A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2004-0310-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON INFORMATION TECHNOLOGY CONTROLS
AT THE DEPARTMENT OF TRANSITIONAL ASSISTANCE

July 1, 2002 through August 24, 2004

OFFICIAL AUDIT REPORT
JUNE 1, 2005

2004-0310-4T

TABLE OF CONTENTS

INTRODUCTION

The Department of Transitional Assistance (DTA) is organized under the authority of Chapter 18, Section 1, of the Massachusetts General Laws, as amended, and is under the purview of the Executive Office of Health and Human Services' (EOHHS) Office of Children, Youth, and Human Services. The DTA operates from a central office in Boston and is organized into four regional areas that oversee 31 Transitional Assistance Offices (TAOs) throughout the Commonwealth. The DTA is comprised of a commissioner, a deputy commissioner, four assistant commissioners, a general counsel, a director of hearings, and a director of equal opportunity who have overall responsibility for operational programs, such as field operations, management information systems, policy and program management, and administration and finance. Four regional directors supervise operations at the TAOs while DTA is staffed by approximately 1,600 employees.

The DTA's mission is to assist eligible individuals and families with inadequate income and resources to move towards self-sufficiency. To help them with this transition, DTA provides them with interim services, cash and food stamp benefits and emergency assistance. To achieve its goal, DTA operates a variety of financial assistance programs for families, elders, and disabled people. Transitional Aid to Families with Dependent Children (TAFDC) provides monthly financial assistance to approximately 49,000 households representing approximately 112,000 individuals. Unless otherwise exempted, benefits are limited to 24 months in any 60-month period. Approximately 156,000 elderly and disabled people receive income assistance through the federal Supplementary Security Income (SSI) program. Emergency Aid to Elderly, Disabled and Children (EAEDC) provides income assistance to about 16,000 individuals who do not qualify for TAFDC or SSI. The Food Stamp (FS) program provides benefits to approximately 124,000 individuals most of whom receive income assistance through other DTA programs. DTA relies heavily on information technology to help carry out its mission and business objectives. For fiscal year 2004, DTA administered over one billion dollars, comprised of a state budget appropriation of $830 million and an additional $200 million in federal Food Stamp benefits.

In March 1996, DTA developed an Implementation Advance Planning Document to develop the Benefit Eligibility and Control On-line Network (BEACON) system that would replace the Program Automated Calculation and Eligibility System (PACES) that was the prior mainframe-based legacy system implemented in the early 1980s. The BEACON system was developed as a local area network (LAN)-based, custom-designed, comprehensive, integrated, automated system. State and federal monies were used to fund the development of BEACON. According to DTA, the total cost for the development and implementation of BEACON was approximately $63.56 million, of which approximately $34.96 million (55%) was comprised of state funds and $28.6 million (45%) was comprised of federal funds. According to DTA senior management, the implementation of the BEACON system was required to

address the significant limitations and deficiencies of PACES to support caseworker administration, assessment, and benefit delivery.

BEACON was developed to properly support caseworkers in the following functions: intake and screening, assessments, case management, benefit services, family resource services, and to help ensure system availability and meet regulatory requirements, such as those for federal reporting. According to senior management, caseworkers using BEACON must enter recipient data only once. In addition, the system automatically applies the information across all possible aid programs, helping to enhance caseworker productivity and assure that eligibility guidelines are followed across all programs and TAOs. BEACON functions calculate benefits such as cash assistance and food stamps, track clients' paths into the working world, schedule appointments, issue day-care vouchers, and send notices informing recipients of benefit changes. The system was developed using an object-oriented application development toolkit known as Forté and the Oracle relational database. All data necessary to determine eligibility and benefit amounts is stored in the Department's Oracle database. Once the data is verified through external sources, eligibility and the benefit amount is calculated online, authorized notices are produced, and benefits are issued through the Financial Management Control System via electronic benefit transfer, direct deposit, or check.

The DTA information technology (IT) infrastructure used to support BEACON and administrative applications consists of local area networks (LANs) installed at the central office, and at regional and area offices linking over 1,600 workstations to a Novell network for print and file servers. At the start of our audit, the LANs were linked via routers to a frame relay, wide area network (WAN), that ran TCP/IP over T1 lines connected to DTA's Network Operations Center (NOC) at 600 Washington Street in Boston.

During our audit, DTA was in the process of completing its Dual Data Center project. This project will have the primary production data center migrate from the 600 Washington Street address to the Massachusetts Information Technology Center (MITC) in Chelsea. In concert with the Commonwealth's Information Technology Division (ITD), DTA will maintain their connectivity at 600 Washington Street in order to create this dual data center "hot site" backup facility in Boston. DTA offices will be able to access BEACON data files and software directly through the WAN to the MITC's file server containing the BEACON database via ITD's Massachusetts Access to Government Networks (MAGNet).

Our Office's examination focused on a review of selected internal controls over the BEACON system, specifically physical security and environmental protection controls over IT resources at the central office, TAOs, and a sample of area offices; system access security; business continuity planning; and on-site storage of computer-related media. In addition, we reviewed control practices over and within DTA's IT environment and data integrity related to TAFDC case records within the BEACON system.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Department of Transitional Assistance (DTA) for the period of July 1, 2002 through August 24, 2004. Our audit scope included a general control examination of internal controls related to the organization and management of IT activities and operations including strategic and tactical planning, physical security and environmental protection over the DTA IT infrastructure, business continuity planning, and on-site and off-site backup magnetic media storage. We also performed an evaluation of IT-related contract management and DTA's compliance with the Information Technology Division (ITD)'s policy regarding enterprise security as they relate to DTA's access security.

Our audit scope included an assessment of the adequacy and effectiveness of controls in place to protect the integrity of Benefit Eligibility and Control On-line Network (BEACON) data. Consequently, we performed an assessment of controls in place by DTA to ensure that Transitional Aid to Families with Dependent Children (TAFDC) benefits are being provided only to eligible applicants. The audit was conducted from November 13, 2003 through August 24, 2004.

Audit Objectives

Our primary audit objective was to determine whether DTA's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support DTA's business functions. In this regard, we sought to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required.

Our audit objective regarding organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and whether IT-related policies and procedures adequately addressed the areas under review. We also sought to determine whether DTA had implemented IT-related strategic and tactical plans that help to fulfill DTA's mission and goals and whether DTA had appointed a steering committee to oversee its information technology division and activities.

We sought to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to DTA's data files. We sought to determine whether procedures were in place to prevent and detect unauthorized access to automated systems and IT resources including the UNIX, BEACON, Oracle, LAN file servers, and microcomputer systems. In

addition, we determined whether the BEACON system data was sufficiently protected against unauthorized disclosure, change, or deletion and whether DTA was in compliance with the ITD's enterprise security policy.

We further sought to determine whether adequate physical security controls were in place to provide reasonable assurance that access to the NOC and the on-site and off-site media storage areas was limited to authorized personnel. Moreover, we sought to determine whether sufficient environmental protection was being provided to prevent and detect damage or loss of IT-related equipment and media.

Regarding systems availability, we sought to determine whether adequate business continuity plans were in effect to help ensure that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render processing inoperable or inaccessible. Moreover, we sought to determine whether adequate controls were in place to provide reasonable assurance that appropriate magnetic backup copies of application systems and data files would be available on-site and off-site to support disaster recovery and business continuity planning objectives.

Regarding data integrity, we sought to determine whether information necessary for determining eligibility and providing benefits and referrals for services contained in source documents within TAFDC case records was accurately and completely recorded within the BEACON system. We also sought to evaluate DTA's policies and procedures for issuing facsimile or "dummy" social security numbers (SSN) to TAFDC applicants.

We sought to determine whether contractual relationships with third-party IT-related service providers were covered by written contracts, the contract agreements sufficiently detailed services or deliverables to be provided, and the contracts were properly signed and dated. We determined whether incorporated vendors were properly registered with the Office of the Secretary of State. In addition, we determined whether IT-related contract services had been monitored and evaluated for the provision of adequate services and deliverables.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of DTA's mission and business objectives. Through pre-audit interviews with managers and staff and reviews of documents, such as descriptions of DTA's organization and operations, we gained an understanding of the primary business functions supported by the automated systems. We documented the significant functions and activities supported by the automated systems, and reviewed automated functions related to operations designated as mission-critical by DTA.

As part of our pre-audit work, we reviewed and evaluated the organization and management of IT operations at DTA's central office. We inspected the central office in Boston, including the network operating center; reviewed relevant documents, such as the network configuration, internal control plan,

and business continuity plan; and performed selected preliminary audit tests. We interviewed DTA management to discuss internal controls regarding physical security and environmental protection over and within the network operating center housing the file servers, the business offices where microcomputer workstations are located, and the on-site and off-site storage areas for mission-critical and essential magnetic media storage. In conjunction with our audit, we reviewed written, authorized, and approved policies and procedures for control areas under review. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with regulations and to meet generally accepted control objectives for IT operations and security.

To determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft or damage, we performed audit tests at the central office, including the NOC. We also reviewed and evaluated physical security at selected TAOs and their associated file rooms. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with DTA management and staff.

To determine whether adequate controls were in effect to prevent and detect unauthorized access to the selected business offices housing IT resources, we inspected physical access controls, such as the presence of security personnel on duty, locked entrance and exit doors, the presence of a receptionist at the entrance point, intrusion alarms, and whether sign-in/sign-out logs were required for visitors. We reviewed physical access control procedures, such as the lists of staff authorized to access the NOC, magnetic key management regarding door locks to the central office's entrance, and other restricted areas within the central office. We determined whether DTA maintained incident report logs to record and identify security-related events, such as unauthorized entry attempts, threatening phone calls, or thefts of computer-related equipment.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS) and surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server room or in the vicinity of computer-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air conditioning units in business offices and the NOC which houses the file servers. Further, we reviewed control procedures to prevent water damage to automated systems, agency records, and magnetic backup media stored on site.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated microcomputer systems. To determine whether DTA control practices regarding system access security would prevent unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the Director of System Security and LAN Manager responsible for management of the network and evaluated selected controls to the automated systems. In conjunction with our review of network security practices, we reviewed control practices regarding remote user procedures to the Commonwealth's internal network known as the Massachusetts Access to Government Networks (MAGNet), via the Virtual Private Network (VPN).

