40. Organized “in but not of” the Department of the Treasury, the Office of Information Technology (OIT) provides information technology services to State agencies. To that end, it oversees the mainframes, servers, networks, and databases that compose the State’s technical infrastructure; operates the Garden State Network, a statewide integrated communications network; and runs the State’s major data centers, including the Office of Information Technology Availability and Recovery Site (OARS). In addition, it manages the State’s internet environment and offers application development and maintenance, geographical information systems, and data management services.

Attrition, a hiring freeze, and an early retirement program have shrunk the Executive Branch workforce by almost 4,000 since FY 2007, producing an annualized $312 million in cost savings (FY 2010 Budget-in-Brief, page 73). The Governor’s FY 2010 budget proposal envisions continuation of the hiring restrictions coupled with possible furloughs or layoffs.

• **Questions:** In general terms and by means of specific examples, how has the reduction in staffing affected Office of Information Technology (OIT) operations? What strategies has the office employed to deal with staff reductions? What projects, work products or functions has the office scaled back, discontinued or deferred because of declining staffing levels?

• Would OIT be able to accommodate furloughs in FY 2010 without increasing spending for overtime or temporary workers? In which programmatic areas would layoffs occur, if any? Please comment on the likely impact of the planned furlough program and contemplated employee cuts on OIT operations and services. Would the office be ceasing certain activities, programs, or services? Would the downsizing cause OIT to reassess its priorities and reassign staff accordingly among its programs? If so, please describe the internal reorganization.

• How many employees was the office authorized to hire in FY 2009 despite the hiring freeze? Please indicate for which activities these hires were crucial.

**RESPONSE**

**Effect of Staffing Reductions:** Since FY 2005, OIT has seen a 20% reduction in its filled FTE level. Hiring over the past three fiscal years has been limited to support for mission critical functions, major agency-driven initiatives and areas where cost savings can be realized (for example, in 2008 OIT was allowed to convert 10 consultants to state employees which resulted in cost savings of $800,000). The chart below provides a history of OIT’s staffing levels since FY 2005.
During the same period, OIT’s workload has increased significantly. The increase in workload is being driven by the need to modernize the State’s systems and the continual migration to automated processes such as e-government. Balancing the increase in workload against the reduction in staffing (see chart below) has been challenging but it’s also creating opportunities for OIT and the State to re-prioritize workload and phase out low-value projects.

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>Filled</th>
<th>Adjusted OIT Base (Filled less Special FTE Increases)</th>
<th>Diff from 2005</th>
<th>% Diff</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>962</td>
<td>962</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>2006</td>
<td>929</td>
<td>914</td>
<td>(48)</td>
<td>(5%)</td>
</tr>
<tr>
<td>2007</td>
<td>919</td>
<td>895</td>
<td>(67)</td>
<td>(7%)</td>
</tr>
<tr>
<td>2008</td>
<td>891</td>
<td>858</td>
<td>(104)</td>
<td>(11%)</td>
</tr>
<tr>
<td>Actual as of 5/1/09</td>
<td>806</td>
<td>776</td>
<td>(186)</td>
<td>(19%)</td>
</tr>
</tbody>
</table>

Revised 5/15/2009
Overall the areas that experienced the most significant growth are:

1) E-government – E-government applications and the processes and infrastructure that support what in essence is 24x7 government services have been steadily increasing since 2006. As of today, there are in excess of 480 e-government processes supported by the OIT infrastructure. Most of these e-government processes are public facing which ultimately mean better customer service at more convenient times for the general public. Appendix A includes a detailed list of e-government services including usage.

2) Core infrastructure – OIT’s core infrastructure which includes the Garden State Network (GSN), enterprise servers and storage, backup and recovery services, and data management and warehousing. The increase in these areas is as a result of the consolidation effort where OIT is taking the lead to develop a shared computing environment for agencies to use in order to lower the IT capital expenditures across state government.

3) Modernization projects – Legacy renovation projects are large and complex but sometimes necessary to bring government operations into the 21st century. Some of the state’s oldest computer systems that provide critical public-facing services are going through a multi-year renovation effort. All of these projects, MVC’s MATRIX and DHS’s NJKids, are heavily dependent on OIT for support and infrastructure services.

These advances have been accomplished despite reductions in staffing and by leveraging newer solutions (e.g., virtualization and cloud computing) available in the marketplace to reduce the overall operating expenses.

In light of budget and resource constraints, OIT has had to channel its resources to focus on supporting the day-to-day operations of core enterprise infrastructure and deferring certain projects to a future date. Some of the projects that are being deferred to a future date are:

- Establishment of a Quality Assurance (QA) organization within the Program Management Office
- Further development of Service Level Agreements (SLA)
- Redesign of the 3-Tier Architecture
- Design and enhancement of secure file transfer capabilities
- Establishment and consolidation of remote access capabilities
- Consolidation of enterprise printing facilities with the Capitol Post Office
- Establishment of an enterprise data archiving service
Accommodate furloughs in FY2010 without increasing spending: Regarding furloughs, the Department has assessed the potential impact of the measure and as of now anticipates no increase in overtime.

In which programmatic areas would layoffs occur: OIT’s approach to any required Reduction in force (RIF)/layoff would be to concentrate on preserving its core business functions and to minimize any disruption of service. These plans are still under development.

Authorized New Hires in FY2009: OIT has received authorization to hire 19 federally-funded positions that will be used to support DHS and DCF. The positions will be used as follows:

- 17 positions will provide on-site staff at DHS in support of its network, server, and web-development activities. A number of these activities are part of the support that DHS provides to DCF for NJSPRIT.

- 2 positions will provide direct programming support for NJSPRIT (SACWIS). These positions will be in addition to the current OIT complement of five. The primary focus of the existing and new positions is preparation to assume maintenance responsibilities when the CGI contract expires

41. The FY 2009 Appropriations Act anticipated that executive departments would achieve $25 million in procurement savings. A chart on page 75 of the FY 2010 Budget-in-Brief categorizes those savings and indicates that they will continue into FY 2010. The Governor’s FY 2010 budget includes another $25 million in savings from “smarter procurements” (Budget-in-Brief, page 54).

- Questions: Please indicate the FY 2009 amount of procurement savings achieved by the Office of Information Technology (OIT), by the categories set forth in the referenced table, and the sources of those savings by office program. What is the annual amount of these savings as continued into FY 2010? How have these reductions affected OIT? What projects, work products or functions has the office scaled back, discontinued or deferred in order to achieve these savings?

- Please list OIT’s projected contributions to the $25 million in savings from “smarter procurements” budgeted in the Governor’s FY 2010 budget proposal. How would these reductions affect the office? What projects, work products or functions would OIT scale back, discontinue or defer in order to achieve these savings?

RESPONSE
OLS Budget Questions

FY2009 Procurement Savings: As indicated in OMB’s response, OIT’s FY2009 procurement savings are $932,000.

Additionally OIT is working with DPMC to consolidate staff within the Riverview Complex in order to provide two floors for Education which will result in the elimination of a lease.

FY2010 Savings: The annual amount for FY2010 is $1.463 million. This additional reduction will be absorbed through various efficiencies and deferral of several internal initiatives.

