the citywide security management structure, controls applied to protect key resources and systems, and measures to ensure availability of information technology resources for current business needs.

We found there are inadequacies related to the oversight and authority of the department to provide appropriate management of the current city information technology security framework. These shortcomings can be addressed by undertaking appropriate revisions to foundational planning and policy documents, and by the department taking an expanded oversight role commensurate with its citywide management responsibility for these systems. Currently, the department overemphasizes its traditional technical support role and defers monitoring and enforcement to agencies and users. The department should coordinate agencies' management results to improve its security of the citywide information technology system, and allow for agency and user feedback in its management.

Our review also found that there are issues concerning access control practices and environmental controls for the data center. We found that management of physical access to the data center is too relaxed and stems from the assumption that because no adverse access events have occurred in the past, none will occur in the future. As a result, access is not restricted to reflect actual needs, and there is not enough management to maximize security within the current system including

reviewing access logs, managing the card system beyond card issue, and promoting safe keeping awareness among card key holders.

We also found that the department is aware of significant issues related to these physical and environmental controls. However, given the significant nature of the control issues related to water intrusion, fire suppression, and cooling failures, the department needs to seek more durable solutions to protecting the major information technology systems and resources in the center. We acknowledge that design and maintenance of these controls is beyond the powers of the department; however, the department has not effectively sought coordinated solutions or self-help measures to address these issues.

We also found that the department has a reasonable backup and recovery program in place which is effective for the routine business needs of the city, and acknowledge its success in this area. However, we did find that planning for disaster recovery of major IT systems and resources was lacking due to previous administration support, internal issues within the department, and lack of funding.

Though the current disaster recovery plan has been successfully internally tested in the mainframe environment, there are issues involving the current recovery plan. These include determining departmental requirements for service and support in the case of loss, developing service level criteria for business continuity and supported service, and understanding the city's exposure in the event of a major service discontinuity.

We realize that the changes required to improve these control areas will take a substantial amount of time, management dedication, external coordination with other departments, and appropriate funding. However, the city's current approach is one of service-oriented, business-driven, and cost-effective application of information technology. As such, these changes are necessary to meet the growing importance of applying appropriate information security controls to protect from threats to information technology service continuity and availability, minimizing potential damage, and maximizing the utility these systems can provide to public services and governmental operations.

Recommendations

1. The department should:

    a. Develop a comprehensive IT security plan that includes but is not limited to the creation of a functional management plan and an ongoing assessment process to ensure evaluation of the plan;

    b. Seek funding to facilitate a citywide risk assessment, including business impact and business continuity/resumption analysis;

    c. Clarify authority and lines of responsibility for citywide security management by appropriately revising key planning documents and policies, and working with the mayor and city agencies to resolve coordination, management, and oversight issues;

    d. Improve security for the data center by seeking funding for improved physical and environmental controls, and manage data center access to more accurately reflect actual access needs;

    e. Seek ways to further improve routine backup and recovery practices by acquiring funding for upgrading technology or media, and developing appropriate guidelines or other awareness programs to enhance backup and recovery effectiveness;

    f. Pursue an appropriate funding program for disaster recovery planning and required supporting elements, and provide an appropriate level of authority and priority to the disaster recovery function within the department; and

    g. Coordinate and seek agreements from external departments and agencies regarding supporting elements and services related to physical controls and disaster recovery planning.

2. The mayor should:

    a. Ensure the department receives the appropriate budgeting consideration for physical and environmental control priorities, improvements to backup and recovery, and disaster recovery planning; and

    b. Facilitate and guide discussions between the department and other city agencies to ensure proper coordination in support of

physical and environmental controls and disaster recovery planning requirements.

This page intentionally left blank.

APPENDIX A
Information Technology Survey Instrument and Invitation

Sample Survey Invitation - Email Message

As a part of the Audit of Selected City Information Technology Controls, we are surveying employees on issues relating to access card keys for the data center. May we kindly request your participation by completing the brief survey attached. Your participation and answers will be held confidential. As a part of the survey process, we may need to contact you by phone or in person to verify answers or to ask for further clarification. After completing this survey, please return it to wkawamura@honolulu.gov by Wednesday, September 28, 2005.

Thank you for your time and participation. If you have any questions or concerns related to this survey, please feel free to contact me at the email above or by phone at 692-5120.

Sample Survey Instrument - Form

Instructions for completion: For written answers, please complete your answer by typing in the space provided. After completing an answer, press TAB or use the DOWN arrow to move on to the next question or answer choice. If you need to return to a previous question or answer choice, you may use the UP arrow to move back to it. Where necessary, please check the appropriate check box by clicking on the box using your mouse pointer. After completing this survey, please save your completed document and return it to wkawamura@honolulu.gov by Wednesday, September 28, 2005.

1. Please provide the following background information.

Name:

Position Title:

Years with department:

Contact phone number:

2. Have you been issued a security card for the data center?

☐YES ☐NO

If you checked YES above:

If you know it, please provide the following information. It is not necessary to call around for the information if you do not know it.

Card Control Number: _____ Access Color: _____ ☐Don't Know

Which Doors Can Your Card Access?

☐Front ☐Computer/Control ☐Service Door ☐Don't Know

If you checked NO above:

Do you access the data center? ☐YES ☐NO

If YES to access, please describe below how you access the center.

_____

If you have not been issued a card, you have completed the survey. Thank you for your cooperation. The remaining questions are for those who have been issued a card.

1. Are you currently in possession of your card? ☐YES ☐NO

2. Where do you normally keep your card?

3. Have you ever let someone else borrow your card? ☐YES ☐NO

4. Have you ever lost possession of your card? ☐YES ☐NO

If you checked YES to lost card:

Has your card been replaced? ☐YES ☐NO

If you checked NO to replacement of the card, please briefly explain why not?

5. Please estimate how frequently you use the card to access the data center?

☐ Daily

☐ Once or a few days in a week

☐ Once or a few days in a month

☐ A few times per year

☐ Not in the last year

☐ Not at all

Thank you very much for your time and participation. If you have any questions or concerns related to this survey, please feel free to contact Wayne Kawamura at email: wkawamura@honolulu.gov or by phone at 692-5120.

This page intentionally left blank.

Response of Affected Agency

Comments on Agency Response

We transmitted a draft of this report to the Department of Information Technology on January 4, 2006. A copy of the transmittal letter is included as Attachment 1. The department submitted a written response to the draft report on January 19, 2006, which is included as Attachment 2.

In its response to our draft audit report, the Department of Information Technology expressed general agreement with most of the audit findings and recommendations.

The department acknowledged the need to improve security, backup, recovery, and disaster preparation, but noted the difficulty of working under funding and technological constraints that have precluded compliance with many common security management practices. The department views this audit as an opportunity to educate the administration and city council, and indicated its commitment to timely meeting these challenges in a fiscally prudent manner. The department agreed with the security management issues related to citywide IT security oversight, authority, and enforcement; improving the access card system; the need to improve disaster recovery; the need to coordinate and fund improvements to known environmental control issues; and the need to fund supporting measures such as risk assessments, monitoring, and required technology and media upgrades. The department indicated narrow disagreement on the issue of its overall IT security responsibility, stating that agencies should be responsible for IT security much like they are responsible for the physical security of systems and resources.

The department provided additional information clarifying aspects of the draft report, which as appropriate, were incorporated into the final report as additional information and stylistic changes, but did not substantively affect the report contents. The department provided us with a detailed organizational chart and a chart of the major systems under control of the department. These can be found in the department's response. As the department elected to respond to selected excerpts of the report, we offer the following comments to elements of the department's response requiring further explanation.

First, our report noted that "(d)epartments have been left to assess their own security needs, authorize users, create additional policies, and enforce all levels of IT policies". Though the department agrees in other parts of its response with the report's findings related to lack of oversight, authority, and enforcement, it disagrees in this instance, indicating that agencies should be responsible for IT security, much like they are responsible for physical security over IT resources present at their locations, and access to computer information. We concur with the department's position that agencies should retain physical control over resources in their location and that it is the individual agencies' management prerogative to determine access to data. However, our intent is to emphasize the overall management given the department's overall responsibility, which was found to be lacking in non-technical oversight, authority, and enforcement, rather than one of agency autonomy in IT implementation.

Second, our report noted that foundational planning elements such as the IT master plan and strategic plan for the city respectively were not updated or lacked appropriate security management emphasis, and thus the foundation for security management was inadequate. The department indicated that these were conflicting statements. We believe that the source of the confusion relates to the issue of whether the existence of the documents is indicative of the adequacy of the foundation. Our point was that the lack of updating or security emphasis of key foundational planning documents made the foundation inadequate. As such, we have made stylistic changes to improve the clarity of this paragraph.

Third, the department, commenting on its lack of authority to enforce security plans and policies on users, noted that its authority was complicated by semi-autonomous agencies that have access to city IT systems and networks. We concur with the department that per the city charter certain systems operated by semi-autonomous agencies are excluded from the department's control and oversight. However, we emphasize that this situation was recognized and that these systems were not included in the scope of this audit.

Fourth, we noted that at the time of audit, the authorization to continue to use the police department's computer room as a storage site for daily backup tapes was undecided, and if unresolved, posed issues for departmental backup storage given the department's temporary daily storage solution. We acknowledge that the department has renewed its access to the police department's computer room for daily storage of

backup tapes. We also acknowledge the department's completion of the uninterruptible power supply project at Kapolei Hale after completion of this audit's fieldwork, which should improve its suitability as a backup and recovery site.

Finally, we are encouraged that the department has committed to undertake some of the recommendations in the audit as part of its current planning initiatives to revise the Mayor's Directive on information technology, update the department's strategic plan, and to independently seek budgetary and coordinated solutions to the issues raised in the audit report.

ATTACHMENT 1

OFFICE OF THE CITY AUDITOR
CITY AND COUNTY OF HONOLULU
1000 ULUOHIA STREET, SUITE 120, KAPOLEI, HAWAII 96707 / PHONE: (808) 692-5134 / FAX: (808) 692-5135

LESLIE I. TANAKA, CPA
CITY AUDITOR

January 4, 2006

COPY

Mr. Gordon Bruce, Director
Department of Information Technology
650 South King Street, 5th Floor
Honolulu, Hawaii 96813

Dear Mr. Bruce:

Enclosed for your review are two copies (numbers 12 and 13) of our confidential draft audit report, *Audit of Selected City Information Technology Controls*. If you choose to submit a written response to our draft report, your comments will generally be included in the final report. However, we ask that you submit your response to us no later than 12:00 noon on Thursday, January 19, 2006.

For your information, the mayor, managing director, and each councilmember have also been provided copies of this **confidential** draft report.