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the LAN Manager responsible for access to the file servers and microcomputer workstations on which the DTA's application systems operate. In addition, we reviewed control practices used to assign and grant staff access privileges to the application programs and data files. To determine whether controls in place were adequate to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application systems and related data files. We reviewed documents recording the granting of authorization to access automated systems and requested and received a current listing of users. In order to confirm whether access privileges to the automated systems were granted to only authorized users, we compared the user lists received to an active employee list. To determine whether DTA users with active privileges were current employees, we obtained the list of individuals with access privileges to the network and microcomputer workstations and compared all users with active access privileges to DTA's personnel roster of current employees. Further, we determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to resume mission-critical and essential operations in a timely manner should the file servers and the microcomputer workstations be unavailable for an extended period. We interviewed the Director of System Security and LAN Manager to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place and had been periodically reviewed. Further, we reviewed and evaluated procedures in place to resume normal business functions should the file servers or the microcomputer workstations be rendered inoperable.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we interviewed

DTA management responsible for generating backup copies of magnetic media for administrative work processed at DTA and applications such as the BEACON system residing on the file servers. Further, we reviewed the adequacy of provisions for on-site backup copies of mission-critical and essential magnetic media at the central office. We did not review the off-site storage location for backup copies because it was under third-party contract reviewed in prior audits. We did not review ITD's backup procedures for transactions processed through MMARS and HR/CMS.

We sought to assess the internal control process for third-party provider service IT contracts. We sought to determine whether provider service contracts have been properly put out to bid and awarded and whether vendor payment vouchers were reviewed, approved, and contained the required authorized signatures. In addition, we sought to determine whether the DTA had implemented adequate controls to provide reasonable assurance that monitoring and evaluation of provider service contracts was being performed in accordance with applicable Massachusetts General Laws and generally accepted business practices.

To assess the effectiveness of the TAFDC eligibility determination process, we sought to determine whether DTA complied with Federal requirements for verifying applicants' immigration status, the Commonwealth's requirements for assessing the reliability of applicants' eligibility information, as well as initial and ongoing eligibility determinations were correctly performed and monitored at five local TAOs. To be eligible to receive TAFDC benefits, individuals must meet certain requirements. For example, their income cannot exceed a certain level, they generally must participate in employment-related activities, and they must be a U.S. citizen or a qualifying alien. The specific requirements are set by each state, and must comply with overall Federal requirements. We interviewed senior management and reviewed policies and procedures at DTA and five local TAOs: Brockton, Dorchester, Lawrence, Newmarket, and Worcester. We selected these local offices because they had relatively high TAFDC caseloads and comprised 32% of the Commonwealth's current active TAFDC participants at the time of our audit. As of June 25, 2004, we selected from the 49,767 active TAFDC cases a random sample of 200 from these five local TAOs (40 from each office) to determine whether they were correctly performed.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices and auditing standards.

AUDIT CONCLUSION

Based on our audit at the Department of Transitional Assistance (DTA), we found that adequate controls were in place to provide reasonable assurance that IT-related control objectives would be met for system access security, physical security, environmental protection, and the generation and storage of on-site and off-site copies of backup media. However, the updating and maintaining of information contained in the Benefit Eligibility and Control On-line Network (BEACON) application system for Transitional Aid to Families with Dependent Children (TAFDC) needs to be strengthened to ensure an adequate level of data integrity. In addition, controls need to be strengthened to provide reasonable assurance that control objectives regarding system availability, monitoring and evaluation of IT vendor service contracts, and IT strategic and tactical planning will be met.

Our review of IT-related organizational and management controls indicated that DTA was aware of the need for internal controls and had a defined organizational structure for the agency, an established chain of command, and documented job descriptions for information technology staff. We also found there were clearly delineated reporting responsibilities for IT functions and other associated business functions we reviewed. However, our review of IT-related planning found that DTA had not developed a comprehensive strategic or tactical plan to address IT functions within the Department or across the TAOs. We determined that although short-term plans existed, they lacked sufficient detail regarding assignments, priorities, milestones, or performance metrics.

Although DTA is required to document and maintain certain information to support eligibility for TAFDC recipients, our test of original source documentation demonstrated that monitoring procedures needed to be strengthened to ensure continued data integrity. We determined that data elements regarding the identification of applicant, date of birth, Social Security Number (SSN) or SSN application date, relationship of child to grantee, U.S. citizen or Immigration and Naturalization Service (INS) designation, and residence tested at an error rate of zero to six percent**.** However, our sample of cases examined reflected error rates ranging from 10 to 21 percent for the four other data elements regarding immunization or school verification, verification of employment/non-employment, signed application by parent/guardian, and verification of non-custodial absent parent. We noted that the required supporting documentation was either missing or incomplete regarding these four data elements and as a result, we estimated that cash payments to possibly ineligible clients within the sample drawn totaled approximately $263,000 during the time of examination. In most of the 153 data element errors we identified in the sample drawn, the non-compliance resulted from either clients or caseworkers not reporting and/or recording changes to TAFDC status subsequent to clients' initial eligibility.

Our test of the BEACON system revealed that ineligible non-citizens were receiving benefits. We determined this was due to a breakdown in internal controls, particularly with regard to the risk assessment related to the BEACON system and a result of "worker and supervisory error". After further examination, our findings indicated a change in DTA policy had taken place which contributed to non-citizens receiving benefits. The ineligible non-citizens identified had an immigration status of "Undetermined" per a new DTA policy. However, because of this recent change in DTA policy, combined with a lack of cross edit checks within the BEACON system against eligibility and the limited feedback to case workers, these ineligible recipients were allowed to receive benefits for an extended period of time of up to six months.

We determined that in order to create a TAFDC record in the BEACON system, DTA issued facsimile or "dummy" social security numbers that begin with 99 to individuals who had supporting documentation that they had applied for a social security number. Although this is slated as a temporary number, we determined that DTA does not systematically reverify eligibility information regarding TAFDC active participants who have been assigned "dummy" social security numbers. This failure to re-verify eligibility information allowed certain TAFDC recipients to receive questionable benefits for extended periods, some for over six years, without a valid social security number.

Our examination of physical security revealed that controls provided reasonable assurance that DTA's IT resources were safeguarded from unauthorized access. We found that the Network Operating Center was locked, and that a list was maintained of individuals who had access to keys. The DTA had full-time security guards on duty 24 hours per day, seven days per week, and the facility was equipped with intrusion alarms. However, we found that physical security over the NOC could be strengthened by the elimination of an interior window that separates the NOC from the office environment.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply, were in place in the building housing DTA to help prevent damage to, or loss of, IT-related resources. Our audit disclosed that the Network Operating Center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We found that an uninterruptible power system (UPS) was in place to prevent sudden loss of data, and hand-held fire extinguishers were located within the NOC. Evacuation and emergency procedures were documented and posted within DTA's central office inclusive of the NOC. According to management, staff had recently been trained in the use of these emergency procedures. However, we found that environmental protection over the NOC could be strengthened by formally documenting the emergency procedures for shutting down IT equipment.

Regarding system access security, our audit revealed that DTA had developed and documented appropriate procedures regarding the granting of access privileges to automated systems and activation of

logon IDs and passwords. Regarding procedures to deactivate access privileges, we found that informal procedures were in place to deactivate access privileges for users no longer authorized or needing access to the automated systems. Audit tests of access security that compared 160 (10%) randomly-selected users to DTA's payroll roster of current employees confirmed that the users were current employees. Further, we determined that appropriate control procedures were in place regarding granting of limited access privileges to individuals working in other entities.

Our audit indicated that adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media. We determined that DTA had implemented procedures and schedules for generating backup copies of magnetic media, and had documented procedures for maintaining descriptions of data files and software that were backed up. Documentation was in place indicating which backup tapes were stored off-site and logs were maintained demonstrating the authorized schedule for the transport and return of backup copies. However, we found that physical security and environmental protection over the on-site storage location needed to be strengthened. For their on-site storage, DTA stored backup tapes in an unsecured cabinet within the NOC, which could be destroyed in the case of a fire, along with data and programs residing on the server. Previous audits of DTA's off-site storage provider did not indicate any issues requiring that a site visit to the storage facility housing off-site backup copies of magnetic media was needed.

Although on-site and off-site storage of backup media was in place, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. We found that there was a general absence of documented plans to address disaster recovery and business continuity for automated operations. Our audit disclosed that DTA did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for the BEACON system could be regained effectively and in a timely manner should a disaster render automated systems inoperable. Although we found that there was a Y2K rollover plan from December 1999, it had not been updated, nor had user area plans been established to document the procedures required to regain business operations in the event of a disaster.

Our review of DTA's IT-related service contracts revealed that all contracts reviewed were properly signed and approved, and all vendors incorporated as either a foreign or domestic corporation were found to be properly registered with the Commonwealth's Office of the Secretary of State. We also determined that the DTA used the competitive bid process to award IT-related service contracts. However, DTA did not have in place established written internal control policies and procedures for third-party service contract monitoring and evaluation for their use throughout the agency. Consequently, this could contribute to inconsistent monitoring of third-party IT-related service contracts to ensure that the Commonwealth received the goods and services that it had contracted and paid for.

AUDIT RESULTS

1. Data Integrity

With respect to data integrity, the Department of Transitional Assistance's initial establishment of TAFDC case files and initial determination of eligibility benefits indicated that appropriate controls were in existence and that nothing came to our attention to indicate weaknesses existed in this area. However, our audit determined that there was an increased level of risk regarding the continued monitoring and evaluation by caseworkers of TAFDC case documentation, payments to ineligible TAFDC recipients, and TAFDC clients providing social security numbers in a timely manner. Our review of DTA's requirement to document and maintain certain information to support eligibility for TAFDC recipients indicated that not all data files were updated and maintained to an extent necessary, resulting in a reduced level of data reliability and possible payment of funds to ineligible parties. We also determined that ineligible non-citizens were receiving TAFDC benefits due to inadequate internal controls related to the BEACON system, and that weaknesses in DTA's policy had enabled clients to receive TAFDC benefits for an extended period of time without obtaining a required social security number.