Project/Work to Be Scaled Back, Deferred, etc: Refer to the response in question 40 for a list of delayed or deferred initiatives.

Share of FY2010 $25 Million Efficiency: At this time OIT has been given any guidance on a new procurement initiative.

42. P.L.2007, c.56 reorganized OIT consistent with the provisions of Executive Order #42 of 2006. The restructuring institutes OIT as State government’s central information technology (IT) management and oversight body. The law, however, does not consolidate all IT operations in the office, as agencies may continue to run some IT functions if OIT deems such devolution more cost-effective and efficient than rigorous consolidation. According to the IT reform model that is being implemented, OIT should become the central authority for the State’s shared information technology infrastructure. Under the office’s oversight, individual agencies or affinity groups (organized IT communities of interest spanning several State agencies) would eventually assume the responsibility for the development of their business applications.

In response to OLS discussion point #39 in the FY 2008-2009 Department of the Treasury Budget Analysis, OIT related that a cross-agency team had recommended the consolidation of certain IT services: networks, automated document services, enterprise services (e-mail, archiving, enterprise and multi-agency applications, portals), communications, security, disaster recovery, storage, information technology field support, service desk, desktops and data centers (servers and storage). The State’s fiscal situation, however, forced OIT to instead adopt a modified, three-phase consolidation strategy. In the first phase, the office was already in the process of physically collocating mission-critical IT equipment to reduce the number of data centers and energy consumption, and to improve IT disaster recoverability. In a written follow-up response to a question raised during the Department of the Treasury’s budget hearing before the Assembly Budget Committee on April 15, 2008, OIT admitted, however, that progress in migrating equipment to a central location was slow due to a lack of funding. Phase 2, which OIT was just beginning, involved the use of the procurement review process to optimize the IT infrastructure through platform consolidation or virtualization. Phase 3, which had not yet
OLS Budget Questions

commenced, calls for service integration across affinity groups to improve service delivery and internal processes. OIT was also about to finalize the Service Level Agreements (SLAs) templates that would be used within the Executive branch to specify the technical support services OIT would provide to client agencies. OIT also intended to meet with each Executive branch agency in FY 2009 to determine each agency’s IT requirements and the areas that would be conducive to consolidation.

Three barriers keep some agencies from fully cooperating with the goal of consolidating IT resources and management, according to OIT’s written follow-up response to a question raised during the Department of the Treasury’s budget hearing before the Assembly Budget Committee on April 15, 2008. First, federal funds must often be used for specific programs and cannot be used jointly by multiple programs or agencies. Second, rigid title specifications under civil service rules in agency IT offices prohibit the reassignment of duties in support of a centralized model.

* Questions: Please provide an update on the implementation of the three-phase IT consolidation strategy. Has the physical collocation of mission-critical IT equipment been completed? What are the anticipated cost savings of the collocation? If the collocation project has not yet been completed, by which date does OIT expect its completion? Has OIT secured sufficient funding for the migration of equipment to a central location? What level of funding would OIT need to complete the migration? Has OIT been able to focus on the use of the procurement review process to optimize the IT infrastructure through platform consolidation or virtualization? Have there already been positive outcomes? Has OIT started to pursue service integration across affinity groups?

RESPONSE

Phase 1: To date OIT has focused on the consolidation of DOT and Health & Senior Services (DHSS). The DOT data center consolidation represents our first test case. Significant effort has been expended to plan and coordinate this consolidation. This is well underway which includes the virtualization and upgrades of existing DOT equipment, increased capacity of data communications lines and equipment efficiencies aimed at reducing the initial footprint and cost of operation. The second phase is the actual move of equipment from DOT to OIT’s HUB. This is scheduled for fall 2009. DOT staff will be realigned to OIT corresponding to the actual move of equipment. An added bonus of the DOT consolidation is the plan to leverage the DOT disaster recovery site and incorporate its availability in conjunction with the implementation of OIT Application Recovery Site (OARS).

Also working with the Division of Property Management and Construction (DPMC), we are preparing for the relocation of the DHSS data center to one of our data centers. This consolidation is in the support of the elimination of leases on Quakerbridge Road.

Future consolidations of this nature will experience delays or be deferred due to our lack of available computer room floor space at the OIT facilities (HUB and SAC). OIT has been working closely with DPMC.
to relocate printing operations and related equipment from its HUB location. This would free up valuable computer room raised floor space thus allowing for the consolidation of agency data center equipment.

At the present time without the move of print equipment from the HUB, the majority of the available space will be consumed by the NJDOT and DHSS consolidation.

Other additional factors that will affect OIT’s ability to consolidate are the potential of layoffs and new federal mandates that may arise. With regards to layoffs, OIT is working with agencies to gain insight to their plans when available to assess impacts on OIT delivery of services. Until more information is provided, OIT will not know if:

- Additional technologies, in lieu of staff, will be needed to support business processes
- Existing applications may be eliminated or expanded
- Agencies will look to OIT to handle more of their technical support

Regarding new federal mandates, the recent changes in unemployment insurance is an excellent example as to how OIT can be impacted. To-date OIT staff has logged over 4,400 overtime hours (which LWD is funding) to address programming changes and the increased volume in printed output and checks production. LWD’s schedule is extremely aggressive and clearly expects OIT to meet its needs.

Recent State mandates are also impacting other projects in motion.

**Phase 2:** Successes in phase 2 have included:

- Working with Purchase and Property to leverage the Department of Environment Protection’s (DEP) NJEMS system for use by the Department of Community Affairs in support of various registration functions
- Continuing the statewide implementation of E-Cats
- Implementing DCA’s grant systems (SAGE) at DHSS and DOT
- Leveraging the ADF intelligent inserting and certified mail needs for NJKids to provide statewide functionality
- Creating a virtual tape library environment that will be able to support the back up of all data generated within the OIT data centers, regardless of platform or ownership of processing hardware
- Preparing to leverage the DOT disaster recovery site and incorporating its use with OARS
OLS Budget Questions

- Working with the MVC MATRIX project to leverage the existing server and storage infrastructure in conjunction with new purchase equipment
- Leveraging the Treasury email infrastructure to support a number of smaller agency email environments
- Leveraging agency and OIT purchases to obtain greater volume discounts from a number of hardware and software vendors

**Phase 3:** SLAs are discussed later in this question.

**Physical Collocation:** As stated earlier, delays in relocating printing operations in order to provide adequate floor space at OIT main data centers hinders physical collocation with the exceptions of DOT and DHSS.

- Please explain whether the current three-phase IT consolidation strategy is compatible with the original consolidation strategy devised by the cross-agency team. Has OIT abandoned the original strategy permanently or has it conceived the current strategy as a slimmed down version of the original plan, which would easily allow for the implementation of the initial plan once financial resources permit? Is the pursuit of the current strategy likely to render a shift to the original strategy too costly?