Finally, since this report is still in draft form and changes may be made to it, access to this draft report should be restricted to those assisting you in preparing your response. Public release of the final report will be made by my office after the report is published in its final form.

Sincerely,

Leslie I. Tanaka, CPA
City Auditor

Enclosures

DEPARTMENT OF INFORMATION TECHNOLOGY

CITY AND COUNTY OF HONOLULU

650 SOUTH KING STREET, 5TH FLOOR
HONOLULU, HAWAII 96813
Phone: (808) 768-7684 ▯ Fax: (808) 527-6272 ▯ Internet: www.honolulu.gov

MUFI HANNEMANN
MAYOR

GORDON J. BRUCE
DIRECTOR & CIO

January 18, 2006

'06 JAN 19 P1 :48

C & C OF HONOLULU
CITY AUDITOR

Mr. Leslie Tanaka
Director/City Auditor
Office of City Auditor
1000 Uluohia Street, Suite 120
Kapolei, Hawaii 96707

Dear Mr. Tanaka:

SUBJECT: **RESPONSE TO CITY AUDITOR'S REPORT ON DIT SECURITY AND CONTROL**

General response regarding the access control card system:

The Department of Information Technology, expresses its appreciation of the Office of City Auditor's (OCA) audit of this department. Management and staff see this as an opportunity to further educate administration and council about the importance of Information Technology in the day-to-day operations of the City.

DIT acknowledges the need to improve security, backup, recovery, and disaster preparation. Under-funding in this area has made it difficult to comply with many common practices. Every effort has been made to work within these constraints. It should also be noted that the new administration detailed this area in the NEW Department of Information Technology Strategic Plan of calendar year 2005, and continued to document the importance of this issue in the revision of this plan in calendar year 2006, and revised Mayor's Directive of this same year.

The format of the Department's response to the audit will address specific comments in the audit and will coincide by page. It is important to note that the transfer of the 800 MHz Radio System, from HPD and Telephone Systems from DDC occurred during the past 2 years.

Comments about specific statements in the audit:

Page 3, "Of interest in relation to this audit is the rather unchanged staffing level of the Operations Division, and the implications this poses regarding the department's ability to adequately manage its information security."

DIT agrees that staffing has been an issue in adequately carrying out its obligations in the area of physical security and disaster recovery preparedness. For example, to some extent the policies regarding card access to the Data Center are designed to minimize the need to constantly sign in and sign out staff that requires access to the Data Center. However, DIT understands that tighter controls are needed to better manage access to the center and will develop policies and procedures to reflect this requirement in conjunction with the development of the RFP (by SAIC) for overall building control and access management at City facilities scheduled for this calendar year.

In another area (disaster recovery), only one full-time employee (FTE) was available, and responsible for the coordination of all the activities in this area, including developing the strategies, updating and maintaining the plan as the IT environment changes, coordinating activities with the other divisions, and conducting the annual test of the disaster plan. This FTE retired at the end of calendar year 2005.

Other challenges are detailed further in this response.

Page 5. Organization Chart

The Organization Chart included is not the official Org Chart of DIT. See Attachment 1 for the current Organization Chart.

Page 6, "This division provides support for major software applications such as those used for finance, land management, the city geographical information systems, public safety, and management services."

It is important to identify all of the major systems that the DIT supports. Attachment 2 provides this information.

Page 10, "For instance, data center access cards are issued without regard to actual access requirements and key management practices such as actively managing the access control system or reviewing logged access activity are not evident."

DIT acknowledges that the Data Center Card Access system and policies needs to be updated to ensure adequate protection for the City's IT resources. As cited in the audit, while no major incidents of unauthorized entry have occurred since the Data Center was first opened in 1970s; the department understands the importance of restricting and closely monitoring access to its key resources.

The audit criticizes the fact that all employees in DIT are given access cards whether they have needed to enter the Data Center or not. In fact, while all DIT employees have access cards, much of the Application's staff (25) have cards (green level) that only allow them through the first door. This access does not allow entry into the Data Center, but only to the Resource Center area and the area occupied by the Operation's Systems staff. The Applications staff needs to consult with the Systems staff from time to time and, therefore, access to the Systems has been given to the entire Applications staff. Ideally, both the Applications and Systems staff would be in the same location so that they could freely consult with each other. In fact, until a year ago, the Systems staff was located on the sixth floor, which made them more accessible to the rest of the DIT staff. Therefore, although the audit raised concerns about allowing all DIT staff members have access cards, many of these cards do not have access to the critical areas in the Data Center. DIT, however, acknowledges that further restriction of access cards will improve security. DIT as part of the strategic plan of 2006, will review the current access policies and procedures and will issue new guidelines to improve the security of the Data Center.

Among the issues that will be addressed are;

- Issue cards only to staff members that have demonstrated a need for access on a regular basis;
- Set up a procedure to periodically review the continued need for an access card;
- Require all cardholders sign a policy statement that holds the cardholder responsible for the safe keeping of the card;
- Set up a procedure for the daily review of the log files. Ensure that the log files are kept for some reasonable time.

DIT recently completed the preliminary design to upgrade its security camera and access control card system at the Data Center. This will coincide with work that is presently underway at the new HFD Headquarters building to ensure continuity. Attachment 3

Page 10, "Known physical and environmental control issues are evident, but the department has not actively pursued durable solutions to these concerns."

DIT acknowledges that there are known environmental issues that have plagued the Data Center from time to time. As noted by the audit, some of the issues regarding the Data Center facilities are not directly under the control of the department. The department coordinates activities with the Department of Facilities Maintenance and the Department of Design and Construction on issues such as repairs, fire control system, air conditioning, etc.

The needs of the Data Center fall into two general categories, short term and long term. To handle short-term problems and concerns, DIT will ask that a project team be formed that includes staff from DIT, DDC and DFM to address any Data Center issues. The project team will responsible to make recommendations to address issues, such as fire inspection reports, maintenance of the air conditioning system, status of minor repairs, water intrusion concerns, etc. The project team will report its findings and recommendations to the Directors of their respective departments by September 1, 2006.

As for long-term issues, the audit suggests that DIT has not been aggressive enough in pursuing solutions for problems such as water intrusion, physical security, the lack of a security camera system, and the air conditioning system failure. The department has sought solutions to these problems in the past, but has been unsuccessful in getting the previous administration to seek funding to address these problems. The water intrusion problem, fire suppression, and the air conditioning failures require major funding to rectify. DIT has requested CIP funding in the next fiscal year to address these issues. DFM will start this year to replace the chillers and air handlers for the air conditioning system for HMB and possibly for the Data Center. Due to a City ordinance that requires all high-rise building to have sprinklers installed, DFM is currently studying the sprinkler system and fire suppression systems to determine what improvements need to be made.

Page 10, "The department has not effectively managed its disaster recovery and contingency planning responsibilities: there are notable weaknesses with the current disaster recovery plans and insufficient support for implementing an effective recovery program."

DIT agrees that its disaster plans need to be improved. There is a disaster recovery plan in place that has been tested. However, the scope is limited due to lack of resources within DIT and at the various agencies. The department requested funding in the fiscal year 2007 budget for a Business Impact Analysis (BIA) for all City Agencies to identify what City business functions are significantly exposed to what effect they will be adversely affected in a disaster. This study will identify critical application priority order, business processes and vulnerabilities and containment measures. The schedule of this project will be determined after the funding issue is addressed.

The City auditor is critical about the fact that the last business impact analysis was conducted in 1989. DIT acknowledges that the IT environment in the City has changed enough to warrant a follow up business impact analysis. The department has sought funding for such a project several times in the past, but has not been successful in having the funding approved. The department is again asking for funding in the upcoming fiscal year 2007 budget. Disaster recovery planning is like having a good insurance policy. It is not important until you need it. But when you do need it, there is nothing more important than disaster preparedness. Unfortunately, it is all too easy to ignore it until it's too late. DIT will continue to push for adequate funding to continue a viable disaster recovery plan; however, DIT realizes that funding for disaster recovery has to compete with the other needs of the City.

Page 10; "Departments have been left to assess their own security needs, authorize users, create additional policies, and enforce all levels of IT policies."

Agencies "SHOULD" be responsible for IT security just like they are responsible to lock file cabinets, doors, desks. Providing access to files or an application is no different than allowing employees/consultants access to the facility, desk, file cabinets, door, etc. Ultimately, it is the department's director that has the responsibility for determining access to computer information. This function cannot/should not be DIT's role.

DIT should, with the assistance of the auditor and the agencies setup the general policies, assist agencies, and audit compliance.

Page 11, "Key planning documents and other departmental policies have attempted to delegate some oversight responsibility to the departments"

Page 12, "Key security management oversight functions such as monitoring effectiveness and assessing risk have not been implemented"

Oversight responsibility is delegated to the departments as they are ultimately responsible for the software applications and data. DIT recognized that the department should provide assistance in this area. The Computer Service Representative (CSR) position was created to provide this support as part of their role to provide vision and planning support functions. However, DIT's lack of authority and the overall lack of agency responsibility make this difficult to attain. Consideration should be made to assigning this responsibility to a security liaison person within each agency who can be held accountable.

A new DIT Strategic Plan was completed in calendar 2005, not 1998 as identified in the audit report. The revised plan for calendar year 2006, along with the revised Mayor's Directive, has been submitted to the Managing Director's Office for review and approval. Many, if not all of the issues identified in this audit are in the DIT Strategic Plan.

Page 13; "The facts above indicate the department takes a reactive rather than planned approach to managing citywide IT security risks. A more proactive approach would involve the use of risk assessments."

While the Department can be more proactive in managing citywide IT security risks, the Department has been proactive by implementing the following technologies:

- Spam filtering
- Internet Firewall
- County Firewalls
- Virtual Private Networks
- Wireless Security
- Virus Protection
- Intrusion Detection

Without these technologies, we would be faced with compromised internet access, huge amounts of unwanted email, and potential attacks on the City's web sites to name few.

Funding needs to be made available to conduct and detail security assessment of the City's various communications networks. These issues were identified in the DIT strategic plans of 2005 and 2006. Funding is requested in fiscal year 2007.

There is no funding request for ongoing monitoring. Consideration should be given to utilize the services of the Risk Management Department along with appropriate funding.

A comprehensive risk assessment for each agency needs to be conducted. The responsibility has been delegated to the Sr. Advisor of DIT. Funding will need to be sought.

Page 15: "As for foundational planning…."

Conflicting statements exist in this paragraph.

Page 16, "Current administrative guidance divides policymaking from monitoring and enforcement responsibilities"

Page 17, "The department relies on agency and user compliance to manage citywide IT security"

Page 18, "The department does not provide sufficient training on responsibilities and obligations to justify their delegation"

DIT has not been vested with the authority to enforce security plans and policies on City users, so this authority has defaulted to the departments and agencies. DIT has provided departments and agencies management with guidance. Authority is further complicated because of semi-autonomous agencies who have access to a number of the systems and networks.