To receive TAFDC benefits, families must apply at a DTA TAO serving the area in which the family lives or works. At the TAO, an assigned case manager determines the family's eligibility for program benefits and provides the necessary case management services. Families receiving TAFDC must meet specific eligibility requirements based on income and household composition. In addition, to remain on the program, clients must periodically reapply for TAFDC benefits and report changes that may affect their status.

Although DTA is required to document and maintain certain information to support eligibility for TAFDC recipients, we determined that DTA needed to strengthen their monitoring and evaluating procedures to ensure continued data integrity regarding TAFDC case documentation. Contingent upon TAFDC initial and continued eligibility determination, the audit team selected ten financial and non-financial data elements for audit purposes. We then tested 197 active TAFDC cases and determined whether each case had supporting documentation for each of the ten data elements selected, and determined whether individuals were at risk of not meeting selected eligibility requirements. The results of these tests indicated, with a reasonably high level of confidence, that the supporting documentation regarding the intake of cases were done accurately and completely. The failure to consistently update changes to TAFDC status subsequent to clients' initial eligibility to ensure that data integrity was maintained resulted in data elements with incomplete or missing support documentation. We estimated that cash payments to potentially ineligible clients for the sample of cases drawn would total approximately $263,000 during the audit test period.

The audit team requested and received from the Department of Transitional Assistance a copy of the TAFDC Benefit Eligibility and Control On-Line Network (BEACON) system-generated data file of all active records. We subsequently reviewed and analyzed the BEACON Access Database generated report outlining all active TAFDC cases and their associated active cases. We determined that, as of June 25, 2004, the TAFDC database consisted of 49,767 active cases administered by DTA's local Transitional Assistance Offices (TAOs).

The ten data elements the audit team attempted to validate through a review of source documentation were:

1. Identification of applicant
2. Date of birth
3. Social Security Number (SSN) or SSN application date
4. Relationship of child to grantee
5. U.S. citizen or Immigration and Naturalization Service (INS) designation
6. Employment income or reason not employed
7. Continued absence or reason for absence of parent
8. Signed and dated application
9. Residence
10. Up-to-date immunization or school verification record

To determine the integrity of BEACON data, we selected a sample of case files from five local TAOs to provide an adequate representation of the TAFDC case files. The five TAOs selected; Brockton, Worcester, Dorchester, Lawrence, and Newmarket Square, were responsible for processing 32% of the 49,767 active TAFDC cases. We randomly selected a total of 200 TAFDC cases from the five TAOs, representing 40 cases per site, to determine whether the cases were properly initiated, reviewed, and monitored based on TAFDC eligibility requirements. We tested 197 of these (3 had closed between the time we generated our sample and the time we conducted our tests) by reviewing their BEACON TAFDC case files as of June 25, 2004 and tracing selected elements of this data to supporting source documentation kept as hardcopy in the respective case file. Although we sampled 197 TAFDC cases, the actual number of data elements we tested varied, depending on the type of case and whether the recipients were designated as a grantee. In total, our sample included 1,920 data elements reviewed. We determined that 153 (or 8 percent) of these elements lacked the required supporting documentation. DTA is required to follow 106 CMR: Department of Transitional Assistance, The Eligibility Process Chapter 702, Section (702.410: Documentation in the Case Record). This section states, "*The case record is the permanent collection of the information necessary for determining eligibility and providing benefits and referrals for services. All decisions regarding eligibility and case actions must be based on information documented in the case record*." A more complete breakdown of source documentation errors are illustrated in the chart below:

Data Element Number	1	2	3	4	5	6	7	8	9	10	TOTALS
Data Elements Reviewed	197	197	197	161	197	196	190	197	197	191	1,920
Data Elements Correct	192	195	197	157	194	154	171	167	185	155	1,767
Data Elements Incorrect	5	2	0	4	3	42	19	30	12	36	153
Percent Correct	97%	99	100%	97%	98%	79%	90%	85%	94%	81%	92%
Error Rate	3%	1	0%	3%	2%	21%	10%	15%	6%	19%	8%

Our test determined that supporting documentation for the case record was either missing or incomplete for:

- 42 (21 percent) out of the 196 case records regarding the reason a grantee is either not employed or verification of employment income;
- 36 (19 percent) out of the 191 case records regarding the verification of immunization or school enrollment for children over the age of 16;
- 30 (15 percent) out of the 197 case records requirement of a signed and dated TAFDC application; and
- 19 (10 percent) out of the 190 case records requirement of verification for a parents continued absence verification or reason for absence.

Considering that the sample drawn may be representative of the population of all cases, we have projected the risk of potential overpayment for the then current case load. The projected potential overpayment amounts should be used as an indicator for decisions regarding the allocation of resources and management direction in strengthening controls. We understand and fully appreciate that there is a level of risk of overpayment, as well as underpayment. We acknowledge that there are circumstances where clients may not be forthcoming with updated information. However, we also believe that assurance mechanisms to assess the integrity of primary data elements for eligibility can serve as valuable indicators as to whether program functions are within established tolerances.

Regarding immunization requirements, the Code of Massachusetts Regulations 106 CMR 203.800: Immunizations, (A) Requirements, states, "*The grantee must ensure that each dependent child is properly immunized. Failure to comply with this requirement shall result in the ineligibility of the grantee. The grantee must provide verification of the dependent child's immunization at application, upon notification of the birth of a dependent child who will be included in the assistance unit, and when the dependent child turns age two*." 106 CMR 203.800: Immunizations, (C) Sanction for Noncompliance with Immunization Requirement states "*When a grantee fails to comply with these requirements without good cause, he or she will be sanctioned by a denial or a reduction of cash benefits in an amount equal to his or her portion of the assistance grant. In two-parent households, both parents will be sanctioned for failure to comply with this requirement*."

School verifications for recipients, until the age of 14, are regulated by the Code of Massachusetts Regulations 106 CMR 203.900: Learnfare, (A) Requirements, states, "*A dependent child(ren) under the*

age of 14 must attend school regularly." Verifications regarding a child's attendance for recipients between the ages of 6 and 14 are completed through a separate computer mainframe system outside of the BEACON known as the Learnfare Tracking system. Because we did not have access to the Learnfare Tracking system, those individuals who had either missing/incomplete source documentation or data input within the BEACON system were not counted as either missing or incomplete in our TAFDC test case results. Although school attendance for a child under the age of 18 is not required as a condition of TAFDC eligibility, those who are enrolled, according to the Department of Transitional Assistance A User's Guide, age 16 and older, must verify:

- current school status,
- highest level of education,
- attendance requirements for teen parents and pregnant teen grantees, and
- expected date of graduation for an assessed person from ages 16 through age 18.

Primarily, DTA's "School Verification Notice," SV-1, serves as the means by which caseworkers verify these aforementioned requirements for these individuals 16 and older, and unlike the Learnfare Tracking system, either missing/incomplete source documentation or data input within the BEACON system was counted as either missing or incomplete in our TAFDC test case results. Immunizations help protect children from diseases such as chicken pox, polio, tetanus, measles, mumps, rubella (German measles), diphtheria, pertussis (whooping cough), Hib disease, and hepatitis B. These diseases are especially dangerous for babies and toddlers. Without proper immunizations, a child is at greater risk for a disease that could result in death, blindness, brain damage, paralysis or heart problems.

While taking into consideration that some of the sample items could have been in error throughout the audit period while others may have occurred during the audit period, if left uncorrected, all identified problem cases would have been in error at the end of the audit period, to which a potential overpayment could be identified. Based on 106 CMR 204.410 and 204.415, Table of Need Standards, on average, each additional individual (assistance unit) associated with a TAFDC claim benefit amounts to $101 per month. Based on our audit sample results, over $43,632 per year may have continued to be improperly distributed to individuals that should have been sanctioned by a reduction in cash benefits until the proper documentation was provided. If one were to take the immunization and school verification test error rate of 19 percent and apply it to the current TAFDC caseload of over 49,000, one could project a possible risk of benefit overpayment of over $11 million per year if left uncorrected. It is important to note that although the supporting documentation may be incomplete or absent from the case files, in itself that does not solely determine whether the child has been properly immunized or is enrolled in school.

According to DTA's A User's Guide, TAFDC Work Program Requirement, "*Under the Work Program, certain able-bodied grantees (applicants and recipients) have a 60-day work search period in which to find a job of at least 20 hours per week. A grantee who does not get a job within the 60-day*

work search period, or if the youngest child in the grantee's assistance unit is between the ages of two and school age, participate in an education or training activity or does not prove good cause for failure to meet the Work Program Requirement, must work at a Community Service site."

In order to obtain TAFDC assistance, certain clients must be qualified through the User Guide Work Program Requirement guidelines. DTA may assign clients to perform 20 hours of unpaid work for a nonprofit or government agency if the client is unable to find their own community service placement, paid job, or combination of the two for at least 20 hours a week. In order to be exempt from this requirement, clients have to fit one of the following categories:

- have a mental or physical health problem; or
- have to care for a physically or mentally disabled child, spouse, parent, or grandparent.

For the purpose of our test we determined whether the associated documentation for Work Program verification was, in fact, included within the TAFDC test cases. We determined that in 21 percent of the cases, documentation was either missing or incomplete. For example, required verification detailing a client's last job was in some cases missing, while other case files had missing pay stubs required to support an individual's current employment. The Code of Massachusetts Regulations requires the following: 106 CMR 207.200: Failure to Meet Employment Development Plan (EDP) Requirements or the Work Program Requirements, states, "*An individual who, without good cause … fails to meet the work program requirements or fails to fulfill the obligations of the EDP, … shall be sanctioned…*" Sanctioning is similar to the sanctioning involved for the aforementioned immunization and school verification requirement.

Based on our audit results, $50,904 per year may have been improperly distributed to individuals that should have been sanctioned by a denial or reduction in cash benefits until the proper documentation was provided. It is important to note that although the supporting documentation may be incomplete or absent from the case files, in itself that does not solely determine whether an individual has in fact been actively employed. It also should be noted that approximately 25% of the individuals associated with TANF cases are currently required to perform some type of work program. However, if one were to project, applying the work program requirements verification test error rate of 21 percent found in our sample and apply it to 25 % of the current TAFDC caseload of over 49,000, one could project a possible risk of benefit overpayment of over $3 million per year if left uncorrected.