**Compatibility of Current 3-Phase IT Consolidation with Original:** OIT continues to support its three phased strategy. Despite issues related to collocated, we continue to foster data center consolidation and look for every opportunity to exploit such a strategy. For example we have begun to leverage some larger agency data centers in place of expanding on smaller agency data centers. Similarly after detailed analysis of agency e-mail usage, it was discovered that the migration of some agencies to a the statewide email solution would be extremely complex. This has delay the enterprise project. As an interim, we are leveraging the Treasury Data Center Email Exchange environment and have been migrating smaller agencies to this platform rather than allowing agencies to refresh or replace their existing email systems. In most cases these approaches are the same or cheaper than the original agency initiative which balances replacement of obsolete equipment and software refresh at a point that it maximizes the savings. But most importantly it pre-positions OIT with incremental consolidation steps closer to our goal of statewide consolidation. We believe it is the best compromise under the current constraints.

- Has OIT met with each Executive branch agency to determine each agency’s IT requirements and the areas conducive to consolidation? If not, by which date does OIT expect to have completed the meetings? Into how many Service Level Agreements has OIT entered with client agencies? Please submit a copy of a Service Level Agreement with the Department of
the Treasury. Have IT responsibilities been shifted to or from OIT following the start of the reorganization? If so, which responsibilities have been transferred and according to which rationale?

RESPONSE

OIT and Executive Branch Meetings to Determine IT Requirements and Areas Conducive to Consolidation: OIT’s Chief Technology Officer (CTO) has met with all agency heads, as well as regularly meeting with agency IT Directors to discuss consolidation efforts. Agency heads have been very supportive of consolidation as a whole, due to agency priorities driven by mandates agencies have had to balance progress in this area against meeting their core business goals and have asked OIT to provided flexibility. We have noted a marked growth in agencies reaching out to OIT for assistance and where possible we assist.

Service Level Agreements (SLAs): OIT has invested great effort to draft a model SLA incorporating all the components needed for a successful support model for the agencies. Extensive research was performed using advisory services and comparing to other State’s regarding the use of SLA’s. In all cases it was apparent that SLA’s provided a higher expectation from agencies for the delivery of services from a central organization than was previously provided within the agency under their own delivery model. The success of any SLA depends on the provider being able to fund equipment and staff resources as needed. OIT is balancing these against its available resources. While in this balancing mode OIT has been careful to try to work with agencies to formulate a mutual compromise on setting agency expectations. When we finalize the consolidation of the DOT then an SLA will be in place. This will be the model for all future consolidation efforts and related SLA’s

- Does OIT have a strategy to address the three barriers that keep agencies from fully cooperating with the IT consolidation drive: federal funding that can only be used in support of specific programs, civil service rules that prohibit the reassignment of duties, and territorial agencies with public safety missions? Does OIT feel that it is receiving broad overall support from client agencies in its quest to reorganize the delivery of State IT services? Which agencies are stalling? Who settles disputes between OIT and client agencies about who should be performing certain functions?

RESPONSE

Federal Funding: The federal funding issue is one that faces all states with centralized IT initiatives. In order to deal with this issue nationally, the National Association of State Chief Information Officers
(NASCIO) in conjunction with the Association of Government Accountants (AGA) have formed a task force to present recommendations for the revision of Federal OMB Circular A-87, as it pertains to the funding of information technology. This circular which governs funding from the federal Department of Health and Human Services, has been the major impediment for both consolidation and contributions to enterprise upgrade from major federally funded projects. It also should be noted that the federal Department of Labor uses the basic principles of A-87 as the general guideline for use of its programmatic funding.

Until the A-87 issues are resolved it will be difficult to consolidate federally funded agency staff and equipment.

One example where OIT has attempted to address this problem is the Automated Document Factory capabilities implemented on behalf of DHS’s NJKids project. Equipment for both intelligent inserting printing capabilities, as well as certified mail processing, have been funded by OIT through Line of Credit. Funding for the LOC payments will be incorporated in agency bills, based on usage. Currently federally funded agencies are the predominate user of this equipment.

Civil Service Rules: OIT recognizes that agency IT functions are supported by predominately IT titles and vary from agency to agency, however exceptions do exist. Consolidation of IT will require OIT to work closely with CSC to resolve classification issues or exceptions as we merge functions and related titles. CSC has been very supportive in working through these issues to date.

• What was the actual total amount of State information technology spending in FY 2008? What is the projected total amount of State information technology spending in fiscal years 2009 and 2010?

RESPONSE

The total amount expended in FY2008 for IT was $365 million. The FY2009 expended year-to-date total is $249 million. These figures are for non-salary IT expenditures and include the Judiciary and all telecommunications expenditures. 43. Pursuant to P.L.2007, c.56, a nine-member New Jersey Information Technology Governing Board heads the reorganized OIT and determines strategic direction, standards, and funding priorities. A Chief Technology Officer runs OIT’s day-to-day operations and coordinates IT operations across the executive branch. Four Deputy Chief Technology Officers have responsibilities for IT management, planning, and budgeting within four Affinity Groups, or communities of interest that intersect several State agencies (Administrative Services; Health, Education, and Social Services; Public Safety; and Business and Community Services). State agency IT directors are accountable to their Affinity Group’s Deputy Chief Technology Officer. A Project Review Board—composed of representatives from OIT, the Office of Management and Budget in the Treasury, and the
OLS Budget Questions

Purchase Bureau in Treasury’s Division of Purchase and Property—reviews and monitors all large scale IT projects in the executive branch. In response to OLS discussion point #40 in the FY 2008-2009 Department of the Treasury Budget Analysis, OIT noted that the new governance structure had been implemented except that agency IT directors still had to be made accountable to the Deputy Chief Technology Officers, which OIT was planning to organizationally accomplish by the end of calendar year 2008.

• Questions: Please indicate whether OIT has made agency IT directors accountable to the Deputy Chief Technology Officers. If not, by which date does OIT expect to do so and what factors have accounted for the delay? Through which means does OIT hold, or intend to hold, agency IT directors accountable? Do the agency IT directors also answer to superiors in their agencies? If rivaling authorities exist, how does OIT ensure that agency IT directors do not receive conflicting instructions? In the event of conflicting instructions, do OIT instructions trump agency instructions in the mind of the typical agency IT director? On which grounds does OIT base its assessment of the likely behavioral response of the directors to conflicting instructions?

RESPONSE

The governance model in place has the Agency IT Directors obtaining enterprise guidance from the Affinity Group Deputy Chief Technology Officers (DCTOs) but take their direction on a day to day basis from the agency chief executives. Some affinity groups operate more effectively within this world while others continue to exercise greater independence focusing on the delivery of IT mandates and services within their agency. The governance model described below outlines the authority exercised over the agencies.

Additionally, OIT manages issues of standards, interoperability, costs, enterprise solutions and IT personnel issues. Otherwise the day to day operations is left to the Agency IT Directors.

• Please comment on OIT’s experiences with the new governance model. Has it helped to rationalize the management of the State’s IT resources as intended? Has OIT become aware of any shortcomings in the governance structure that might justify additional modifications? If so, what changes would OIT support?