The City currently has over 10,000 employees. A full time training process will need to be instituted and authority given to the appropriate agency.

Consider vesting DIT with this authority, along with the resources and funding to support it.

Page 19, "Almost every departmental employee is issued an access card, with minimal regard to actual need"

Cards are issued to all DIT staff members. Green level access grants access only to the Resource Center and the Systems programming staff areas. Approximately twenty percent of the staff has access to this level. Applications programmers occasionally need to consult with our Systems programming staff. Until a year ago, the Systems staff was located on the sixth floor, which allowed the Applications staff to freely consult with them. Subsequently the Systems staff moved to the Data Center. The "Green level" (access to the first door in DIT's basement area), enables the Applications staff to continue to have direct contact to the System staff.

Page 21, "Except for card issue and establishment of initial privilege level, there is little management of the card system and its related rules."

DIT acknowledges that it could do a better job in managing the card access system. Appropriate action will be taken in conjunction with implementation of the new system budgeted in calendar year 2006. Attachment 3

Page 23, "The Department of Facility Maintenance manages the Kapolei Hale facility. However, the Department of Information Technology has not established access control rules for this room, as it has shared control over the facility."

An access control and monitoring system was installed in Kapolei Hale as part of construction of this facility. The system was never activated and as such is not monitored. Access control design and support was recently turned over to DIT. DIT is in the process of documenting all of the systems, developing a citywide standard, and developing an RFP for a citywide solution that complies with Federal standards including NIMS and FIPS 201.

Page 24, "Logged activity is not regularly monitored or reviewed"

DIT acknowledges that there is inadequate monitoring of the access logs. However, there is an ever greater gap with the lack of overall monitoring of city facilities.

In addition to developing procedures to ensure that the logs are reviewed on a regular basis, proposals are being developed for a complete facilities wide review of access management.

Page 24, "The data center faces known physical and environmental control issues that may jeopardize its IT resources and systems."

The City has been remiss in maintaining the physical plant of DIT. Since the new Director has arrived, there has been a fire in the data center, a failure of the fire suppression system, water intrusion, multiple air conditioning system failures, and ceiling tile collapse to name a few. An aggressive rehabilitation program is warranted. FY2007 identifies funds in the DDC budget to begin to address these issues.

Page 25, "The data center is subject to water intrusion"

[See general comment above.]

Page 27, "Fire suppression may not be in working condition"

As noted elsewhere in the audit, DIT is dependent on the Department of Facility Maintenance for the upkeep of the Data Center facilities. For the most part, DFM has adequately fulfilled its part in keeping the Data Center in operating shape. However, DFM has its own set of obligations that sometime preclude providing support to DIT. The fire suppression system is one area that DIT is dependent on DFM to keep in operating shape. DFM is currently studying the sprinkler system and fire suppression systems to determine what improvements need to be made.

Page 27, "Air conditioning failures are problematic"

Several recent problems have caused concern. DFM has recommended that DIT consider replacing the air conditioning system that serves the Data Center. Initial cost estimates are significant. DIT will investigate an affordable means of replacing the air conditioning system. DFM will start this year to replace the chillers and air handlers for the air conditioning system for HMB and possibly for the Data Center.

Page 28, "Some entry points appear insecure"

DIT acknowledges that there are a couple areas of concern regarding the physical security of the Data Center. As stated earlier, DIT has completed a preliminary review, and will integrate this solution with the overall building solution.

Page 29, "Further issues related to the Kapolei computer room"

See previous statement regarding access control and monitoring in Kapolei.

The uninterruptible power supply has been installed and is going through the final stages of acceptance testing. The UPS should be fully functional within the next 2 months. This culminates a project that languished for 2 years prior to this administration.

Page 30, "Disjointed responsibility contributes to a lack of implementation of appropriate controls"

DIT acknowledges that there are some issues that are a result of the lack of coordination between DIT and DFM. DIT, with the support of DFM, will create a work team to address Data Center specific issues.

Page 30, "The department has sought only temporary solutions to known problems"

DIT acknowledges that it has not sought major repair to fix the known problems in the Data Center. This is based on previous administration direction. This administration has requested CIP funding in the next fiscal year to address the water intrusion, fire suppression, access control and air conditioning issues.

Page 31, "Daily tapes used to be stored offsite but are currently being stored in the Civic Center parking garage. Previously, daily tapes were taken each morning to the Honolulu Police Department at Alapai Street, where they were stored in a minicomputer room secured by an access control card key. The card, however, recently expired and has not been renewed because the police department is reviewing continuing authorization."

Page 32, "The current daily tape storage location, in the municipal building's parking garage, does not offer this protection. Although it is a dedicated storage space for the department and is located adjacent to the municipal building, it is near enough to be affected by any building-specific event. It would also be affected by a local power outage or other disaster such as a storm."

"In the event Honolulu Police Department storage room access is not renewed, the department will need to find another viable daily storage site because the parking garage location is not far enough away from the data center to protect against loss caused by the same event. The department has been warned in a previous review that is practice of storing tapes in the municipal parking garage is not distant enough to protect against impairment."

Page 33, "As noted above, the daily tape drop site is probably too near to Honolulu Municipal to be used as a permanent site for daily backup storage. If the Honolulu Police Department site cannot be reauthorized, another location should be chosen."

The Honolulu Police Department recently renewed the DIT access to the minicomputer room, and the daily backup tapes are once again being stored in the HPD facility.

Page 33, "Some aspects of routine backup and recovery require future management attention."

"Another issue relates to mainframe backups. At present, the department is able to recover mainframe data, but it takes 48 hours to return to useful processing again. More equipment, including updated communication, storage, and mainframe equipment could make this process more efficient, so that the department could lose only 3 to 4 hours instead of 48. Pending budgetary approval, the department plans to acquire the necessary equipment within the next 18 to 12 months."

"Similarly, the age of some equipment was also cited as a barrier to upgrading to more effective technology. The reliance of out-of-date hardware or software, which is no longer supported by vendors, is a related problem that creates maintenance and efficiency issues in this area. Some interviewees voiced concerns that the limited problems experienced with backups and recovery were caused by bad tapes, recovery time required not timely meeting business productivity needs, or other problems with current technology applied."

As noted in the audit, DIT conducts annual tests of the mainframe recovery plans and feels that the production mainframe applications, such as Motor Vehicle Registration, Driver's Licensing, Voter Registration, etc. can be restored within a forty-eight hour period. DIT is attempting to

obtain the current hardware and software needed to provide a much faster recovery period. The department plans to have the improved recovery process in place before the end of 2006 to allow a recovery within a four-hour window. DIT is also replacing old cartridge tapes when new tapes as problems occur. Tape technology is an outdated form that will be used in the interim, since the City already owns the equipment.

Page 33, "Under the existing plan, there is no client server recovery strategy; however one is being drafted."

Page 34, "Notable weaknesses related to the current state of disaster recovery planning exist"

"The department's disaster recovery plan is founded on a business impact analysis conducted in 1989. In the intervening years, responsibility has been passed to city agencies to conduct their own business impact analyses and risk assessments. To date, neither the department nor agencies have conducted a risk or impact analysis that would align with current conditions. Furthermore, the prevalence of client server/local area networks in use warrant assessment as to their risk, business impact and continuity, and incorporation into the city's disaster recovery contingency plan."

DIT has requested funding without success in the past to conduct a study. A server consolidation study in planned for calendar year 2006. This study will encompass backup, recovery, archiving and disaster recovery related to the DIT "server farm". The business impact analysis forms the basis of all disaster recovery planning activities. Without an up to date business impact analysis, it will be difficult for DIT to set the correct priorities in its disaster recovery plans. DIT is also currently working on developing a client/server recovery strategy. DIT has asked for funding to hire a consultant so that the client/server process can be developed in a shorter period.

Page 34, "During the most recent mainframe database recovery testing period, tests were performed with a modified 48 hour (the two day requirement) timeframe to accommodate a standard work day, and did not incur staff overtime. However, the department's testing report summary notes that an actual 48 hour test should be performed in the future to simulate disaster conditions."

DIT will consider whether an actual 48-hour test should be done. Overall city-wide impacts will need to be addressed before hand.

Page 34, "Furthermore, off-island technical support that was unavailable during the test period is problematic." "… testing, maintenance, reconciliation, and coordination should be made mandatory since one county recently opted out of a testing exercise."

While DIT can relay to the other counties the importance of their participation in the annual disaster recovery testing, the department has no jurisdiction over the counties, and therefore, cannot mandate that they participate in the exercise.

Page 35, Priority of recovery is another important issue. We were provided with a list indicating the order of emergency processing priorities among city entities. These priorities, however, have not been coordinated with agencies. The department's director acknowledged this gap, noting the department does not know agencies' own priorities in the event of loss and there are no criteria on which the department can judge its service and support to agencies."

DIT has requested funding for fiscal year 2007 for a business impact analysis in planning to work on creating risk assessments for City departments to address this issue. This project is to be headed up by the departments' senior advisor.

Page 35, "The support site issue is problematic."

DIT acknowledges that it has not been in contact with the police on this specific issue. HPD has given no indication that the availability of their minicomputer center is an issue. While DIT considers the Kapolei site as its primary backup site, DIT feels that the HPD site is still a viable recovery site. DIT will check with HPD as to the availability of the minicomputer room as a disaster command site. DIT will also be reviewing other managed service alternatives.

Page 35, "Most functions in the plan are meant to be carried out by Honolulu Municipal Building-based personnel"

DIT acknowledges that the plan is based on the participation of HMB based personnel. The department has no choice, since ninety-five percent of DIT's staff resides in HMB. The disaster recovery plan is somewhat generalized intentionally, as the plan cannot rely on any specific person or persons. In a disaster situation, the response as presently defined inhibits the ability to determine who might be available to carry out the recovery process.

Page 36, "Kapolei site is not fully suited for recovery or command activities"

DIT acknowledges that the Kapolei site has its shortcomings. The lack of funding has contributed to this issue. DIT would certainly acquire a bigger and better recovery location if funds were available. However, DIT feels that the Kapolei facility is adequate in most respects. DIT had asked the prior administration for commitment of additional space to ensure adequate recovery area. The past administration was reluctant to commit space to something that MAY OR MAY NOT happen. The prior administration felt that priorities at the time of disaster would dictate what facilities would be made available to DIT's recovery process.

DIT plans to address this as part of the city wide disaster planning activities that are currently underway.