A total of 30 claims in our statistical sample of 197 claims were not supported by properly signed and dated applications for TAFDC. The Code of Massachusetts Regulations, 702.115: Filing of Applications: (B) Definition, states, "*An application is a signed and dated request for assistance on a form prescribed by the Department. The application is filed when the applicant signs and dates the prescribed forms*." Since a TAFDC application that is incomplete or missing cannot support or attest to a

particular TAFDC case, this places into question whether the decisions made regarding benefits and services were in fact for eligible applicants only. Based on our audit results, cumulative payments to recipients in the amount of $145,813 per year could not be supported by a proper signature of a parent or guardian for the sample drawn. Based on the quality control process of the cases and data elements reviewed, if one were to project these errors to the universe of claims, the possible risk of benefit overpayment could be estimated at over $35 million per year. It is important to note that although the supporting documentation may be incomplete or absent from the case files, that in itself does not solely determine whether an individual has not signed the initial application.

As part of a broad effort to reform the nation's welfare system, the United States Congress made significant changes to Federal policy regarding client child support cooperation requirements in the Personal Responsibility and Work Opportunity Act of 1996. Currently, unless exempted from cooperation requirements through a good cause or other exception, TAFDC clients must name and provide information about the noncustodial parent of their children, and cooperate in any way possible with the Commonwealth. DTA requires clients to complete the "Assignment of Support Rights, Cooperation with Child Support, or Good Cause Claim Form (T-A34/36 (7/2002)" as well as a BEACON-generated "Declaration of Absent Parent Affidavit" in order to fulfill both these mandated requirements. Formerly, state public assistance agencies determined whether clients were cooperating with their state's child support agency; however, welfare reform made state child support agencies responsible for determining if clients were cooperating in "good faith" and notifying the public assistance agency of each client's cooperation status. According to DTA's A Users Guide, Absence, Sanctions, states, "*Benefits for the assessed person will be denied by having the benefits for the Assistance Unit reduced by an amount equal to one member's portion of the TAFDC benefits*." As indicated, based on our audit results, cumulative payments to recipients in the amount of $23,028 per year could not be supported by the aforementioned documentation for the sample drawn. Again, this sanction is comparable to the immunization sanction mentioned previously. If one were to take the noncustodial absent parent verification test error rate of 10 percent and apply it to the current TAFDC caseload of over 49,000, one could project a risk of potential benefit overpayment of over $6,030,340 per year. It is important to note that although the supporting documentation may be incomplete, or absent from the case files, that in itself does not solely determine whether an individual has in fact been identified as the absent parent.

Because most of the TAFDC case files had multiple documentation errors, our estimates for the individual errors are not mutually exclusive of each other and should not be added together. The estimates that are presented below are only to show the possible effect the individual errors could have on the sample and the entire active DTA's TAFDC case claims on an annualized basis.

Types of Data Element Errors			
Documentation Errors	Number of Actual Errors in Test	Projected Possible Overpayment Amounts for TAFDC Test Cases	Projected Possible Overpayment Amounts for Entire TAFDC Cases
Ineligibility of the TAFDC Service			
1. No Immunization or School Verification	36	$43,632	$11,489,460
2. No Verification of Employment/Nonemployment	42	$50,904	$3,149,698
3. No Signed Application by Parent Guardian	30	$145,813	$35,025,780
4. No Verification of Noncustodial Absent Parent	19	$23,028	$6,030,340
Actual Totals	136	$263,377	N/A

Regarding ineligible non-citizens receiving TAFDC benefits, the audit team selected a random sample of Transitional Aid to Families with Dependent Children (TAFDC) recipients from the active population in order to determine through testing whether the recipients were eligible for TAFDC benefits, based upon the information in the BEACON system. We determined that of the 25 randomly-sampled TAFDC recipients tested, two were ineligible non-citizens receiving TAFDC benefits based upon the information in the BEACON system. The two ineligible non-citizens had an immigration status of "Undetermined" per DTA policy. However, because of the relatively recent DTA policy change combined with a lack of cross edit checks within the BEACON system against eligibility, these two individuals were allowed to receive benefits for an extended period of time. The total amount paid for the ineligible non-citizens that we identified in this sample had incorrectly received $2,212 in TAFDC benefits.

In response to our test results, DTA identified the two recipients as "incorrectly aided" and started the termination and subsequent reimbursement process for the applicants mentioned above, citing "…*worker and supervisory error*." Upon our notification to senior management regarding the two non-citizens receiving TAFDC benefits, DTA administrators initiated a Systems Request (SR) within the BEACON system that queried all active TAFDC case files in order to identify any similar instances of ineligible non-citizens receiving TAFDC benefits. This SR queried and identified an additional 76 ineligible non-citizens that possibly may have been receiving TAFDC benefits incorrectly. DTA administrators generated from this SR a listing of these 76 individuals and distributed it to senior management and their associated managers at the monthly Statewide Directors' Meeting in April 2004. According to DTA senior management 18 of the 76 individuals listed were found to been incorrectly coded as "Undetermined" while the remaining individuals were found to be correctly coded.

DTA is required to follow the A User's Guide, Transitional Assistance Programs and BEACON, Chapter XIII, Section E, page 6, which states, "*A non-citizen who is unwilling or unable to provide acceptable verification of an eligible noncitizen status is ineligible for benefits. In such cases, the Department will not continue efforts to obtain documentation*." Page 14 of the User's Guide continues, "*AU Managers enter Undetermined as the INS Designation on BEACON when a non-citizen refuses or is unwilling to submit documentation of non-citizen status, does not verify an illegal status*…" DTA is also required to follow the Transitional Aid to Families and Dependent Children (TAFDC) Nonfinancial Eligibility Policies, 106 CMR Chapter 203.675, which states, "…*A non-citizen unwilling or unable to provide acceptable verification of an eligible non-citizen status is ineligible*."

We determined the cause of these improper payments could be traced to a lack of, or breakdown in, internal control regarding the BEACON system and that DTA had not performed a risk assessment related to the change in eligibility status for non-citizens. Internal controls are an integral component of an organization's management system that provides reasonable assurance that the organization achieves its objectives of effective and efficient operations, reliable financial reporting, and compliance with laws and regulations and prevents and detects undesired events. The five components of internal control include the control environment, risk assessment, control activities, information and communication, and monitoring.

We defined a risk assessment as any systematic method for identifying risks and exposures, and assessing the degree of risk, or potential vulnerability, associated with an entity, or function or process. Through risk identification it assists management efforts in risk management and in the design, implementation and exercise of internal controls to address the identified risks. To determine whether risks of improper payments exist, what those risks are, and the potential or actual impact of those risks on program operations. Conducting risk assessments helps to ensure that public funds are used appropriately and clients receive the proper benefits. Risk assessments also help to identify risks that need to be mitigated through internal controls. Improper payments, including fraud, may occur in several different ways in the TAFDC program, involving clients, providers, and agency personnel. For example, an inadvertent error may result in an overpayment or underpayment when:

- a client mistakenly fails to report some income,
- a provider accidentally receives payment due to a billing error, or
- as was the case with undocumented workers receiving benefits, a caseworker incorrectly records some information or makes an error in calculating a benefit amount.

DTA had limited feedback to assess whether their TAFDC program was at risk for improper payments through single state audits of the Commonwealth and other audits by state auditors and fraud units, and regular reviews of TAFDC client cases by DTA's Internal Control Unit. However, these efforts were uneven and would not constitute a risk assessment that DTA management is responsible for

performing. We determined that DTA needed more comprehensive reviews of new, changing, and rescinded program policies as they relate to the BEACON system. Senior management employs a method of risk management that includes developing bulletins that alert program staff to new and revised policies to better ensure proper implementation and reduce improper payment. However, DTA officials should establish work groups that can assess the risk of new policy initiatives and consider methods to better manage these risks as they relate to the BEACON system. DTA relies heavily on updates to the BEACON system for verifying eligibility through data matches and information received from various sources. When these BEACON system updates occur, DTA should make certain that adequate verification procedures are in place to ensure that only eligible recipients are enrolled as active TAFDC recipients.

We determined that weaknesses exist in DTA's policy that enables clients to receive TAFDC benefits for an extended period of time without an established social security number. Clients are required to provide their social security number in a timely manner. However, DTA policy does not indicate what constitutes a timely manner and whether client benefits would be withheld for their noncompliance. We also determined that the BEACON system accepts both facsimile and dummy social security numbers.

We discovered that several hundred TAFDC recipients had these facsimile or "dummy" social security numbers. Using computer-assisted audit techniques to search the TAFDC data within the BEACON system, we found 2,769 TAFDC participants having dummy social security numbers amounting to over $95,000 in questionable payments of benefits for individuals with invalid social security numbers. Facsimile social security numbers are numbers assigned to:

- a grantee/primary applicant who has not yet provided an SSN; or
- an applicant/recipient unable to obtain an SSN.

Facsimile social security numbers begin with 991 through 997 and are assigned sequentially in each Transitional Assistance Office (TAO). Dummy social security numbers are BEACON system-generated numbers assigned to assess persons (other than the primary applicant/grantee) who have applied for, but have not yet received an SSN. According to DTA personnel, some applicants who do not have their social security cards and/or newborns who have not yet been issued social security numbers are assigned these "pseudo" numbers.

While it is not always possible to obtain social security information for newborns (zero to three months), we noted that several individuals with "dummy" social security numbers were over one year old or had "dummy" social security numbers for several months or years. A "dummy" social security number is a temporary number and should be corrected to the employee's actual SSN as soon as possible.

DTA is required to follow the Transitional Cash Assistance Program General Policies, 106 CMR Chapter 701.230, Section A, Requirements, which state, "*A Social Security number (SSN) must be*

provided orally or in writing for each applicant or recipient for TAFDC …unless good cause exists in accordance with 106 CMR 701.230 (C)". Although the Transitional Cash Assistance Program General Policies, 106 CMR Chapter 701.230, Section C, Requirements, which state, "*TAFDC …may not be denied, delayed or decreased pending the issuance or verification of an SSN if the applicant or recipient has applied for an SSN …*" a level of reasonableness should be instituted. This meant that applicants with an SSN application that is over four months old should have been issued a verifiable SSN by this point in time.