RESPONSE

The OIT governance model, as outlined in the Public Law, was implemented, this included an IT Governance Board, a Project Review Board (PRB), Agency IT Steering Committees, Affinity Group Deputy Chief Technology Officers (DCTO’s), Strategic Plans, Tactical Plans and procurement oversight.
IT Governance Board – provides overall enterprise direction on IT related matters as well as reviews and sets IT policy. The Board is envisioned to include public and private members. The Board is currently comprised of internal public members. Project Review Board – this board was established shortly after the public law and has responsibility for review of IT projects valued at $1 million and above or where the projects have great sensitivity. This board is represented by OMB, Purchase Bureau, OIT and the Governor’s Office. The purpose of this board is to review new project submissions and existing projects over it lifecycle and ensure proper attention is given from a statewide perspective. Resources and costs are also reviewed.

Affinity Group Deputy Chief Technology Officers (DCTO’s) – Affinity Groups of agencies were formed to provide synergy amongst related agencies to promote interoperability and sharing as well as leveraging technology where appropriate. Agency IT Directors obtain enterprise guidance from the Affinity Group Deputy Chief Technology Officers.

Agency IT Steering Committees – address prioritizing agency demands within their agency. OIT strongly suggested that all agencies institute such committees. Most agencies have done so. IT initiatives are presented to a cross section of business and technology leaders within the agencies so that they can rationalize demands with available resources. This provides greater guidance to the agency IT directors.

Strategic and Tactical Plans - OIT has mandated the continued maintenance of agency strategic plans as well as tactical plans that enable the Affinity Group DCTO’s visibility to agency initiatives. Armed with this information the Affinity Group DCTO’s attempt to develop synergy amongst the affinity group agencies and leverage technology solutions across them and across the enterprise where appropriate.

Program Management Office – focuses on the delivery of IT services by reviewing strategic and tactical plans, ensuring procurements are leveraged for the best value of the state, developing standard procurement templates (RFI, RFQ, RFP) for use by agencies, and coordinating the review of agency initiatives through an Integrated Project Planning (IPP) conceptual, logical and physical review process to facilitate the best IT solution on all agency requests. Enterprise contracting is also addressed within this unit. A future plan for Quality Assurance (QA) was envisioned as this group evolved to ensure that projects were meeting targets and moving to successful completion. This has been deferred due to the current financial restraints.

Recommended Changes: OIT still believes that this model, given enough time and resources, represents the best approach to managing IT initiatives. However with the ever growing demand for IT services we believe that an adjustment should be made that would incorporate enterprise business prioritization that would include additional members that would represent the agency business needs.

As part of the new governance structure at OIT, an interim Project Review Board—composed of representatives from OIT, the Office of Management and Budget in the Treasury, and the Purchase Bureau in Treasury’s Division of Purchase and Property—reviews, approves, and monitors IT projects.
that typically exceed $1 million in value. Replying to OLS discussion point #40 in the FY 2008-2009 Department of the Treasury Budget Analysis, OIT stated that the board was still overseeing many projects in whose conceptualization it had no part. Over time, OIT intended to place the board at the beginning of the planning cycle so that it could influence priority setting, funding, and resource allocation. OIT also noted that the board held each agency head accountable for the agency's IT projects.

The Project Review Board (PRB) is part of New Jersey's new governance model for statewide IT and was established to address two important components of information technology projects in the State’s executive branch. The first is to establish a protocol for the initiation and prioritization of statewide or significant value projects; and second, to provide oversight of ongoing projects and ensure sufficient attention and resources are applied to the project to ensure successful completion within budget and target.

The PRB actively plays this review and oversight role on the progress of larger scale projects in relation to overall state competing needs as well as to provide balance in the progress of the projects from a variety of perspectives which include OMB budgetary impacts, procurement impacts, and information technology standards, architecture and methodologies. These are focused on the organization of the project team as well as the daily management of the project to its successful completion. Risks would be identified early on and managed appropriately.

- **Questions:** Please explain the process the Project Review Board uses to monitor large-scale IT projects. What is the periodicity of reviews of approved projects? Are there specific events that trigger a review? What means does the board have to hold an agency head accountable for floundering agency projects?

**RESPONSE**

The following criteria are used as a basis to determine applicability for inclusion in the Project Review Board process:

- Cost
- Sensitivity (time, mandates, etc.)
- Size and duration
- Enterprise impact
- Projects encountering risk of failure
Once a project is identified as meeting the criteria, the project teams were required to present to the PRB a detailed report on the project which included:

- Background / History
- Project purpose and goals to be achieved
- Project Approach and methodologies
- Funding Components
- Project Plans
- Project Staffing
- Business commitment
- Current Status of Project
- Risks
- Future milestones

Once a project is presented to the PRB, the PRB reviews the status of the project and determines the value of continuing the project. The aforementioned criteria are used in the evaluation and a decision rendered for continuance or discontinuance of the project. The project teams are notified in writing.

It is envisioned that these projects will be required to submit monthly progress reports and may be asked to come back to the PRB for an update presentation over the life of the project.

As new projects are identified through the strategic planning and tactical planning process additional projects will be added to the PRB schedule for review.

The PRB focuses on existing and potential projects of $1.0 million or more or those that have sensitivity or critical in nature. The PRB becomes aware of projects through the Affinity Group Deputy CTO or through agency interaction. These projects can be listed in the agencies strategic plan or identified through federal or state mandates.

The initial thrust of the PRB was to review all projects in motion in order to catch up the process. New projects are added as needed. Projects are reviewed on an as needed basis or at a minimum every 6 months. This is dependent on the size and scope. Progress reports should be provided to the PRB through the PMO, however this has not been consistent. Reviews of the progress reports would stimulate additional reviews if necessary. Events triggering a review are primarily related to project initiation, target date changes, cost changes, scope changes, problems identified, policy issues and sensitivity to meeting mandates and enterprise impacts.

The PRB exercises the authority to continue, hold or stop a project where appropriate. Aside from this it does not have the authority to hold an agency accountable.
OLS Budget Questions

• Does the Project Review Board have rigid guidelines governing the decision whether to approve or reject a procurement request or do the board’s procedures allow it some discretion in how to evaluate projects that come before it? What specific guidelines does the board have?

RESPONSE

The PRB reviews projects at a more comprehensive level rather than individual procurements. It assesses the project based on the soundness of its scope of work, funding, project approach, quality of internal staffing to support the project, vendor competency, and high likelihood of success. The PRB uses the expertise of its members, OMB, Purchase Bureau, and the State CTO drawing upon resources within their respective organizations to review and provide feedback. In addition, each project goes through the OIT IPP (SAR) project review process which addresses the more detailed conceptual, logical and physical reviews lending to a more balanced technical solution balancing business needs against standards and interoperability. The goal of the PMO is to refine the IPP process to oversee this more detailed daily execution process of periodic reviews of projects as well as the procurements as they pass through the process.

• Please list all projects with a value in excess of $1 million that the Project Review Board has reviewed since inception, indicating for each project whether the board has approved or rejected it, as well as its original and most current cost projection.

RESPONSE

See Appendix B for the list of outstanding PRB projects.