Page 36, "Previous administration was primarily concerned with high profile and public relations activities"

True, and as such low visibility infrastructure projects were negatively impacted.

Page 37, "Disaster recovery coordinator has responsibility but no authority to accomplish disaster recovery planning"

True. DIT will be reviewing alternatives as part of their response to address this audit.

Summary

The Director wishes to thank the auditor for this effort. The DIT staff has done a commendable job over the years considering what resources have been made available. Also, it is the role of administration to address the issues identified in this audit in a timely and fiscally prudent manner.

Sincerely,

GORDON J. BRUCE
Director and CIO

GJB:mo

cc: Mayor's Office

Attachments (3)

Attachment 1

SUBMITTED BY

Department Head — Date 4/7/99

REVIEWED BY

Chief Budget Officer — Date 6/24/99

APPROVED

Managing Director — Date 6.29.99

DEPARTMENT OF INFORMATION TECHNOLOGY (DIT) ADMINISTRATION

CHART I
(rev. 06/02/99)

EXISTING

ADMINISTRATION

Plans, directs and coordinates the City's data processing system which includes equipment selection, systems analysis, programming and operations; provides technical leadership in data processing to all City agencies; advises the Mayor and departments on all matters relative to electronic data processing systems; establish City-wide data processing standards, guidelines, conventions, and compatibility of data processing systems.

Positions

1 - Director of Information Technology	(IS 100)	NC
1 - Deputy Director of Information Technology	(IS 170)	NC

Administrative Office

Coordinate the internal administrative affairs of the department, including budget preparation and control of expenditures; personnel administration; analyze manpower utilization and recommend staffing levels of operating units; analyze and plan improvements in organization, methods, systems and equipment; assist in the development of specifications for acquisition of equipment and software; provide and clerical services for the department such as maintaining the inventory and payroll records.

Position

1 - Chief of Data Processing	(IS 105)	EM-08

Positions

1 - Private Secretary II	(IS 201)	SR-22
1 - Private Secretary I	(IS 154)	SR-20

Administrative Services Positions

1 - Administrative Assistant II	(IS 193)	SR-22
1 - Personnel Clerk I	(IS 108)	SR-13
1 - Clerk Typist	(IS 162)%	SR-08
1 - Sr. Clerk Typist	(IS 173)@	SR-10

Applications Division

Performs the full range of computer system development including feasibility studies, systems analysis and design, and computer programming; performs systems testing, personnel training and detail documentation of the developed systems; maintains implemented systems; provides consulting services to end users; provide file conversion support for Information Center. Also assist the user departments to plan and coordinate data processing goals in line with DIT objectives. Coordinate all efforts between the user department and DIT as it relates to information processing.

Technical Support Division

Serves as technical advisor to Operations Division, Applications Division and end user agencies that have achieved some self sufficiency with regard to developing computerized systems using their own resources; maintains systems software; trains application staff and operations staff in the use of systems software; establishes and maintains the communication network; prepares reports on systems usage and capacity requirements; establishes and conducts training programs for end users; and evaluates equipment. Establish, maintain, monitor and manage databases for all City agency's systems.

Operations Division

Plans, administers and coordinates the data processing operations of the central computer, data entry equipment and auxiliary equipment; develops and maintains monetary and document controls to ensure accuracy of data processed; develops computer schedules; routes documents and reports to and from users; coordinates software and hardware changes with user agencies; provides diagnostic services on computer network; acts as network controller by coordinating installation and deinstallation of terminals for all agencies; establishes and maintains sites and procedures for offsite storage; establish, maintain and implement (if necessary) disaster recovery plans; provide help desk and storage management services. Establish and maintain computer security systems.

% Proposed reallocation of IS162 Data Entry Operator I to Clerk Typist; upon approval of IS162's reallocation, position IS106 is proposed to be abolished

@ Proposed reallocation of IS173 Data Entry Supervisor I to Senior Clerk Typist; upon approval of IS173's reallocation, position IS107 is proposed to be abolished

SUBMITTED BY:

11/23/04

Department Head — Date

REVIEWED BY:

11-29-04

Director of Budget & Fiscal Services — Date

APPROVED BY:

11.30.04

Managing Director — Date

DEPARTMENT OF INFORMATION TECHNOLOGY (DIT)
APPLICATIONS DIVISION

CHART II
(rev. 11/15/04)

Existing
~~Proposed~~

APPLICATIONS DIVISION

	Position	
1 - Chief of Data Processing	(IS119)	EM-08

Database Section

	Positions	
1 – DP Systems Analyst IV	(IS166)	SR-26
2 – DP Systems Analyst III	(IS115, IS171)	SR-24
1 – DP Systems Analyst I	(IS126)	SR-20

Financial and Land Management Applications Branch

Performs feasibility studies, systems analysis, systems design and computer programming for departments, divisions and agencies that perform activities that support financial, land management, and geographic information systems; performs systems testing and provides detail documentation and operating procedures for the completed systems; receives, analyzes, and makes revisions to the operational programs and supporting documentation to maintain continued operations; and provides computer service representative support to the department.

	Position	
1 – Data Processing Program Manager	(IS122)	EM-05

	Positions	
1 - DP Systems Analyst IV	(IS113)	SR-26
4 – DP Systems Analyst III	(IS124, IS137, IS199, IS217)	SR-24

	Positions	
4 - DP Systems Analyst III	(IS116, IS131, IS206, IS221)	SR-24
2 - P/T DP Systems Analyst III	(IS01A, IS01B)	SR-24
4 - DP Systems Analyst II	(IS127, IS140, IS192, IS197)	SR-22
1 – DP Systems Analyst I	(IS232)	SR-20

Public Safety and Management Applications Branch

Performs feasibility studies, systems analysis, systems design and computer programming for departments, divisions and agencies that have direct contact with the public in the areas of health, service, and safety; performs systems testing and provides detail documentation and operating procedures for the completed systems; receives, analyzes and makes revisions to the operational programs and supporting documentation to maintain continued operations; and provides computer service representative support to the departments.

	Position	
1 – Data Processing Program Manager	(IS112)	EM-05

	Positions	
1 – DP Systems Analyst IV	(IS114)	SR-26
4 – DP Systems Analyst III	(IS123, IS165, IS213, IS236)	SR-24

	Positions	
9 – DP Systems Analyst III	(IS152, IS168, IS177, IS189, IS204, IS207, IS208, IS212, IS214)	SR-24
2 – DP Systems Analyst I	(IS130, IS136)	SR-20

CSR Branch

Performs as IT manager for each City agency. Provide IT planning. Coordinate various IT projects for the agency including DIT initiatives. Serve as a liaison between DIT and the user agency. Assist with the support of agency mission critical systems. Ensure timely and acceptable technical support is available to keep the agency's PCs and printers functional.

	Position	
1 – Data Processing Program Manager	(IS235*)	EM-05

General City Services Section

	Positions	
1 – DP Systems Analyst IV	(IS144)	SR-26
8 – DP Systems Analyst III	(IS102, IS159, IS181, IS182, IS183, IS185, IS186, IS216, IS227)	SR-24
5 – DP Systems Analyst II	(IS188, IS202, IS218, IS226, IS234)	SR-22
1 – Computer Programmer II	(IS228)	SR-18

Public Health & Safety Services Section

	Positions	
1 – DP Systems Analyst IV	(IS157**)	SR-26
2 – DP Systems Analyst III	(IS209, IS220)	SR-24
3 – DP Systems Analyst II	(IS237, IS239, FC141***)	SR-22
1 – DP Systems Analyst I	(IS238)	SR-20
1 – Computer Programmer I	(IS187)	SR-16

*Proposed reallocation from Data Processing Systems Analyst II, SR-22
**Proposed reallocation from Data Processing Systems Analyst II, SR-22
***Proposed transfer of Data Processing Systems Analyst II, SR-22 position to DIT from Fire Dept

SUBMITTED BY:

11/18/04

Department Head — Date

REVIEWED BY:

11/18/04

Director of Budget & Fiscal Services — Date

APPROVED BY:

11·22·04

Managing Director — Date

DEPARTMENT OF INFORMATION TECHNOLOGY (DIT)
TECHNICAL SUPPORT DIVISION

CHART III
(rev. 11/01/04)

Existing
~~Proposed~~

TECHNICAL SUPPORT DIVISION

	Position	
1 – Chief of Data Processing	(IS109)	EM-08

Network and Telecommunications Branch

Receives, evaluates, implements, and modifies new/existing operating systems software furnished by the computer manufacturer and other vendors for the Local Area Network (LAN), Wide Area Network (WAN), Internet and Intranet systems. Tests and evaluates all data processing equipment required to establish a total LAN environment including interfacing to all other systems including the City's mainframe system. Establishes and maintains mainframe, LAN, WAN, Internet and Intranet security systems.

	Position	
1 – Data Processing Program Manager	(IS110)	EM-05

Network Section

	Positions	
1 – Data Processing Systems Analyst IV	(IS128)	SR-26
1 – Data Processing Systems Analyst III	(IS164)	SR-24
2 – Data Processing Systems Analyst II	(IS190, IS205)	SR-22
1 – Computer Programmer II	(IS233)	SR-18

Security Section

	Positions	
1 – Data Processing Systems Analyst IV	(IS121)	SR-26
1 – Data Processing Systems Analyst III	(IS167)	SR-24
1 – Data Processing Systems Analyst II	(IS175)	SR-22
1 – Data Processing Systems Analyst I	(IS206)	SR-20

End User Support Services Section

Administers the City's Server infrastructure which involves both hardware and software maintenance of servers such as active directory, file and print, email, web, database and application servers; performs feasibility studies, analysis, and design for computer systems; conducts computer training classes; develops procedures and guidelines for the procurement of computer equipment and software.

	Positions	
1 – Data Processing Systems Analyst IV	(IS136)	SR-26
7 – Data Processing Systems Analyst III	(IS111, IS118, IS180, IS184, IS191, IS215, IS219)	SR-24
1 – Data Processing Systems Analyst II	(IS125)	SR-22

Radio and Telephone Systems Branch

Directs the planning, design and operation of communication facilities for the City, including telephone, microwave, R-F wireless telecommunications and data systems.

	Position		
1 – Communications Coord	(IS291)	Jerry M H Loo	SR-28

Radio Systems Engineering Section

Provides planning, management and maintenance support of the 800 MHz system; planning, management and operation of the microwave system, the fire and local government radio systems, and the GPS island-wide system.

	Position		
1 – Electrical Engr V	(IS294)	Vacant	SR-26
2 – Radio Technician I	(IS210*, IS293**)	Vacant	SR-19
1 – Engrng Support Tech II	(IS290)	Benigno Maodac	SR-17

Telephone Systems Engineering Section

Provides planning, management and operation of the City telephone system; programming of services, design modifications and maintenance support for City agencies; management of the emergency facilities E911 system; administration and implementation of cellular telephone and long-distance systems.