The dummy social security numbers for 23 of 75 individuals tested (30%) had no record of a Social Security Application within the BEACON system verification window with some receiving benefits for over two years. Also, an additional nine out of 75 individuals tested (12%) had not been updated to a correct social security number, with some of these individuals having been enrolled for over six years. We determined that at the time of our audit, DTA had not adequately formalized their policies and procedures to identify appropriate and consistent eligibility criteria regarding the use of 900 Social Security numbers to ensure that TAFDC recipients are appropriately and consistently determined to be eligible for TAFDC benefits. Providing a social security number is a requirement for receiving TAFDC cash payments. The absence of that client information lessens DTA's ability to verify other eligibility factors such as client income.

We determined that DTA does not systematically re-verify eligibility information regarding TAFDC active participants with "pseudo" social security numbers. At the time of our audit, the reverification process appears random. Some grantees' eligibility was updated as part of various activities such as BEACON system data matches with internal and external state agencies. However, these methods do not ensure that the eligibility of the grantee population is updated or that the updates are performed timely and completely. Without systematic and timely review of eligibility information, there is no assurance that current information is used to determine how many grantees are still eligible for TAFDC benefits.

Recommendation:

DTA should set up monitoring procedures to ensure that caseworkers continuously update TAFDC recipient files with all supporting documentation required for continuing eligibility. DTA senior management should work with their in-house internal audit group to develop a risk management approach for improving controls over data integrity for data contained within the Beacon application.

DTA should develop and implement adequate uniform procedures to ensure that the eligibility status regarding the usage of 900 Social Security numbers for TAFDC recipients is determined properly, consistently, and timely. DTA should enhance their policy by determining what constitutes a reasonable period of time for TAFDC clients to provide their social security numbers. To assist caseworkers, the BEACON system should be programmed to generate written notices to clients who, after their first month

of eligibility, have not provided their social security numbers. If a client has not provided their social security number by the time frame established by DTA senior management, the BEACON system should generate a notification indicating benefits will be withheld. The Director should ensure that only eligible enrollees are receiving TAFDC, and all ineligible enrollees should be removed from the program. When possible, DTA should recover payments made to ineligible enrollees of TAFDC. DTA should ensure that verification procedures regarding TAFDC recipients are adequate, understood, and fully implemented. To evaluate the effectiveness of the procedures, reports detailing verification results should be produced regularly and reviewed for content and accuracy.

Auditee's Response:

> *While we do not dispute that there are areas in which the Department can improve its business practices, we feel that it is important to note that many of the conclusions reached in this section of the report may not be an accurate reflection of the scope of the problems noted. For example:*
>
> *In the case of work related documentation, it appears that the methodology conflates verifications that individuals are meeting required work activities with the initial verification that an individual is not employed. These are two distinct matters and the verification requirements are necessarily different. The former has to do with those who are working or participating in work related activities and is verified by monthly written verifications for approximately 25% of the caseload subject to the Work Program. The latter factor -- the individual says she is not working -- is simply verified by the client statement because there would not be written documentation that someone is not working. By adding two different items together to arrive at a percentage, the extent of any problem is stated as higher than it actually is. (This methodology was also followed in the category dealing with immunization and school attendance where two discrete data elements are added together with the result that the reported potential error is higher than it actually could be.)*

Auditor's Reply:

As stated within our report, the purpose of our test was to determine whether the associated documentation for verification was included within the TAFDC test case files selected regarding employment income/reason not employed. Prior to our testing, we provided DTA with a complete copy of our data test elements along with the their required forms of supporting source documentation for case records as outlined by DTA documentation standards. Prior to our audit testing, we had a meeting with DTA's senior management to discuss our audit approach, during which we reviewed any concerns that DTA might have before we began our field-testing at the five selected TAOs. The purpose of our review was to ensure that all active TAFDC clients had the appropriate source documentation for the selected data element verifications within their case record. We tested the data elements independently of one another and our results indicated an increased level of risk for employment income/reason not employed verifications. Where

changes to our tests were warranted based on information and criteria that was provided by DTA, subsequent to the completion of our fieldwork, we modified our audit conclusions and the statistics noted in the report. Regarding immunization and school attendance, DTA's A User's Guide, Verification of Immunization Status states *"The AU Manager must first determine the school enrollment status of each child. Those who are enrolled in school meet the immunization requirement since immunizations are required for school enrollment. No further verification is required."* Also, since immunizations are required for participation in Head Start or licensed day care programs, we needed to ensure that source documentation verifications satisfied the requirement for a child participating in Head Start or a licensed day care program.

Auditee's Response:

> *A second problem with the conclusions regarding work-related documentation is that it does not take into account the dynamic nature of the Work Program. In any given month there will be those who have not provided verifications. It is precisely for this reason that the Department has an automated process that will result in sanctions -- first a decrease in benefits, and then a termination of benefits if compliance is not achieved. What this means, of course, is that any calculation of possibly erroneous overpayments that is annualized does not actually represent the nature of the exposure to the Department.*

Auditor's Reply:

The "dynamic nature of the Work Program" was taken into consideration by incorporating two elements into our review. First, audit teams used a June 25, 2004 TAFDC database to perform their case file documentation review and did not start conducting case record reviews until a mid-July to mid-August 2004 time frame. Second, any documentation requirements within 30 days of the June 25, 2004 TAFDC database was not including in the testing. As stated within our report, we understand and fully appreciate that there is a level of risk of overpayment, as well as underpayment. We acknowledge that there are circumstances where clients may not be forthcoming with updated information or their information may be temporarily missing from case files. However, we also believe that assurance mechanisms to assess the integrity of primary data elements for eligibility can serve as valuable indicators as to whether program functions are within established tolerances. The results of our review indicated an increased level of risk regarding case record source documentation verifications for employment income/reason not employed.

Auditee's Response:

> *In addition, we did not have the opportunity to collaborate on the specific findings of your staff on a case by case basis. Such a review would have provided the ability to*

clarify and correct any findings that may have been made in error. Our own review of many of the case files identified as being in error found that documentation either existed or was not required given the circumstances of the case. This discrepancy leads us to question a significant portion of the errors identified in this area. Our review indicates that the error rate identified in the report would drop significantly based on the verifications we located for the cases.

Auditor's Reply:

As stated earlier, we provided DTA with the list of our selected case files in advance so that the case files could be readily available at the area site offices. After performing our audit work we brought forth to DTA our audit results regarding our examination of the selected TAFDC case files. We did not reexamine the case files after DTA's review because our assumption was that deficiencies noted would have been either corrected or notated with an explanation within the records.

Following their review of case files we identified as being in error, DTA asserted that documentation was in fact in the case file. It is important to note that although the supporting documentation was incomplete or absent from the case files, that in itself does not solely determine whether an individual is in compliance with specific data element verification. It should be noted that on a number of occasions, DTA's review stated that we had labeled a particular case file's data element as missing or incomplete, when we had not. For example, DTA's case file review identified one particular TAFDC case file recipient as having source documentation verifications for all data elements identified in our audit test. However, our re-review determined that for this particular TAFDC recipient, the local TAO had submitted a "dummy" case file to the audit team that, in fact, lacked any supporting documentation.

Auditee's Response:

As noted in the report, the lack of appropriate information in the case record does not automatically mean that the verifications did not exist – it may not have been filed correctly, or may have been awaiting filing. While such process issues are problematic, they would not translate to the overpayment levels cited.

Auditor's Reply:

We acknowledge this point and have stated so within our report. We understand and fully appreciate that there is a level of risk of incorrectly filed verifications or case files that may not include updated information. However, we hope that with the enhanced monitoring of TAFDC case files, the degree of possible overpayments noted within the report would not be realized by DTA.

Auditee's Response:

Lastly, even if all of the cases identified were in error and should have been subject to financial penalties, the extrapolation of these errors to annual figures would not be an

accurate representation of the likely financial exposure. It is our experience that the sanctioning process (described above for Work Program issues) is an effective method to ensure compliance. The maximum duration of any such sanction is typically only one to two months before the client complies with program rules. The area to which the report attributes the largest amount of annualized overpayments -- lack of a signed application -- would never achieve the level stated in the report because the case would be terminated immediately if compliance was not prompt. In assessing the potential exposure of the shortcomings identified by the report, it is important to bear in mind that the report concluded there were no weaknesses in determining the initial eligibility of the cases reviewed.

Auditor's Reply:

While DTA implies that there are system-generated controls that would force sanctions to occur, DTA is assuming that a review of the source documentation would be completed by a case manager. Unfortunately, that is where the monitoring process may break down, since many case workers are overburdened and may not review individual case file source documentation on an on-going basis. Regarding the lack of a signed application, the Code of Massachusetts Regulations, 702.125: Application Activities: (A) Completion of Forms, states, *"The form for the determination of initial eligibility is the application. The worker is responsible for the completion of the form, which is then signed by both the worker and the applicant. The worker is responsible for assuring that the information recorded on the form accurately represents what the applicant states about his or her circumstances."* As we state within our report, a TAFDC application that is incomplete or missing does not provide adequate support to attest to a particular TAFDC case. For the selected TAFDC cases in our audit review, questions could arise as to whether the decisions made regarding benefits and services were for eligible applicants only.

Auditee's Response:

Given those caveats, we acknowledge that there are weaknesses in some areas concerned with the continued monitoring and (re)evaluation of TAFDC cases. In response to the specific Audit Report findings detailing these areas, we are taking steps to minimize the risk of having insufficient documentation of required verifications, issuing inaccurate benefit payments, and utilizing unvalidated Social Security Numbers for those recipients who continue to receive benefits following the initial establishment of eligibility. These new operational processes and additional internal controls will help ensure the accuracy of benefits issued and improve the management of verification documents.