45. In response to Discussion Point #39 in the FY 2008-2009 Department of the Treasury Budget Analysis, OIT indicated that its Program Management Office was planning to implement a Quality Assurance function for IT projects and to adopt a framework for facilitating the delivery of high-quality IT services. The Program Management Office coordinates multi-agency IT initiatives and guides in-house staff on application development and implementation, engagement management, project management and control, risk assessment and mitigation, cost estimation, and integrated planning. The office also participates in the review of strategic and tactical plans to ensure that agency projects conform to the State’s Enterprise Architecture structure. It also reviews all procurement requests to facilitate compliance with tactical plans and to find opportunities for cost savings.
Questions: Please explain OIT’s specific role in the managing of IT contracts and the monitoring for contract compliance. Does OIT manage and monitor all IT contracts or only a subset that meets specific criteria? Concerning project monitoring, what are the respective responsibilities of OIT’s Program Management Office, the Project Review Board, the Division of Purchase and Property in the Department of the Treasury, and the client agencies? Does OIT intend to alter this allocation of responsibilities? How many employees does the Program Management Office have?

RESPONSE

The PMO follows the guides established in Circular Letter 08-23-DPP regarding contract management functions. As part of its procurement review, the PMO ensures that all procurements comply with current state contract or processes (including Delegated Purchasing Authority (DPA)), regardless of whether or not OIT is responsible for the contract management. On a number of occasions, OIT has denied requests where the use of a specific contract is inappropriate (response to Question 49). Further OIT is involved in the development of all statewide IT contracts. Currently the PMO manages the following contracts:

- T-2158 Data Management Services
- M-0483 WSCA Hardware contract
- M-0003 Dell/ASAP software contract
- M-0817 Computer Aid IT Staff Augmentation
- M-7000 Data Communications and Network Equipment (NEW)

Further, the OIT Division of Telecommunication Services manages all statewide telecommunications contracts, including the negotiations to extend a number of contracts which resulted in significant savings to the State, along with corresponding budget reductions.

At this time, due to limited resources, OIT only manages OIT and statewide IT contracts. Agency contracts are managed internally. However, DTCOs and members of their staff are involved in all major agency IT projects to varying degrees.

The PMO currently does not participate in the actual management of projects but does participate indirectly through a variety of checkpoints in support of the PRB. However, it does review and collate agency tactical plans which identify projects and associated hardware, software and services that will be acquired during the current fiscal years as well as the next two years. These plans are then used to:

- Validate that procurements supporting such projects are in alignment with the tactical plans
- Identify projects that must go through the existing System Architecture Review (SAR) (see below)
Office of Information Technology FY 2010

OLS Budget Questions

- Identify potential cooperative, multi-agency projects when agencies identify similar projects. Examples of this include:
  - Time tracking systems for DHS and DMAVA health care facilities
  - Laboratory information managements for Agriculture, DEP and DHSS
  - Grants Management
  - Time keeping

Further, the PMO is about to implement the Integrated Planning Process (IPP). This process will be an expansion of the current System Architecture Review (SAR) process. The current SAR process requires agencies to submit information to OIT on projects that are in the conceptual and, later, development and implementation phases. Appendix C identifies the outstanding agency projects that have been submitted to the IPP/SAR process.

The IPP will expand this process to identify at five major milestones the types of resources that are required, the impact of those resources if committed to the process, and if OIT can support the project. These milestones include reviewing every project beginning at a conceptual step, logical planning, physical design, development/implementation and post implementation. Larger more complex projects can be reviewed at multiple times within any milestone to ensure success.

Based upon review of the tactical plans and the initial stages of the SAR, and now the IPP, information is formulated for the Project Review Board, whose responsibilities and activities are outlined in Question 44.

The Program Management Office currently has 18 staff members. Responsibilities and numbers of staff are as follows:

- Strategic & Tactical Plan review - 3
- Agency Procurement review – 3
- Enterprise Contract Management – 2
- Integrated Planning Process (IPP/SAR) – 2
- OIT Planview (time keeping)/project tracking system support – 5
- OIT Billing system support – 1
- OIT Asset management - 1
- Research and advisory services - 1

46. In cooperation with IT organizations in Executive branch agencies, OIT has developed the State of New Jersey Information Technology Strategic Plan for fiscal years 2008 through 2010. The plan
expresses goals, objectives, and strategies in six IT areas: governance, statewide efficiencies, enterprise architecture, e-government, security, and IT workforce management.

One goal under the plan is to maximize the efficient delivery of agency IT services through the cost-effective use of all state IT resources. Among the initiatives is the completion of an inventory of statewide IT assets and services, the completion of an infrastructure consolidation assessment and plan for all agencies, the establishment of statewide IT data sharing policies to increase efficiencies of data collection and use among different layers of government, and the creation of a formal process by which OIT and the Division of Local Government Services in the Department of Community Affairs meet periodically with all 21 of the county IT officers as a group and communicate with them on an ongoing basis so as to identify areas where the State and its counties could join resources to achieve greater statewide efficiencies.

• Questions: Please provide an update on the infrastructure consolidation assessment. Has the assessment been completed? If not, by which date does OIT expect its completion? What have been the results of the assessment? Does OIT perceive a potential for significant cost savings? Has an infrastructure consolidation plan been adopted? If not, by which date does OIT expect its completion? If so, please submit a copy of the plan.

RESPONSE

To-date the detailed infrastructure consolidation assessment has been performed for DOT, DHSS and disaster recovery. Additionally information has been gathered as part of the redesign and upgrade of the Garden State Network and asset information has been gathered from 17 agencies. The completed enterprise infrastructure consolidation assessment has not been completed, due to our focus on more immediate priorities.

• Please provide an update on the establishment of statewide IT data sharing policies to increase efficiencies of data collection and use among different layers of government. Have the policies been established? If not, by which date does OIT expect their establishment? If so, how do the new policies specifically allow for cost efficiencies and what are the projected cost savings?

RESPONSE

OIT has drafted and published a number of Data Sharing Policies directed to classification of data assets and outlining how data should be shared. These provide the framework for all agencies to align to the state enterprise. Copies of these are provided in Appendix D.
OLS Budget Questions

• Please elaborate on OIT’s outreach to county IT offices and its efforts to jointly leverage resources. Has a formal consultation process been established? With which counties has OIT communicated thus far? What categories of projects does OIT have in mind when it studies resource pooling with counties? Has OIT already identified a possible joint project or implemented one?

OIT has been actively working with local governments on primarily three fundamental fronts. This is not a formal process for the most part but executed as needed. OIT’s criteria are primarily aimed at ensuring minimum standards, consistency, interoperability and opportunities for cost savings. OIT initiates such projects when there is a statewide need identified in its own strategies or when we notice a trend in local initiatives whereby interjecting. When OIT becomes aware of local initiatives that involve a greater state impact, OIT performs an outreach and involves appropriate state entities in the process. The three most notable are as follows:

• Use of Broadband – OIT has been organizing an avenue between the State and the local governments on the use and expansion of broadband. Since this will lay the groundwork for all future uses of broadband and related interconnectivity and has the greatest potential for use and cost, OIT needed to take a lead. OIT has been working with local governments, NJN, Education and quasi state entities, to list a few, to review the trends. OIT is working closely with the principal parties and will form a statewide broadband committee to make recommendations for the best implementation of such technology.

• Radio Interoperability – through the use of grants, the state interoperability group under OIT has been fostering a greater degree of cooperation across local government and promoted significant consolidation efforts while modernizing equipment. This trend will continue.