	Positions		
1 – Engrng Support Tech III	(IS292)	Dennis S Ing	SR-19

*Proposed reallocation from Data Processing Systems Analyst III, SR-24
**Proposed reallocation from Communications Assist, SR-11

SUBMITTED BY: 9-17-04
Department Head — Date
REVIEWED BY: 10-15-04
Director of Budget & Fiscal Services — Date
APPROVED BY: 10-21-04
Managing Director — Date

DEPARTMENT OF INFORMATION TECHNOLOGY (DIT)
OPERATIONS DIVISION

CHART IV
(rev. 08/01/04)

Existing
~~Proposed~~

OPERATIONS DIVISION

	Position	
1 – Chief of Data Processing	(IS142)	EM-08

Systems and Operations Branch

Assumes the duties of the Chief of Operations in his/her absence. Manages, directs, and coordinates activities of the Systems programmers. Evaluates, selects, and implements hardware and software appropriate for the City's IT environment. Manages the operation of the Computer Center, including the operators and data entry personnel. Develops procedures and policies for computer operations.

	Position	
1 – Data Processing Program Manager	(IS143)	EM-05

Systems Section

Receives, evaluates, modifies, and implements new operating systems software, security software, and database software furnished by the computer manufacturer and other vendors. Designs and develops customized supervisory programs as required; evaluates data processing equipment for use in the City's mainframe environment; trains the technical staff in the use of programming aids and techniques; monitors system performance and recommends appropriate equipment and procedures to optimize performance; initiates capacity planning studies.

	Positions	
~~1 – Data Processing Systems Analyst IV~~	~~(IS128)~~	~~SR-26~~ *
2 – Data Processing Systems Analyst III	(IS129, IS203)	SR-24
1 – Data Processing Systems Analyst II	(IS198)	SR-22
1 – Data Processing Systems Analyst I	(IS132)	SR-20

Computer Operations Section

Provides the day-to-day operation of the computer equipment, including the mainframe, servers, and communications gear; establishes schedules for all production jobs; performs tasks necessary to keep the Computer Center and all IT equipment in good working order; and works with the technical staff, City IT users, and outside vendors when necessary.

	Position	
1 – Data Processing Control and Entry Supervisor	(IS134)	SR-24

Computer Operators

	Positions	
3 – Computer Operations Supervisor	(IS145, IS147, IS148)	SR-19
3 – Computer Operator III	(IS141, IS146, IS153)	SR-17
9 – Computer Operator II	(IS103, IS135, IS138, IS139, IS149, IS155, IS158, IS179, IS196)	SR-15

Data Entry Operators

	Positions	
3 – Data Entry Operator I	(IS163, IS176, IS194)	SR-08

Disaster Recovery and Storage Management

Develops, documents, and maintains the City's IT Disaster Recovery plans. Coordinates activities with technical staff to modify plans as necessary as requirements change. Develops, documents, and maintains the City's corporate IT data. Ensures that adequate back up and recovery procedures are in place for all production files.

	Positions	
2 – Data Processing Systems Analyst III	(IS172, IS211)	SR-24

Help Desk

Manages, directs, and coordinates all activities related to the City's centralized Help Desk. Evaluates and implements appropriate hardware and software to provide tools necessary to run an efficient Help Desk. Manages the activities of the ITST technicians and call takers, and supports the Computer Service Representatives (CSRs) by providing technician help as necessary.

	Position	
1 – Data Processing Systems Analyst III	(IS151)	SR-24

Call Takers

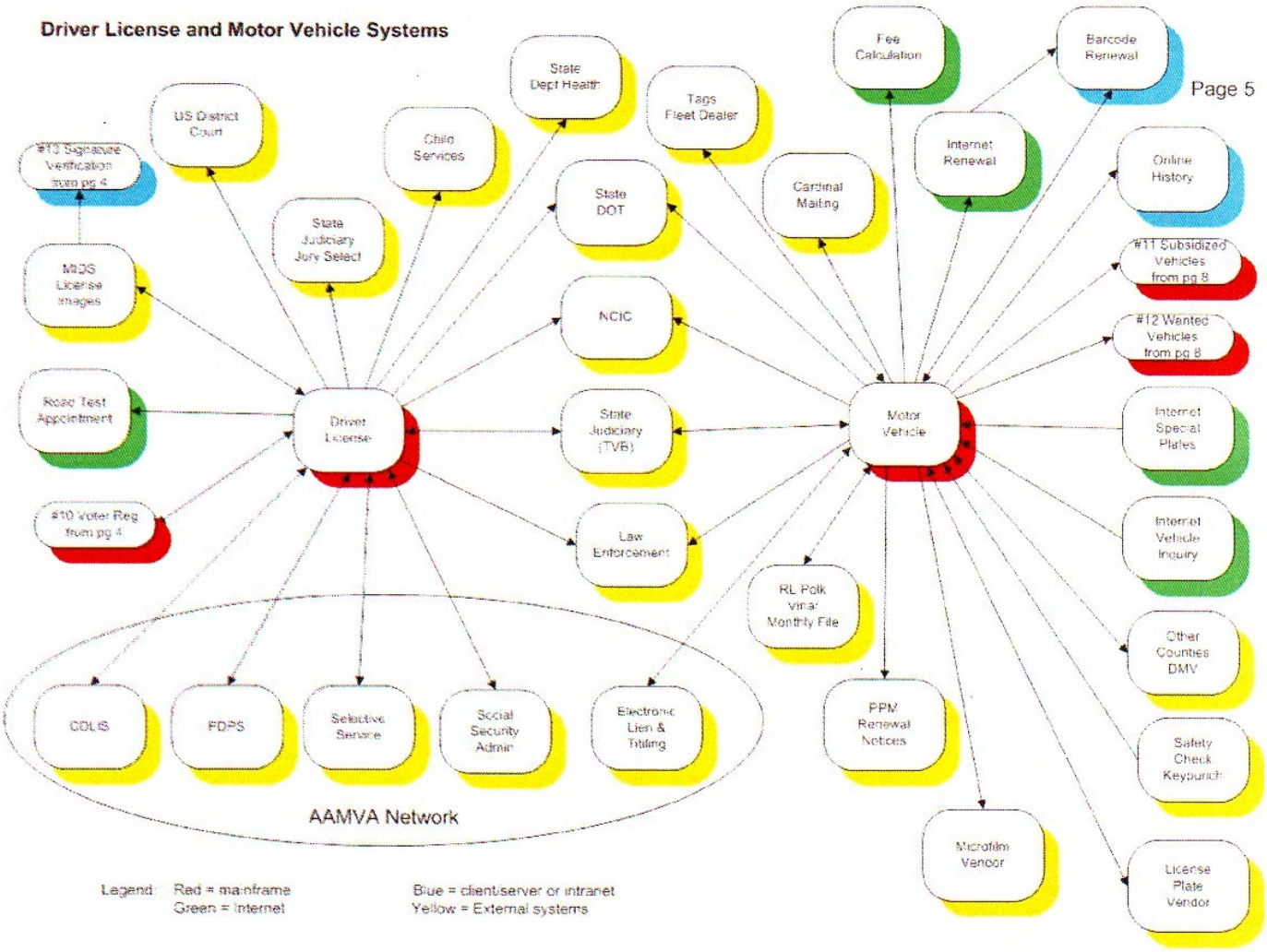
	Positions	
2 – Information Technology Support Technician II	(IS104, IS133)	SR-15

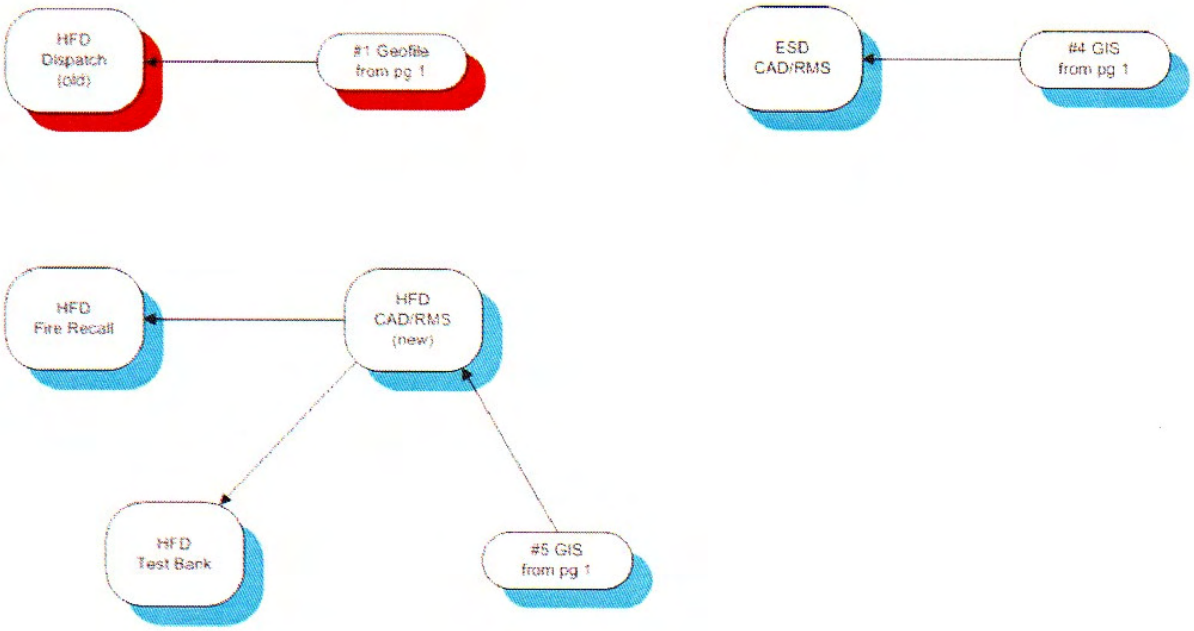
Technicians

	Positions	
6 – Information Technology Support Technician II	(IS222, IS223, IS224, IS225, IS229, IS231)	SR-15
1 – Information Technology Support Technician I	(IS230)	SR-13