We will institute a regular TAFDC quality assurance review. This review will be conducted by teams of program specialists sampling a statistically valid selection of cases in each Transitional Assistance Office (TAO) and performing payment and processing quality reviews. Any errors identified will be reviewed with the management team in each TAO for possible reconciliation. To ensure an objective assessment, the staff who will conduct the reviews do not report to the Field Operations division whose performance they review.

Following the review, the performance results will be published and analyzed to determine the areas of most significant risk. The Department will then develop changes to its manual and automated processes, as appropriate. In addition, corrective action plans will be required by each TAO management team whose office results are deemed to be unacceptable. The TAOs' performance will be tracked and monitored by the Field operations division of DTA's Central Office.

Auditor's Reply:

We hope our recommendations will assist DTA in fortifying your internal controls to ensure that only recipients that comply with your standards related to verifications and obtaining valid social security numbers will continue to receive TAFDC benefits. We commend DTA in establishing new operational processes and additional internal controls that will help ensure the accuracy of benefits issued and improve the management of verification documents. Enhancing your independent monitoring procedures is an essential element in strengthening your overall internal control environment. We believe regular TAFDC quality assurance reviews will help assist DTA in mitigating risks associated with errors in payment and processing for TAFDC recipients. The monitoring or assurance procedures, combined with risk analysis, will help identify the residual risk of operational or control objectives not being met.

Auditee's Response:

The results will be evaluated within the context of our risk assessment analysis, while serving as an internal audit process. We believe that this local office case review process is consistent with the recommended, standardized risk management approach for improving controls over data integrity.

With regard to the recommendation that we establish a work group to assess the risk of new policy initiatives, it should be noted that we already have in place such a process. Before any new policy is promulgated, every major division in the Department must approve it. The particular new policy cited in the report was not only analyzed extensively -- with potential risk of erroneous payments a major focus -- but also resulted from a federal government review that found deficiencies in the prior policy.

The Department also engages in an ongoing quality assurance process, conducted through monthly Program Accuracy meetings held at the Department's Central Office, and chaired by the Assistant Commissioner for Field Operations. The agenda of these meetings is to review Quality Control error findings within the Food Stamps program and to develop methods to preclude the recurrence of the specific errors. Participants include the affected TAO Directors (whose cases were found to contain payment error) and Central Office support staff from Program Management, Systems, Legal, and Program Assessment divisions. While the primary reason for the review is to ensure the integrity of our Food Stamp benefit payments, the overwhelming majority of TAFDC recipients receive Food Stamp benefits, so the error reduction strategies that evolve apply to the cash program as well.

Auditor's Reply:

We believe that having DTA senior management work with their in-house internal audit group to develop a risk management approach will improve controls over data integrity for data contained within the Beacon application. DTA's approach of employing a local office case review process is a good start to standardize the risk management approach for improving data and system integrity controls. While we were aware that a work group to assess the risk of new policy initiatives was in place at the time of our audit, we believe the work groups should also include end users in order to help minimize any level of confusion that may be experienced by caseworkers in the dynamic DTA environment.

DTA's monthly Program Accuracy meetings held at the Department's Central Office, and chaired by the Assistant Commissioner for Field Operations, is to ensure the integrity of the Food Stamp benefit payments. For this reason, our audit team did not review this process for inclusion within our audit report. We recommend that DTA develop a similar assurance mechanism or approach that is currently employed for the Food Stamps program to help ensure the integrity of DTA TAFDC benefit payments.

Auditee's Response:

> *With regard to our utilization of valid Social Security Numbers, the agency will reissue instructions to field staff regarding the proper assignment of numerical identifiers used as alternatives to SSNs via standard Field Operations memos and procedural updates to the BEACON Users Guide. These instructions will establish uniform procedures and reasonable timelines for the acquisition of valid SSNs. In addition to these policy and procedural reinforcements, systems changes have already been implemented to preclude the issuance of benefits to noncitizens coded by our case managers as "undetermined" in our BEACON system. Noncitizens not applying for benefits are not required to furnish SSNs. The Department is also reviewing its automated procedures for the automatic verification of SSNs by the Social Security Administration, and will make changes as appropriate.*

Auditor's Reply:

We believe the establishment of uniform procedures and reasonable timelines for the receipt of valid SSNs will help ensure that the eligibility status regarding the usage of 900 Social Security numbers for TAFDC recipients is determined properly, consistently, and timely. Whenever a change occurs in DTA policy, cross edit checks within BEACON system against eligibility should always be completed. This will help ensure that only eligible enrollees are receiving TAFDC, and all ineligible enrollees are being removed from the program in a timely manner.

2. Business Continuity Planning

We determined that DTA did not have a documented and tested disaster recovery and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems be rendered inoperable or inaccessible. The only document relating to business continuity planning that was available was a Year 2000 rollover plan that had not been updated since December 1999. Although DTA had procedures for testing the recovery of their database to resume operations in the event that the BEACON system goes off line, there was no policy regarding recovery testing.

We determined DTA was performing a nightly backup to tape of its mission-critical and essential systems, including the UNIX AIX, BEACON system and Oracle RDBMS, and that backup copies were being stored in a secure off-site location. However, we found that added physical security should be applied to the on-site storage of backup copies located in the Network Operating Center (NOC). DTA incurred the risk that in the event of a disaster, on-site backup tapes that were kept unsecured on a shelf within the NOC could be destroyed, along with data and programs residing on the file servers.

At the time of the audit, senior management had stipulated that the current production environment at the NOC was in the process of migrating to the Information Technology Department's (ITD) Massachusetts Information Technology Center (MITC) in Chelsea, Massachusetts. Subsequent to the migration of production data to MITC, targeted for original completion by September 2003, the NOC would then serve as an alternate processing site for DTA. However, subsequent delays extended the self-titled "Dual Data Center Project" to January 2004, and then to February and into March, leaving the migration to MITC incomplete. Towards the end of our audit, the audit team was informed by the Director of System Security that the production environment migration to MITC had been achieved, however, documentation to support that statement was not provided. At that time, there was no evidence that recovery tests had been performed from the NOC, and its viability as an alternate site had not been validated. The absence of a tested business continuity plan, including recovery tests at an alternate processing site, does not provide DTA with sufficient assurance that mission-critical and essential data processing operations can be regained within an acceptable time period.

Because IT operations support DTA and its area offices, the business continuity plan should take into account recovery strategies to address various scenarios, including the loss of IT components, for each of the DTA Transitional Assistance Offices (TAOs). Without a formal, comprehensive recovery and contingency plan that includes required user area plans and network communication components, which has been sufficiently tested, DTA could be inhibited from processing information for the BEACON system or other applications residing on DTA's LAN, or from accessing information or processing transactions related to the Massachusetts Management Accounting and Reporting System (MMARS) or

the Human Resources Compensation Management System (HR/CMS) residing on the ITD mainframe. As a result, DTA would be hindered from obtaining information needed to continue critical business operations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted control practices and industry standards for IT operations support the need for DTA to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, DTA should assess the extent to which they are dependent upon the continued availability of information systems for all required processing or operational needs, and develop recovery plans based on the critical requirements of their information systems to support business functions.

The assessment of impact should identify the extent to which departmental business objectives and functions are affected from loss of processing capabilities over various time frames. The assessment of criticality and impact of loss of processing should assist DTA in triaging its business continuity planning and recovery efforts.

The DTA should perform a risk analysis of their IT systems to more clearly identify the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could damage or preclude the use of the systems and the likelihood and potential frequency of each threat. The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative critical character and importance of systems, and that adequate resources are available. The recovery strategies should address potential scenarios of loss of IT operations and should be based upon the results of risk analysis and an assessment of processing requirements. Without a formal, tested recovery plan, critical and essential information related to the Department’s clients and programs might be unavailable should the automated systems be rendered inoperable.

Sound management practices, as well as industry and government standards, advocate the need for comprehensive and effective backup and disaster recovery and business continuity planning to ensure that mission-critical and essential operations can be regained. Disaster recovery and business continuity planning should be viewed as a process to be incorporated within the functions of the organization, rather than as a project that would be considered as completed upon the drafting of a written recovery plan. Since the criticality of systems, importance of business objectives, or the risks and threats associated with

IT operations may change, a process should be in place to identify the change in criticality, business requirements, or risks, and assess the need to amend and test recovery and contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans. Business continuity and contingency planning has taken on added importance given that potential processing disruptions could be caused by man-made events.

Recommendation:

We recommend that DTA strengthen controls over on-site storage for backup copies of electronic media. The on-site location should be accessible by only authorized personnel and should incorporate appropriate physical and environmental controls to protect the backup copies of magnetic media.

The DTA should establish a business continuity planning framework that incorporates criticality and impact assessments, business continuity plan development, risk management, recovery plan testing and maintenance, training, and communication. Disaster recovery procedures should be developed to ensure that the relative importance of the Department's systems is evaluated on an annual basis, or upon major changes to user or business requirements, IT configuration, or identified risks. The DTA should also conduct a formal risk analysis of its IT-related components, including outsourced services provided by ITD, on an annual basis, or upon major changes to the relevant IT infrastructure or to business operations or priorities. Based on the results of the risk analysis and criticality assessment, DTA should confirm its understanding of business continuity requirements and, if necessary, amend recovery plans to address mission-critical and essential IT-supported business functions.

The DTA should ensure that the business continuity plan provides recovery strategies with respect to all potential disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover mission-critical and essential operations within the needed time frames. In addition, DTA should ensure that appropriate user area plans are in place and are sufficiently understood by administrative and operational management, as well as staff, to enable business areas to continue their operations should automated processing be lost for an extended period of time. The user area plans should take into account unavailable processing due to a loss of mainframe, LAN, or microcomputer-based system operations.

We recommend that DTA determine whether the Boston alternate site is viable. If the site does not meet the DTA's requirements, we recommend that another alternate processing site be identified and tested. We recommend that the business continuity plan identify the alternate site(s) that have been approved for business operations and data processing.

We further recommend that the business continuity plan be tested and formally reviewed and approved. The plan should be periodically reviewed and updated when necessary to ensure that it

remains appropriate to recovery needs. The DTA should ensure that management and staff are adequately trained in the execution of the plan. The completed plan should be distributed to appropriate management and staff members, and a copy should be stored in a secure off-site location. Since recovery actions may need to be made in concert with ITD or other third parties, we recommend that recovery tests be coordinated with ITD and any other required third parties and that a copy of the plan be available to appropriate ITD and third-party personnel. Moreover, the plan should specify off-site storage of backup media and required physical security and environmental protection of on-site storage of backup media.