• Use of the GSN and existing state owned fiber resources – OIT has been working closely with DOT and the Turnpike Authority over the past three years examining opportunities to leverage its fiber assets. To date connections to OARS and a number of redundant paths have been shifted to state owned fiber thus reducing increased costs for leasing data lines. Strategies have been prepared to further leverage these assets with significant projected savings to the state. By leveraging these assets OIT would position the future of the GSN to provide connectivity to local governments amongst themselves as well as the enterprise. County government is connected to the Garden State Network today, principally where county law enforcement is co-located with local law enforcement and uses the network for these purposes. As the GSN migrates from its current leased-line-based core infrastructure to a fiber-based infrastructure, the opportunities for local government use of the state asset will grow.
47. In December 2006, the Administration placed a **moratorium on the procurement of IT equipment and consultant services** under the Direct State Services budget category (operating expenses). Exempted from the moratorium are initiatives whose disruption would increase future costs or trigger a significant loss of investment, as well as emergency maintenance, repairs and supplies under $2,500, and projects mandated by the federal government. In response to OLS discussion point #41 in the FY 2008-2009 Department of the Treasury Budget Analysis, OIT indicated that the moratorium was not only intended to achieve reductions in spending, but also to provide for structured growth in the IT infrastructure and to force agencies to prioritize their IT projects. OIT noted that the “unstructured growth of technology projects during 2002 and 2005 resulted in the individual build-out of infrastructure capacity within each agency” and that the State could no longer financially sustain that pace.

In a written follow-up response to a question raised during the Department of the Treasury’s budget hearing before the Assembly Budget Committee on April 15, 2008, OIT stated that the continuation of the moratorium jeopardized projects that should normally be undertaken in fiscal years 2009 and 2010: a major upgrade to the State’s core IT infrastructure to meet the projected growth in network demands; the replacement of enterprise servers and storage and of agency servers and PCs that are near the end of their useful life; the replacement of backend business applications that are more than 20 years old (payroll, financials, personnel); and the development of soft- and hardware for the retention and search of electronic records to better respond to requests for discovery from the courts.

- **Questions:** Please provide an example of the unstructured growth of IT projects during 2002 and 2005, explaining the ways in which the disorganized arrangement worked to the detriment of the State, and the ways in which OIT rectified it, including an indication of the resources the rectification consumed. Has OIT now gained control of the unstructured growth of IT projects? Has the ordering process consumed significant resources and kept OIT from advancing its restructuring agenda more aggressively?

- **Is OIT aware of cases in which the moratorium has adversely affected the quality of services provided by State agencies?** Please indicate in which areas OIT expects the continuation of the moratorium in fiscal year 2010 to adversely impact program performances and service delivery. Please report on the status of the following projects that OIT would normally like to undertake: an upgrade in the core infrastructure, the replacement of enterprise servers and storage, the replacement of agency servers and PCs, the development of backend business applications to replace applications that are more than 20 years old (payroll, financials, personnel), and the finding of an IT solution to e-mail archiving and electronic records retention needs.

**RESPONSE:**
Unstructured Growth of IT Projects: Several projects were in motion during the time frame in question. These projects were driven by federal mandates and associated federal funding OIT through the PRB has gained greater control over these projects and interjected greater control and oversight while managing a concert of multiple projects with sometimes conflicting demands on OIT resources. For example, NJSPIRIT was encountering problems during its development cycle, the PRB focused attention on the project and lent OIT resources to work with the agency to finalize its implementation. This project was implemented in April 2008 as a phased in approach and continues to operate. As indicated in question 40, OIT is working with DCF and DHS to staff for the long-term maintenance of this system when the vendor contract expires in the spring of 2010.

NJSuccess was recently placed on “Hold” in order to focus available OIT and LWD resources on the Unemployment Insurance program. This was accomplished through delivering a Web based self service application thus averting the need to hire 122 additional operators to cover the demand.

In addition to the large scale projects addressed by the PRB there are almost 1800 individual small project requests in queue at OIT which are not reviewed by the PRB. These same projects are not prioritized by any cross agency board and they vie for the same limited OIT resources.

Affect of Moratorium: OIT is not aware of any direct problems caused to date by the moratorium. However, we are aware that potential problems could arise with respect to aging infrastructure within OIT and the agencies.

Status of the Following Projects: Typically, OIT defines the core infrastructure as the wide-area network, or Garden State Network, storage and backup, and mainframe/distributed server environment. For the purposes of responding to the above question, the GSN will be referred to as “core infrastructure, since the other categories are identified separately,

- **Upgrade in the Core Infrastructure:** The GSN consists of lines that are leased from major telecommunications vendors and are connected by a myriad of state-owned hardware and software. Staff is responsible for controlling the increase of leasing costs, while providing the bandwidth needed for e-government demands. To address this growth, in FY2008, OIT began its redesign of the GSN. This design is based upon leveraging the state-owned NJ Turnpike Authority’s (NJTPA) fiber optic network. This will eventually reduce the state’s reliance on leased lines and will provide a much more robust network. Without initiative, at the current rate of growth in network traffic, OIT anticipates the need to increase the size of the leased lines in early FY2011 at a cost ranging from $2-8 million annually.

Progress on this major initiative has been slow. It has only been within the last month that a contract has been in place to buy much needed network equipment and there are a variety of issues related to acquiring the services of the NJTPA utility vendor. Despite these
setbacks, OIT continues to move forward so that the State can realize both the long-term cost savings through the reduction in the number of leased lines and the capacity growth and expansion of service capability required to support agency business needs. At their extreme, not having the capacity or service capability.

- **Replacement of Enterprise Servers and Storage:** During the past fiscal year OIT has made some progress in this area. The most significant upgrade has been the partial replacement of an antiquated and labor intense backup environment for server environment with a comprehensive virtual tape library infrastructure. Ultimately, this new environment will allow all servers and both mainframes to generate backup data at OARS.

With regards to servers, OIT, in conjunction with MVC purchases for MATRIX, was able to negotiate a 50% discount with IBM in order to upgrade two of our enterprise servers.

**Replacement of Agency Servers and PCs:** OIT’s role in the replacement of agency servers is normally handled through review of the tactical plans and procurements. However, in a number of cases, OIT has worked with agencies to provide OIT server capacity for agency applications or to house agency servers. OIT’s support of NJKids and MATRX are examples of the latter.

For PCs OIT’s primary role is to ensure, through the procurement review process, that agencies are getting the best configurations for their needs and best volume discounts. OIT feels that the support of PCs is an appropriate responsibility for agency staff, since the PC is the primary desktop tool for most employees.

- **Development of Backend Business Applications:** Due to budgetary constraints there has been little progress on replacement of the major centralized administrative systems cited in the question. The replacement of these systems would be extremely expensive would require full-time dedicated business and IT resources. However, the implementation of administrative systems projects, including e-CATS, SAGE, and e-procurement continue to replace and/or enhance legacy processes. OIT understands the overall issue and has been working with the agencies to explore incremental upgrades to these systems rather than wholesale replacement efforts. Examples of this include the recent E-Catalog application as a front end to the state’s procurement system (MACS-E).