*IS-128, duplicate position in Technical Support Services Division

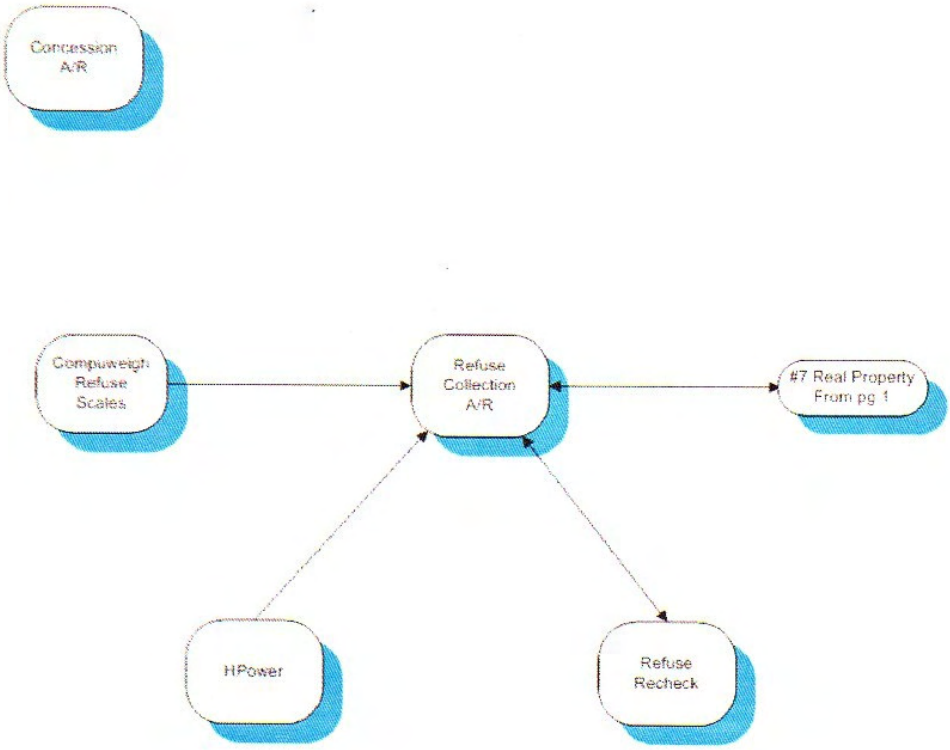
Attachment 2





Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

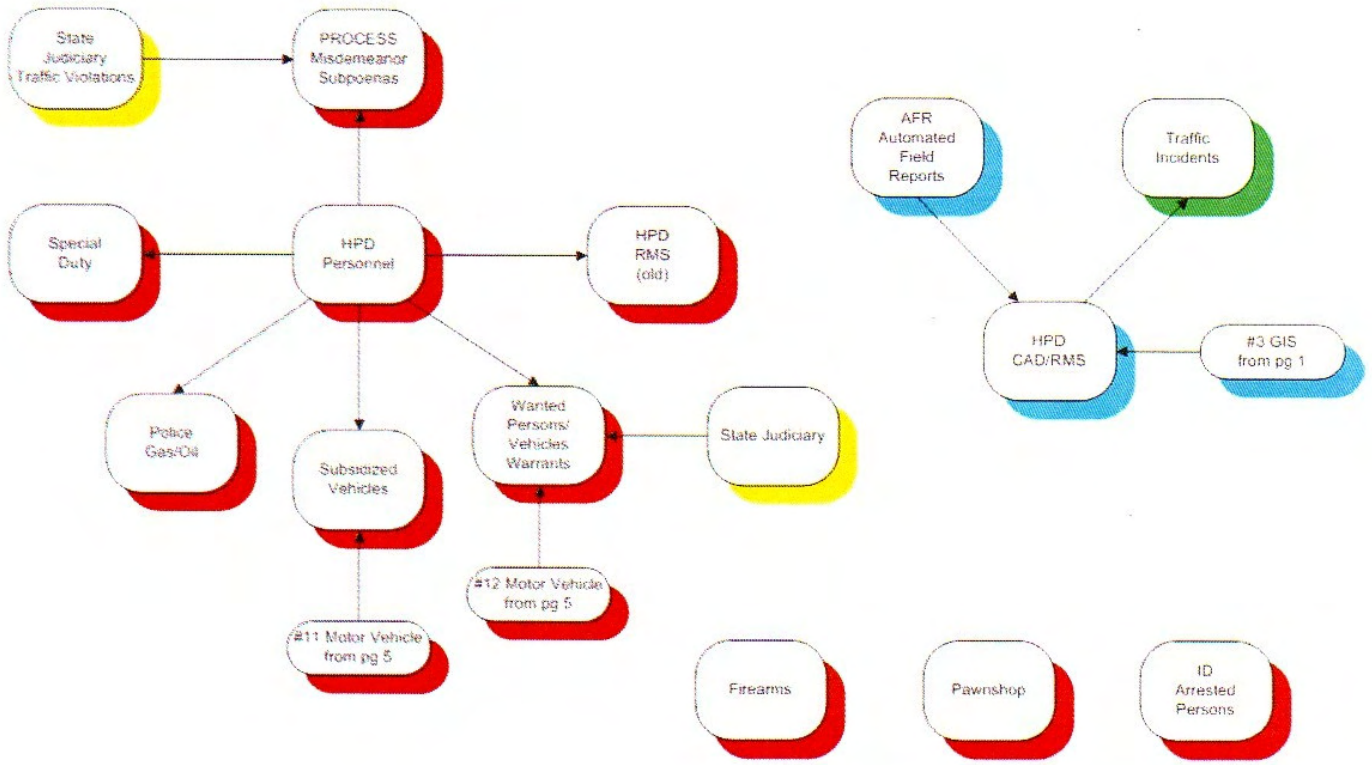
Miscellaneous Financial Systems



Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

Miscellaneous Systems

Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

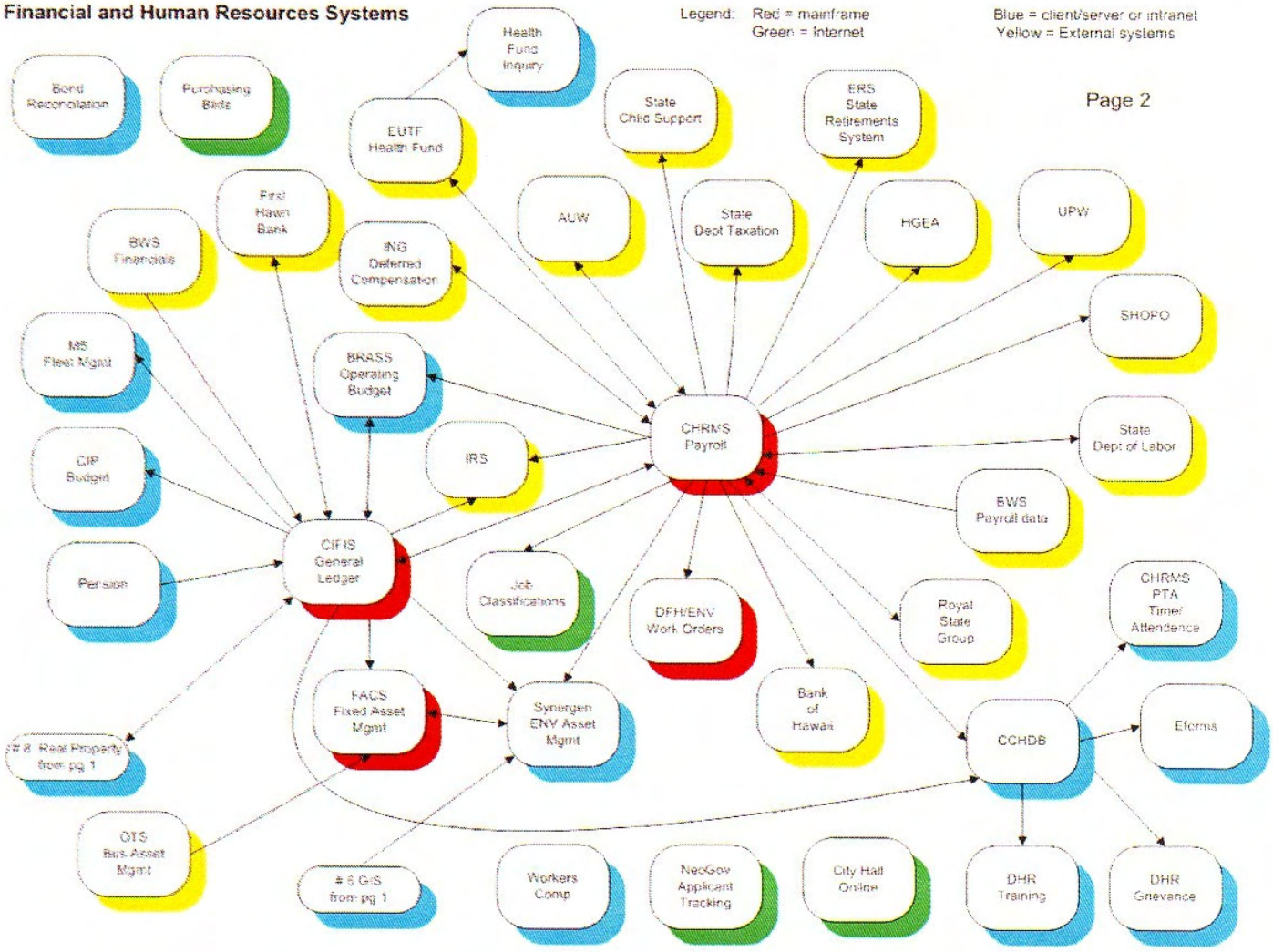


Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

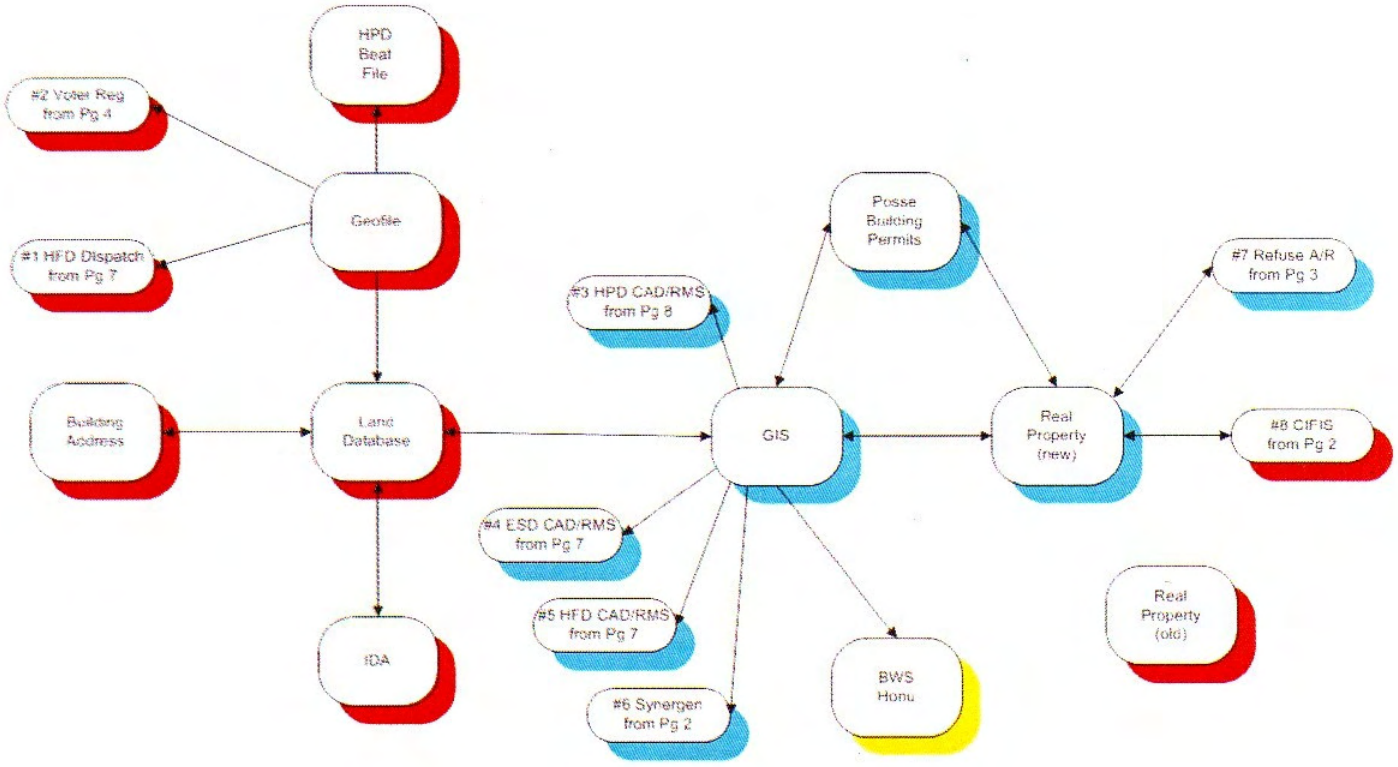
Financial and Human Resources Systems

Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

Page 2



Land Systems

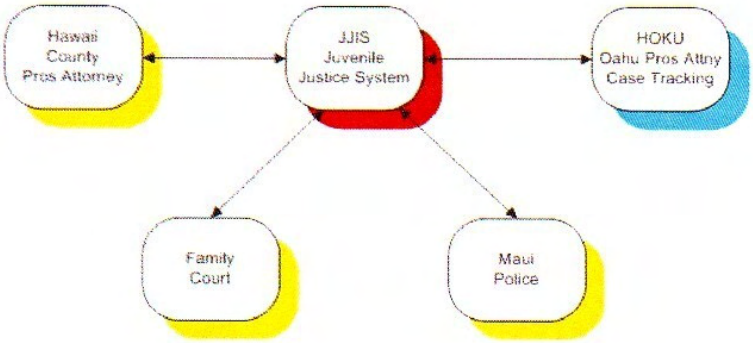


Legend. Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

Miscellaneous Licensing & Permitting Systems

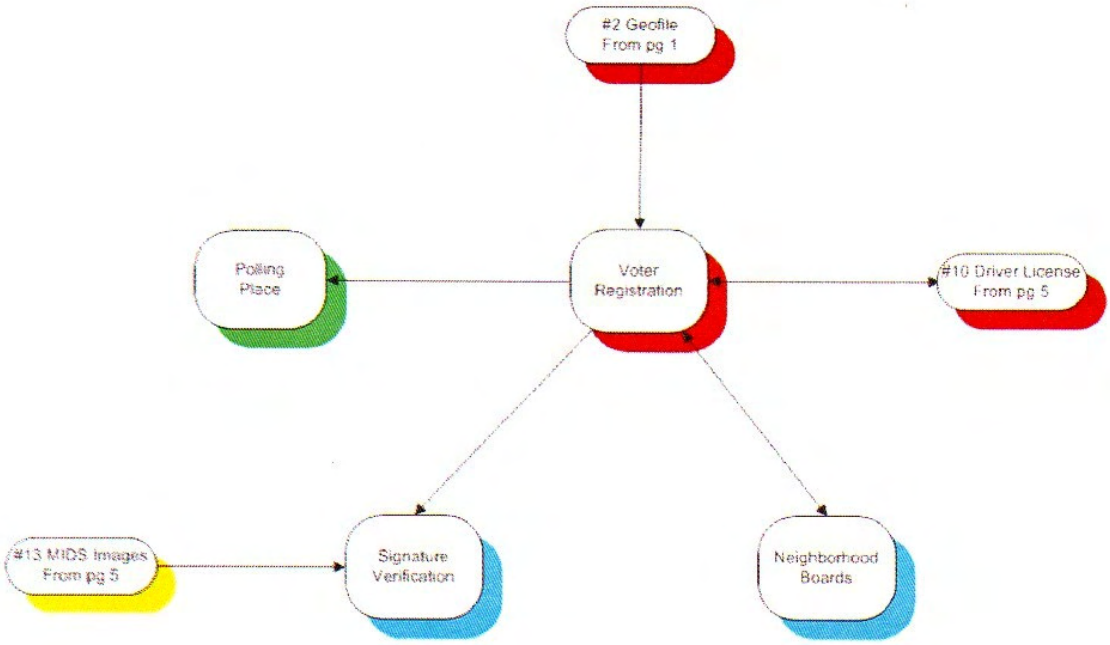
Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

Miscellaneous Police Systems



Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

Voter Registration System



Legend: Red = mainframe
Green = Internet
Blue = client/server or intranet
Yellow = External systems

Attachment 3

PROPOSAL

CUSTOMER	City and County of Honolulu Department of Information Technology	**CONTRACT**	
		PROJECT	DIT Data Center

QTY	DESCRIPTION
	Operations Center:
	Access Control
1	Intelligent System Controller – 12 VAC or 12 VDC, (5 year lithium battery or 3 months full run) 512K standard memory and stand-offs
1	CoBox Micro serial server, Flash ROM RJ45 (10BaseT), diagnostic LED's Dimensions 1.57' (40mm) x 1.93' (49mm) includes standoffs, for LNL-500 and LNL-2000 only
2	2-Door Controller
4	REQUEST TO EXIT PIRS
4	945WH MAGNET ASSY, WH
2	Mortise Unlatch Motorized Strike