Auditee's Response:

The audit report recommends improvements to the Department's Disaster Recovery Plan and Business Continuity Plan.

The Department has already complied with the recommendations related to disaster recovery. Prior to the period covered by the Audit, DTA had in place a very elegant and expensive Disaster Recover Plan for the recovery of its mission critical systems and environments. DTA has reengineered its disaster recovery plan and was in the process of implementing the new plan at the time this audit was being conducted.

BEACON Production has now been migrated to the Massachusetts Information Technology Center and the fail over site is the Computer Center at 600 Washington Street, Boston. The sites are configured as high availability sites allowing one to fail over to the other with a Time to Recovery (TTR) of less than 4 hours and Point of Recovery (POR) of less than 45 minutes. The system configurations and technical platforms have been validated and tested. A complete Disaster Recover Test was conducted and documented on May 2, 2004.

The Assistant Commissioner for Systems will ensure that tests of disaster recovery preparedness are conducted and documented semi-annually. Additionally the Department has taken steps to strengthen controls over on-site storage for backup copies of electronic media. Tapes will now be stored inside a locked room within the data center complex.

As a contingency in the unlikely event that the Department's Disaster Recovery Plan is inadequate, we have developed a Business Continuity Plan. The Business Continuity Plan identifies the multiple scenarios for continuing to issue benefits in the event that one or more of the Department's mission critical systems are down. The Business Continuity Plan will be reviewed and updated on an annual basis, and key staff will be provided updated copies and related information.

Auditor's Reply:

We are pleased that the DTA has developed a viable business continuity and disaster recovery plan. However, as noted in your response, after the plan's completion it should be reviewed and updated annually, or whenever there are significant changes to processing requirements, risks, or changes to the Department's IT infrastructure. Designation of an alternate

processing site and procedures for the generation and storage of backup copies of magnetic media are an integral part of any recovery strategy and should be maintained and appropriately monitored.

3. Monitoring and Evaluation of IT-related Vendor Service Contracts

Despite incurring approximately $3.89 million in IT-related vendor service contract costs during fiscal years 2003-2004, DTA had not standardized written internal control policies or procedures for use throughout the agency to monitor contract performance or quality of services rendered to clients. Although we found the IT Department had used the competitive bid process and properly awarded the service provider contracts we reviewed, we found that the service provider contract monitoring that had taken place was inconsistent. While nothing came to our attention to indicate that DTA did not receive specific contract services and deliverables, monitoring and evaluation needed to be strengthened to provide adequate assurance mechanisms to document and confirm that IT-related contract deliverables are received.

Although DTA required managers to informally monitor IT-related contracts, the Department needed to expand their policies and procedures to offer more detailed guidance on how to monitor these contracts. Our review for monitoring and evaluation of vendor service contracts disclosed that the DTA central office entered into seven vendor service contracts during fiscal year 2004. To determine whether DTA was in compliance with ITD's fiscal year 2004 directive outlining the discount rate reduction plan for all contractors with bill rates over $25.00 per hour, we reviewed each applicable contract and analyzed whether the discount had been applied. We determined that of the seven contracts, three contracts were either maintenance or flat fee contracts, and were not applicable to the hourly wage decrease. Although two of the remaining contracts did include documentation outlining the ITD rate reduction, DTA did not institute rate reductions for the other two contracts, accounting for over $100,000 in possible unnecessary payments to vendor service contract providers. Although senior management stated that there was a formal methodology as to why these two particular contracts were not included in the rate reduction, and that previous fiscal year (2003) vendor service contracts were of a much greater value than present, we were not provided with, nor could we locate within the vendor files, any documentation outlining the process by which DTA came to their determinations.

Throughout the life of a contract, DTA must diligently and regularly monitor the quality of service and assess the deliverables being provided by contractors, and determine whether the contract represents an effective and efficient use of public funds. When DTA identifies contractors that are not meeting required expectations, they should take steps to have the contractor remedy the situation, or impose appropriate sanctions, including contract termination. When contractors repeatedly demonstrate an inability to meet these expectations, they should be denied the privilege of contracting with the

Commonwealth. Monitoring procedures should be designed to ensure compliance with all significant contract provisions, program requirements, and financial-related requirements. Contract oversight procedures should:

- Clarify roles and responsibilities for the various contract monitoring functions.
- Define a risk assessment methodology for determining the cost-effective level of monitoring for each contract.
- Ensure that monitoring and evaluation results are reported to key individuals within the Department.

Not having adequate contracting policies and procedures increases the risk that DTA:

- may not obtain the best contractor for the job.
- may pay the contractor more than is reasonable or necessary.
- may not adequately monitor the quality of the contractor's goods or services.
- may not receive needed goods or services in a timely manner.
- may be unable to hold the contractor accountable for inadequate goods or services, or
- may expose the agency to inappropriate use of funds.

The Operational Services Division's " Procurement Policies and Procedures Handbook," Chapter 5 states: *" The Commonwealth has a responsibility to conduct monitoring and evaluation of the commodities and services it purchases. These activities can assist in identifying and reducing fiscal and programmatic risk as early as possible, thus protecting both public funds and clients being served."* Chapter 5 also provides several monitoring procedures, including the requirement to: *"document date, time and name of contractor representative who contacts the department regarding contract performance, questions, etc., and responses given; review and require progress reports to verify if contractor is meeting targeted performance deadlines, or ask for documentation to support that performance is on schedule; conduct announced or unannounced site visits and record reviews; solicit customer feedback on contractor performance, outcomes, and value."*

Recommendation:

The Department of Transitional Assistance should establish written and standardized internal control policies and procedures for vendor service contract monitoring and evaluation for use throughout the agency. Management should develop written policies and procedures that will ensure that all contract determinations and decisions are memorialized and supported with proper documentation within vendor files.

Auditee's Response:

> *The report recommends that the Department establish written and standardized internal control policies and procedures for vendor service contract monitoring and evaluation for use throughout the agency. It further states that management should develop written*

policies and procedures that will ensure that all contract determinations and decisions are memorialized and supported with proper documentation within vendor files.

The Department acknowledges that contract management and monitoring responsibilities have historically varied across the agency. As stated in the report, DTA is in the process of establishing standardized monitoring and evaluation policies and procedures for vendor service contracts. In November, 2004, the Department initiated a "Contracting Review" process, an internal review of the DTA procurement, contracting, and contract management processes including contract monitoring.

One of the outcomes of the "Contracting Review" process will be the issuance of a procedural handbook intended to ensure a consistent, efficient, coordinated and automated procurement, contracting, and contracts management process throughout the agency. The handbook will include the following sections: process summary; guidelines/procedures; standardized forms to be used in the procurement and contracting process; and the identification and clarification of roles and responsibilities of all staff involved in the process.

An important part of the handbook will be information on the monitoring role of a contract manager and the activities that should be completed to assess performance. Program and administrative units will utilize the handbook to document internal controls that insure that the handbook guidelines are followed.

To further strengthen DTA efforts in procurement and contracting, a recent reorganization of the DTA Office of Administration and Finance (A&F) in March, 2005, included the creation of a new Administrative Operations Unit within A&F. The new unit is responsible for providing direction, training and oversight to department staff involved in contracting.

The Department believes that the handbook, coupled with a recent reorganization of the DTA Office of Administration and Finance, will clarify roles and responsibilities in the contracting process and greatly improve the overall consistency of contract monitoring activity.

Auditor's Reply:

We believe the efforts initiated by DTA to standardize internal control procedures for contract management will help ensure the integrity of the entire contract management process. We concur with the Department's decision to modify their policies and procedures regarding contract administration. We are also encouraged that DTA is establishing a "Contracting Review" process that will establish a procedural handbook for the entire agency. We believe that this procedural handbook will assist DTA in contract management, including obtaining the best contractor for the job, adequately monitoring the quality of the contractor's goods or services, and receiving needed goods or services in a timely manner. We also believe establishing an Administrative Operations Unit will help assist DTA in strengthening controls over the contract monitoring and evaluation process.

4. Information Technology Strategic and Tactical Planning

Our audit indicated that DTA's IT Department had not developed comprehensive strategic or tactical plans to address IT functions within the department or across the DTA Transitional Assistance Offices (TAOs). We observed that the IT Department had a rudimentary IT-related short-term plan, but that it lacked sufficient detail regarding assignments, priorities, milestones, or performance metrics. We determined from an enterprise-based perspective that there was no overall IT strategic plan covering all IT functions and projects. We found that management control practices needed to be strengthened to ensure that IT strategic planning for the IT Department is sufficiently defined and aligned with overall IT strategies to support DTA's operations and business objectives.

Although the IT Department had developed a mission statement outlining its overall purpose and key duties, the statement needed to be enhanced to adequately identify the department's role in supporting enterprise-based management of IT activities. The latter would include establishing appropriate IT-related policies and guidelines, setting strategic direction for IT functions and configuration management, and providing oversight of IT activities.

It was apparent based on our interviews and observations that there were no clear directives for the IT Department to develop a documented IT strategic plan, or detailed tactical plans. The absence of an IT steering committee over the IT Department may have contributed to the lack of IT strategic and tactical plans not being identified and highlighted to senior management.

Strategic planning is an essential process to assist an organization in setting direction and appropriate courses of action to meet its mission and business objectives. The more that IT strategic planning can be integrated in the DTA's overall strategic planning process, the more likely that the management and use of IT resources will become a key enabler of operational processes to support the agency's business objectives. A comprehensive strategic planning process should incorporate a formal, organizational-tailored approach to developing and managing automated application systems, whether the systems are acquired or internally developed. The planning process should also address IT configuration management for all IT resources, including the computer systems and networks supporting the application systems. Effective IT strategic planning should help direct the IT Department's actions and incorporate milestone and performance measurements to be used as effective management tools. Performance measures provide management with qualitative and metric-based feedback against which the progress of strategic initiatives and IT operations can be evaluated. The IT Department would benefit from having performance metrics gradually applied to its functions and service areas.