- **IT Solution to e-Mail Archiving and Electronic Records Retention:** An internal committee of agency business and IT personnel was created by OIT to develop and recommend strategies and implementation blueprints for an enterprise-wide e-mail archiving solution. The committee is finalizing a report of those recommendations. Once the report is finalized and reviewed, OIT will determine the next steps.
As the internal committee worked on an enterprise solution, OIT convened a separate work group of agencies who have urgent archiving needs due to litigation. These agencies, DEP, DOT, and State Police, must have solutions in place well before an enterprise solution is finalized. This work group is in the final phases of evaluating four products and will have a recommendation shortly.

- **What was the value of approved IT equipment and consultant services procurements by department in fiscal years 2007 and 2008? What is their projected value in fiscal year 2008 and 2009?**

**RESPONSE:**

See Appendix E for detailed lists of all FY2007, 2008, and 2009 procurements submitted to OIT for review and the total number approved.

48. According to the Office of the State Auditor’s March 2008 audit report on the Office of Information Technology, **Enterprise Data Warehouse**, an enterprise data warehouse “is a database environment dedicated to providing a single, comprehensive view of the enterprise and provides a reliable source of consistent information for financial and strategic decision-making for the enterprise as a whole.” To improve the performance, integrity, and security of New Jersey’s enterprise data warehouse; the State Auditor recommended that OIT develop a strategic plan for the enterprise data warehouse architecture; that it continue to develop and employ the required policies, procedures, and standards to fully implement OIT’s Information Security Program; and that it continue to develop and employ the appropriate technical documentation required to ensure the integrity of processed data.

In reply OIT noted that a strategic plan for the enterprise data warehouse had existed since its inception, yet it disputed the practical need for the production of a project plan in light of the environment in which the project actually operated. Since the data warehouse had not had consistent funding, it had expanded incrementally and opportunistically as resources for smaller projects had become available. But OIT concurred that more emphasis needed to be placed on ensuring the accuracy of the data entered into databases. It stated that it had just improved the processes that document the loading of data and verify the quality of those loads.

- **Questions: Please illustrate the history of the enterprise data warehouse either in the form of a brief description or a chronological listing. Please pay particular attention to any expansion and how it was financed. Does OIT believe that not having a project plan for the data warehouse might adversely affect the chances of securing funding for improvements?**
OLS Budget Questions

- Please outline the strategy OIT would like to deploy to improve the integrity of the data stored in the enterprise data warehouse. Has the office devised multiple courses of action in anticipation of various financial contingencies? To which extent can OIT, as opposed to the users moving data into the data warehouse, control the quality of the data that are being stored in the data warehouse?

RESPONSE

Please illustrate the history of the enterprise data warehouse either in the form of a brief description or a chronological listing. Please pay particular attention to any expansion and how it was financed.

The term Data Warehouse does not refer to a single data file but rather an environment that fosters data sharing. This environment is dynamic and will grow over time as needed to support agency and enterprise needs. It is a construct or framework under which data sharing is enabled and to the extent possible normalized (duplication reduction). New Jersey has an enterprise data warehousing environment. It is this environment that houses multiple subject areas, such as Financial, Payroll, Motor Vehicle Crash, Human Resources, Emergency Medical Service Responses, Motor Vehicle Revenue, Time and Leave, Purchasing, and others. However, this is a brief description of the development of the environment, followed by a chronology of work efforts. Please note that costs include estimates of staff time at the appropriate billable rate, not at the actual, lower salary costs.

The initial enterprise data warehousing initiative, the OMB Financial subject area version 1.0, was created at a total cost of about $950,000. This includes an estimate for the pro-rata portion of existing enterprise infrastructure used, the original vendor development contract, the additional software licensing, and the State employee time. Subsequently, there have been additional software investments of 1.4 million dollars for a broad range of data management tools used both in this environment and for non-data warehouse initiatives. These include data quality tools, metadata management tools, and reporting tools. There has also been about $1.1 million in additional hardware, primarily the pro-rata portion of the shared environment refresh and the additional storage required by the many new data sources.

With regard to development costs, the three release of the Crash data warehouse environment will total about $1.3 million when completed. The largest single effort is release 1.0 of the DOT Integrated Data Warehouse, with a budget of about $800,000 for personnel (State and consultants). The approximately seventy-five other efforts have cost between four thousand and three hundred thousand dollars for development, with the majority of the efforts costing less than fifty thousand dollars.

All of these efforts have leveraged the tools purchased, the environment deployed, the expertise of State development staff, and data where it already existed. There is no other investment in technology
OLS Budget Questions

tools and methodology that has produced a greater return on investment, both tangible and intangible, than the enterprise data warehousing program.

Does OIT believe that not having a project plan for the data warehouse might adversely affect the chances of securing funding for improvements?

Data Warehousing is considered an enterprise dynamic program, not a single project. Our data warehousing program is defined in the New Jersey Common Information Architecture (NJCIA), the State’s strategic enterprise information strategy. The enterprise data warehousing environment has substantially followed the program plan originally established in September 2000. That program plan has been modified periodically to reflect changes in technologies, priorities, and data assets.

In place of a traditional project plan, OIT follows constructs and policies regarding the development and expansion of any data warehousing need as it integrates into the data warehouse. This is applied to all data warehouse candidates which leverages the previous data contained therein. This allows for the maximum use of data collected. Any growth in the data warehouse is addressed individually through project initiatives. New data is identified and incorporated, and old data is no longer used.

Dozens of individual projects have added new data to the environment or published new data from the environment. These incremental efforts have had their own individual project plans. There have also been project plans for hardware and software enhancements and refreshes. These activities are the appropriate level for project plans.

Please outline the strategy OIT would like to deploy to improve the integrity of the data stored in the enterprise data warehouse.

OIT believes its current integrity of the data in the enterprise data warehousing environment is operating well within industry and government guidelines. We perform extensive cross-checking with data stewards before data is “released” for consumption in the data warehouse. In some cases, this cross-checking has uncovered data quality issues in the source systems feeding the data warehouse that led to overall improvements in the data quality.

OIT will continue to pursue efforts that improve the quality, usefulness, and timeliness of the data. Our data architects and our data warehouse data analysts make incremental improvements to data, data models, data definitions, data processes, data structures, and data publication mechanisms as time permits. These efforts are part of every data warehousing initiative’s ongoing support. Greater strides could be made to improve our integrity efforts if more resources were made available.

Has the office devised multiple courses of action in anticipation of various financial contingencies?
Fiscal constraints reduce or in some cases delay new data warehouse project development. Our focus would shift to maintaining the current production environment, reacting to emergency information requests, developing data warehousing projects, and adding additional enhancements as time permits. In about two to three years, the hardware platform that hosts the data warehousing environment would need to be refreshed. This will be addressed in future budget submissions.

To which extent can OIT, as opposed to the users moving data into the data warehouse, control the quality of the data that are being stored in the data warehouse?

OIT estimates that the overall quality of the data in the data warehouse is above standard, because it has been a partnership between the agency business users and the OIT data warehouse developers. Developers are responsible for process, but business users are responsible for definition. You must have both to have good data quality. What the State could improve on, not just in data warehousing, but across the board, is better data governance.