4	iCLASS R40 READ ONLY contactless smart card reader, Wiegand output, US/EU/Asian back box sizes , read range 1 to 3.5 inches (2.5 to 8.9 cm), 80/230mA Avg/Peak @ 12 VDC, color BLACK
	Digital Video
1	24VAC Rack Mount Camera Power Supply
8	Additional Single LNR Channel- Support for an additional IP / Network based camera channel to be used with (PC-LNR8-3U) Turnkey Solution. (maximum of 32 IP/network channels per LNR)
2	Videoserver, communicates over Internet/Intranet, four channels PAL or NTSC, up to 30 FPS. Modem support, PHP3 and Linux.
6	Interior, Recessed Mount, High Resolution, Color, Camera with 2-6mm Varifocal, Auto-Iris Lens
2	High Resolution Color Camera
2	10-50 mm Varifocal, Auto-Iris Lens
2	Camera Wall Mount
80	* Cabling and Hardware Equipment Installation, Configuration, Termination, and Testing. ** Software Installation, Configuration, and 4 Hours End-User Training.
	* - Presumes reuse of existing enclosure and power supply. ** - Presumes existing IP connectivity is available, and usage of existing Lenel system database software license (HFD). ** - PC's to be provided by C&C
	Interior Light Switches
2	Motion Activated Light Switch
5	Install Push-in box for single gang motion light switch
	Parking Garage Storage Room:
	Access Control
1	Power Supply
1	Intelligent System Controller – 12 VAC or 12 VDC, (5 year lithium battery or 3 months full run) 512K standard memory and stand-offs
1	CoBox Micro serial server, Flash ROM RJ45 (10BaseT), diagnostic LED's Dimensions 1.57' (40mm) x 1.93' (49mm) includes standoffs, for LNL-500 and LNL-2000 only

Signature & Date

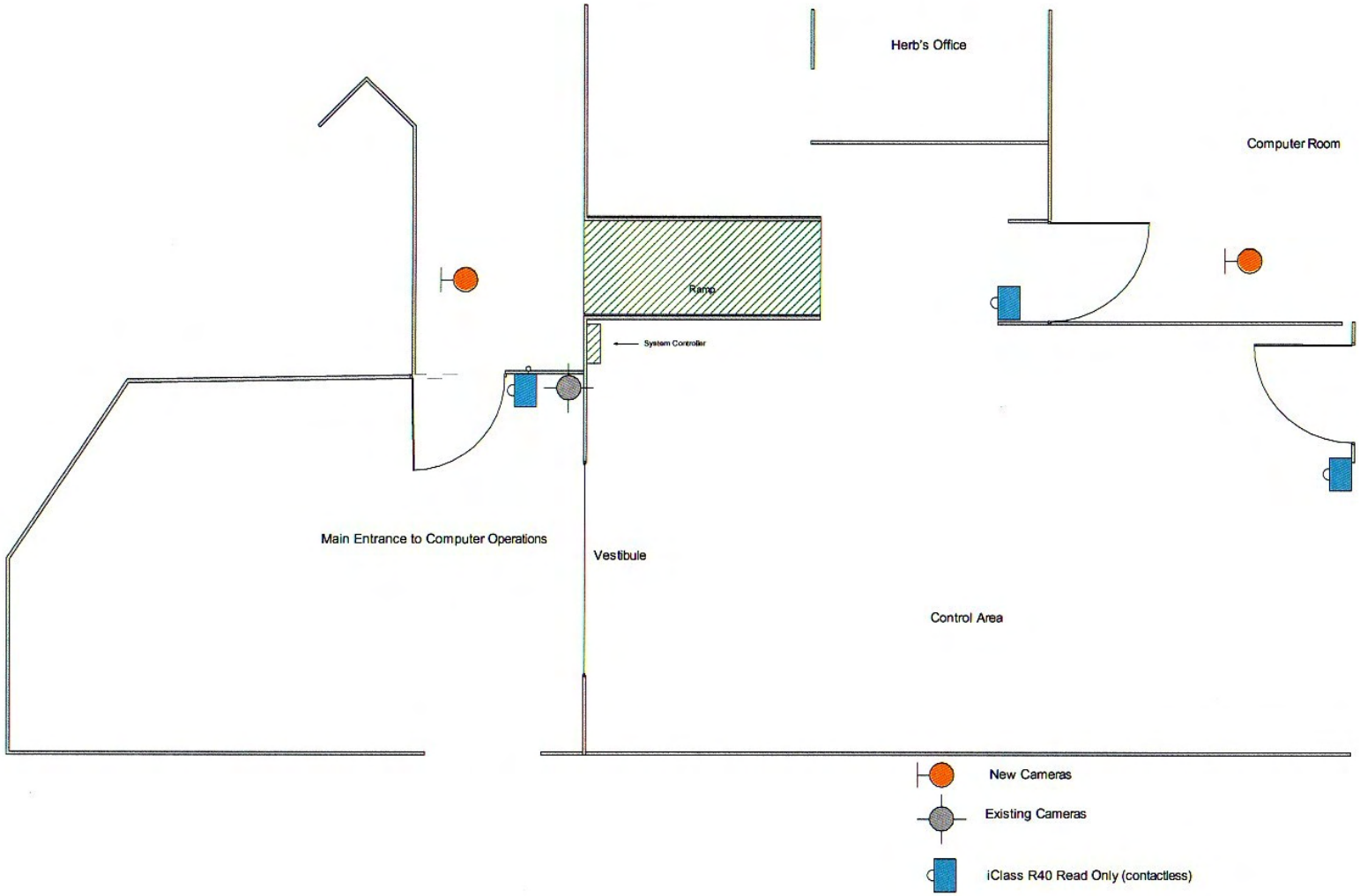
* This proposal is only good for (30) days from proposal date. *