An IT strategic plan should include the following components:

- Statement of organizational mission and primary business objectives identifying the linkage of the IT strategic plan to the overall enterprise strategic plan(s).
- Summary of the organizational strategic plan goals and strategies enabled by IT and supported by IT functions.

- Statement of critical success factors for IT and the IT Department.
- Statement of IT requirements to adequately support the enterprise's business objectives and overall long and short-term plans for the enterprise.
- Statement on how each IT goal and strategy will support organizational goals and strategies.
- Detailed information on DTA's current IT infrastructure (inventory of current IT resources and IT capabilities, including hardware, software, communications, personnel, capacity and utilization, strengths and weaknesses, and associated risks).
- Definition of information architecture model that addresses DTA's information requirements. The information architecture model should be cross-referenced to the established data classification scheme with respect to data sensitivity and privacy requirements.
- Statement on technological direction taking into account technology standards, current technology base, operational and fiscal strengths and limitations, and any acquisition or system development plans.
- Statement on capabilities of IT and non-IT personnel responsible for performing IT-related tasks and activities and plans on staff development regarding skills and knowledge.
- Forecast of internal and external developments that could impact the IT strategic plan.
- Statements of technological solutions taking into account the organization and business processes, re-engineering opportunities, control objectives and preferred control practices, personnel requirements, and performance indicators.
- Acquisition and development schedules for the IT environment.
- Statement on operational, administrative, and quality service issues related to the organization's targeted IT environment, taking into account recommended policies and procedures.

The lack of a comprehensive strategic planning process that incorporates all IT functions places at risk DTA's ability to identify and develop business cases to support IT operations and initiatives, as well as the IT Department's ability to successfully address management's business objectives and user expectations through future BEACON system projects and IT-related acquisitions. Without comprehensive strategic planning, the analysis and development processes may vary substantially among projects, potentially resulting in information systems that may be inefficient, incompatible, or have cost overruns on development or system maintenance. With respect to costs, the planning process should require identification of total cost ownership so that more comprehensive business case analysis can be performed for each development or acquisition project. The strategic planning process should require that IT strategic and tactical plans be updated to reflect accomplishments, changes, and new initiatives. Having detailed, enterprise-wide IT strategic and tactical plans for DTA is critical to the success of future modifications to the BEACON application.

Benchmarking at the time of our audit against generally accepted management control practices, such as those outlined in the CobiT control model, we identified that key elements of an IT strategic planning process were not sufficiently in place. For example, the IT Department's tactical plans needed

to be driven more from enterprise-based strategic plans, taking into account all IT functions and initiatives. At the beginning of our audit, the IT Department did not have readily available IT strategic planning documents that clearly indicated technological direction and specific planning activities. From a documentation standpoint, formal notes or minutes of IT Department meetings regarding strategic issues were generally not maintained. There was also evidence that the IT Department's efforts were driven by short-term demands placed on the department and in meeting technical operational requirements.

The strategic planning documents provided during the course of our audit did not clearly specify IT configuration requirements for the systems operating in the DTA environment. Also, at the beginning of our audit, the IT Department did not have readily available detailed results of assessments of existing systems. Essentially, very little written documentation regarding IT assessments was in place. The IT Department lacked an inclusive IT strategic plan that covered all IT initiatives, projects and IT functions with an integrated and coordinated approach considering risk assessment results. In summary, our examination indicated that IT configuration management (strong inventory control, status accounting of all IT resources, assessments of IT resource capabilities, and database management) had not been a traditional priority of the IT Department.

Recommendation:

We recommend that DTA and its IT Department:

- Develop an enterprise-based IT strategic plan that incorporates all IT initiatives and functions. The plan should also include strategic initiatives of the IT Department.
- Incorporate project management techniques, risk assessment, performance measurement, and assurance mechanisms into the strategic planning process to provide feedback and to help assure that management control practices are operating as intended.
- Conduct performance, risk, and control assessments of IT systems and the operational and IT processing environments on a regular basis to provide a basis for strategic planning.
- Develop strategic planning control mechanisms over all IT processes to determine whether technological direction will satisfy the business requirement of taking advantage of available and emerging technology offered through acquisition of new technology or modifications of current application systems.
- Create and maintain a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms.
- Formalize the process of developing and maintaining IT strategic and tactical plans adopting a structured format and content requirements for the plans.
- Develop a strategic plan to address all IT initiatives, projects, and IT functions, including access security, data center operations, network administration and security, inventory control, and IT configuration management.
- Develop documented IT tactical plans, based on IT strategic plans that identify IT Department tasks and activities and enterprise-wide initiatives.

Auditee's Response:

The Audit report recommends enhancing the strategic and tactical planning associated with information technology. DTA strongly believes that strategic planning is an essential process that is required to assist an organization in setting direction and the appropriate course of action to meet its mission and business objectives.

The Department currently has a number of planning mechanisms. At daily Senior Staff meetings, goals and objectives are constantly refined. IT Strategic Initiatives in support of the Department's Mission, Goals and Objectives are also identified and approved. The Assistant Commissioner for Systems estimates funding required for these initiatives, reviews these estimates with Senior Staff and, upon approval, incorporates estimates into the IT Budget Detailed Spreadsheet for current and outlying fiscal years. The IT Budget Detail estimates are incorporated into the Agency's current year spending plan and out-year budget requests.

It is the responsibility of the Assistant Commissioner for Systems to design, engineer, procure and implement the appropriate technology in support of the Agency. It is also the responsibility of the Assistant Commissioner for Systems to review and manage these implementations and report to the Senior Staff on the condition and performance of the technology initiatives and infrastructure. The Assistant Commissioner for Systems, as a member of the EOHHS Secretariat and in partnership with CSC Corporation, embarked on developing an IT Strategic Plan for the Secretariat in early 2003. This consisted of a current inventory and assessment of technology across the Secretariat, a Vision Document and a Transition Plan. The chosen strategic direction of implementing a Service Oriented Architecture is documented in the EOHHS Information Technology Architecture (ITA) document.

The EOHHS infrastructure consolidation and rationalization team also developed a strategic plan and direction for the technical infrastructure across the Secretariat. Initially the infrastructure consolidation and rationalization effort was led by and managed by the DTA Assistant Commissioner for Systems and DTA IT staff. Infrastructure staff were later consolidated into the EOHHS organization in August, 2004. The Department of Transitional Assistance and the Assistant Commissioner for Systems are actively involved in pursuing and implementing the strategic direction in the areas of Integrated VoIP, migration to MassMail, server standardization and consolidation to open source standards, standard desk tops, end user computing and a single standard environment for trouble ticket tracking, problem resolution, defect management, configuration management and asset management.

DTA realizes the importance of strategic planning, and acknowledges the need to formalize some of the current planning efforts. The Assistant Commissioner for Systems, together with the Senior Staff of the Agency will develop a high level enterprise-based IT strategic plan that incorporates all IT initiatives and functions. The Assistant Commissioner for Systems will formalize the process of developing and maintaining IT strategic and tactical plans incorporating project management techniques and the conducting of performance, risk, and control assessments of IT systems to inform the process. The Assistant Commissioner for Systems will create and maintain a technical infrastructure plan consistent with the infrastructure strategic direction of HHS and monitor compliance to the plan.

Auditor's Reply:

Although DTA may have had informal IT planning activities in place, the degree of documentation to support an overall IT strategic vision was inadequate for the size and scope of DTA's IT environment. Effective IT strategic planning should help direct DTA's and the IT Department's actions and incorporate milestone and performance measurements to be used as effective management tools. Performance measures provide management with qualitative and metric-based feedback against which the progress of strategic initiatives and IT operations can be evaluated. The IT Department would benefit from having performance metrics gradually applied to its functions and service areas.

An IT strategic plan should include the following components:

- Statement of organizational mission and primary business objectives identifying the linkage of the IT strategic plan to the overall enterprise strategic plan(s).
- Summary of the organizational strategic plan goals and strategies enabled by IT and supported by IT functions.
- Statement of critical success factors for IT and the IT Department. Statement of IT requirements to adequately support the enterprise's business objectives. It is important that the IT strategic plan reflects and supports long and short-term plans.
- Statement on how each IT goal and strategy will support organizational goals and strategies.
- Detailed information on the organization's current IT infrastructure (inventory of current IT resources and IT capabilities, including hardware, software, communications, personnel, capacity and utilization, strengths and weaknesses, and associated risks).
- Definition of information architecture model that addresses the information requirements of the organization. The information architecture model should be cross-referenced to the established data classification scheme with respect to data sensitivity and privacy requirements.
- Statement on technological direction taking into account technology standards, current technology base, operational and fiscal strengths and limitations, and any acquisition or system development plans.
- Statement on capabilities of IT and non-IT personnel responsible for performing IT-related tasks and activities and plans on staff development regarding skills and knowledge.
- Forecast of internal and external developments that could impact the IT strategic plan.
- Statements of technological solutions taking into account the organization and business processes, re-engineering opportunities, control objectives and preferred control practices, personnel requirements, and performance indicators.
- Acquisition and development schedules for the IT environment.
- Statement on operational, administrative, and quality service issues related to the organization's targeted IT environment, taking into account recommended policies and procedures.

GLOSSARY

BEACON	Benefit Eligibility and Control On-line Network
CobiT	Control Objectives for Information and Related Technology
DTA	Department of Transitional Assistance
EAEDC	Emergency Aid to Elderly, Disabled and Children
FS	Food Stamps
GAGAS	Generally Accepted Government Auditing Standards
HR/CMS	Human Resources Compensation Management System
INS	Immigration and Naturalization Service
ITD	Commonwealth's Information Technology Division
MAGNet	Massachusetts Access to Government Networks, Commonwealth's Network
MITC	Massachusetts Information Technology Center in Chelsea
MMARS	Massachusetts Management Accounting and Reporting System
NOC	Network Operations Center, DTA
OSD	Operational Services Division
PACES	Program Automated Calculation and Eligibility System
SSI	Supplementary Security Income
TAFDC	Transitional Aid to Families with Dependent Children
TAO	Transitional Assistance Office