CUSTOMER	City and County of Honolulu Department of Information Technology	**CONTRACT**	
		PROJECT	DIT Data Center

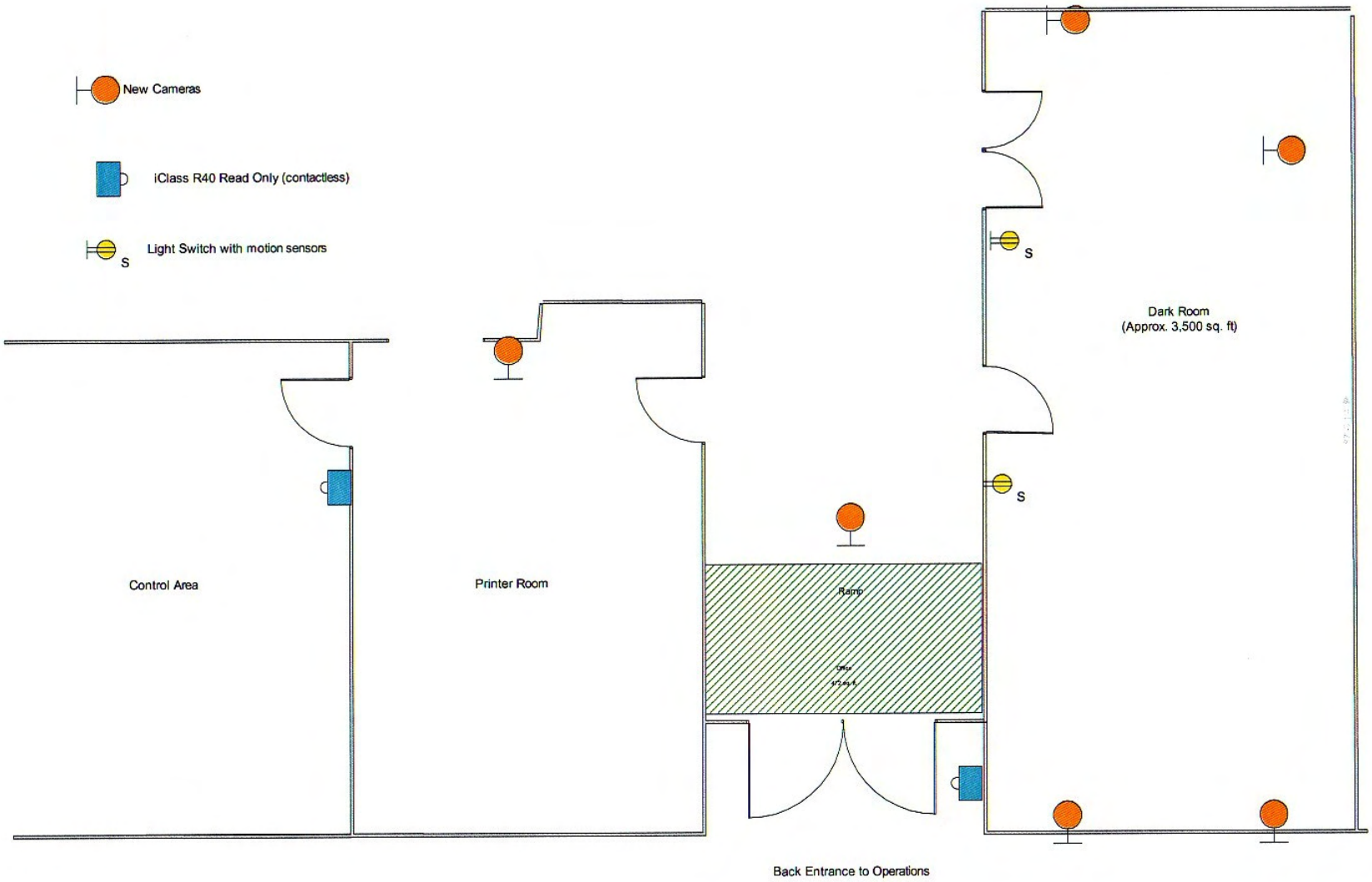
QTY	DESCRIPTION
1	Door Controller
1	1200 LBS Maglock
1	REQUEST TO EXIT PIRS
1	945WH MAGNET ASSY, WH
1	iCLASS R40 READ ONLY contactless smart card reader, Wiegand output, US/EU/Asian back box sizes , read range 1 to 3.5 inches (2.5 to 8.9 cm), 80/230mA Avg/Peak @ 12 VDC, color BLACK
	Digital Video
1	Additional Single LNR Channel- Support for an additional IP / Network based camera channel to be used with (PC-LNR8-3U) Turnkey Solution. (maximum of 32 IP/network channels per LNR)
1	AXIS 211 - Feature-rich network camera with CCD sensor, ideal for professional indoor and outdoor monitoring, has built-in Power over Ethernet, motion detection and delivers superior image quality in simultaneous MPEG-4 and Motion JPEG at up to 30 fps. Includes vari-focal DC-iris lens, adjustable stand and power supply.
1	Mini Magnum Housing with 8" Bracket
20	Cabling and Hardware Equipment Installation, Configuration, Termination, and Testing.
	*** Software Installation, Configuration, and 4 Hours End-User Training.
	*** - Presumes existing IP connectivity is available, and usage of existing Lenel system database software license (HFD).
	Hawaii State Tax

Signature & Date

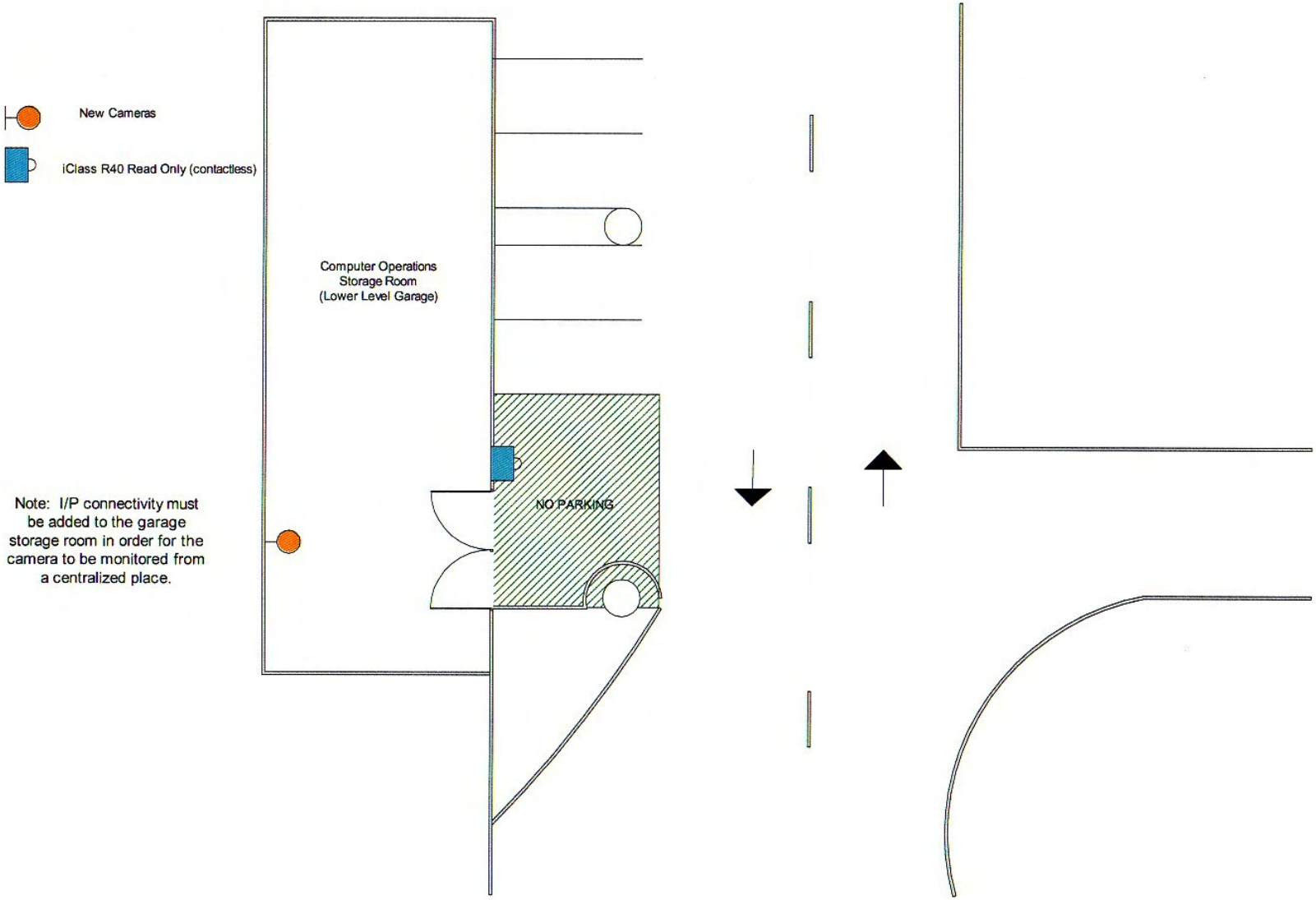
* This proposal is only good for (30) days from proposal date. *



Last revised 09/07/2005



Last revised 09/07/2005



Note: I/P connectivity must be added to the garage storage room in order for the camera to be monitored from a centralized place.

Last revised 09/07/2005