There are two parts to this. One is the identification of a data steward (a business, not a technical, user) who understands the definition of the data in a particular area of the business and who can make decisions on appropriate definition, access, and usage of that data. The second is the use of a data governance board to develop overall policies, resolve definition disputes that cross business domains, and serve as the data steward for universal data at the enterprise level.

49. According to the Office of the State Auditor’s December 2008 audit report on Statewide Data Privacy, OIT has significantly enhanced the privacy of confidential data. Nonetheless, the State Auditor concluded that personal data maintained at State agencies might still be at risk of unauthorized disclosure because of a lack of existing security policies and procedures. To remedy that shortcoming, the State Auditor recommended the promulgation of statewide data security policies on portable data storage devices and data encryption. In addition, the State Auditor advised the drafting of consistent and comprehensive agreements with third parties that require the safeguarding of the confidentiality of personal information.

- Questions: Please comment on the State Auditor’s recommendation to develop statewide data security policies on portable data storage devices and data encryption and to draft consistent and comprehensive agreements with third parties that require the safeguarding of the confidentiality of personal information. Does OIT intend to pursue the initiatives? If so, has it begun to work on them and by which date does it expect their implementation? If not, for what reasons does OIT think that the initiatives do not merit its attention?
Not only does OIT agree with the State Auditors recommendations but has been working to achieve those goals independent of the findings. The details of the initiatives are as follows:

OIT has implemented and continues to implement a comprehensive security policy framework based on ISO 27001 as well as certain NIST standards where applicable to insure the protection of its information assets across the executive branch in a consistent, uniform fashion. These constitute a broad spectrum of policies covering all aspects of information security practices and disciplines. The Statewide Office of Information Security continues to identify gaps in order to publish policies focusing first where the greatest needs are identified as representing the greatest threat or liability. In addition certain foundational Policies must be implemented before other associated protection dictums can be rolled out. To that end and as indicated by the Audit findings, OIT implemented the Statewide Information Asset Classification and Control Policy, Standards and Procedures which comprehensively requires all State Departments and Agencies to classify assets and ensure appropriate protection. As such this was a foundational policy from which other policies reference such as data storage policies.

Since 4th quarter of 2008 (2nd quarter FY 09) and prior to the release of the Audit, OIT began working with “Endpoint” Device Encryption providers to understand the toolset capabilities. This is a necessary precursor to map business requirements for the usage of these toolsets, and to develop appropriate procedures and functionality for protection that can be subsequently used in policy provisions. In addition, OIT worked with agencies to develop security requirements and implementation specifications for such protections and tools. It is important to note that there is a myriad of products in the market place for device protection. Not all provide the same functionality. It was and is important to ensure that products deployed and implemented meet the goals of consolidation and existing architectural builds. Most importantly we began work with the vendors to ensure competitive pricing and availability of products through the DELL ASAP contract. In February of this year agencies were advised that these products were available for purchase and that they had functionality as determined through the group piloting/testing done in the fall.

At this point in time, the Statewide Office of Information Security has recently developed a draft Portable Computing and Storage Device Protection policy that was disseminated to all Department and Agency IT Directors for their review and comment. Comments will be due in late May 2009. Once all comments have been received, and incorporated where appropriate, this policy will be published as a Statewide Policy. This final publication date should be before the end of FY2009.

With regard to the Third Party agreements requiring the safeguarding not only personal but all confidential/classified information, OIT has taken a number of steps. First, it has performed a comprehensive review of the “Extranet” connectivity process (i.e. data transmissions from a server within the GSN to a server of a business partner or other non-state government entity outside of the GSN). From this review process a set of Policy and Procedure documents were developed and disseminated to all Departments and Agencies for their comments. Currently those comments are being
incorporated and these documents will be published before the end of the FY2009. This covers a significant aspect of third party connectivity concerns and articulates the State’s expectations regarding not only those protections but identifies others as well. This policy will cover all existing and future extranet connections to ensure the protection is implemented uniformly.

In addition, OIT has developed a draft Third Party Access Policy which will be disseminated along with the draft Portable Computing and Storage Device Protection Policy and its publication timelines will be consistent as well.

OIT is taking a much more holistic approach on the issue of data encryption and related policies. Data encryption is in general difficult for the end user to use, overwhelming to manage and extremely costly to implement. As a result, a comprehensive data encryption policy would need to cover all access points, desktops, servers, and the transmissions itself. Because of the complexities and costs of encryption, there are so many circumstances that exist today within our IT infrastructure that would render it impossible to write such a policy without confronting so many ways in which it would be impossible to carry out such an edict. Take one such example: A large portion of the State’s information assets reside on the mainframe. There are currently no encryption capabilities on the mainframe. To enable that would cost millions of dollars. There is no encrypted transit (SSL) to the mainframe. To implement that would be costly as well. That said, there are other compensating controls that are becoming widely adopted in the industry which provide similar protections in a more cost effective manner. It is important to note though that even those costs are significant to implement. Consequently, OIT would prefer to develop security protection policies that advocate employing appropriate controls that are not technology specific. Specifically OIT through the Statewide Information Security Office has already begun the groundwork for implementing this foundational policy and would expect this policy to be ready for comment by the end of FY2009.

One trend which is reaching critical mass in terms of a compensating control to be leveraged in lieu of encryption is Data Rights Management (DRM) solutions and Data Loss Protection (DLP) solutions. These products involve the ongoing monitoring of specific assets based on access control rules. Another solution involves the use of file level encryption that is already part of OIT database management services policies.

Concurrent with these solutions, the Statewide Office of Information Security is developing foundational policy for Access control and user management along with associated policies in support of ensuring information is protected. This policy would work in tandem with any DRM/DLP solutions that may be requested for purchase by agencies or OIT. This policy is expected to be ready for draft by August of 2009. Additionally, OIT has implemented a Vulnerability Management Program for all Departments and Agencies in order to better protect information assets by proactively scanning infrastructure devices for known vulnerabilities. Once identified, these vulnerabilities can likewise be proactively remediated
before they are exploited. To date all D & A’s have been trained in the use of these services. OIT has begun working with agency staff to begin a baseline scan of each segment of the GSN.

Finally, in addition to these specific policies and services, OIT will continue to publish additional ISO security policies as well as additional security services to support the confidentiality, integrity and availability of the State’s information assets.

50. In its August 2007 audit report on the Board of Public Utilities (BPU), the State Auditor advised improving computer applications the BPU used in the management of underground utility safety programs. The State Auditor deemed inadequate the application tracking data on the location of interstate gas pipelines and their inspection status under the Pipeline Safety Program. The State Auditor also stated that meaningful analysis of incidents with underground facilities under the “Underground Facility Protection Act” pursuant to P.L.1994, c.118 (C.48:2-73 et seq.), was impossible because the current computer application could not provide adequate data. The law requires excavators to call a toll-free number three days prior to excavation and companies to mark their underground facilities near the excavation to prevent damage. Replying to Discussion Point #52 in the FY 2008-2009 Department of the Treasury Budget Analysis, the BPU affirmed that its current applications did not allow for the effective management of underground facilities. It also provided a chronological listing of events indicating that the BPU’s IT staff had first contacted the OIT in August 2003 regarding a system upgrade. Since then, it appears that OIT has repeatedly endorsed a specific course of action just to make an about-face and impose a different course of action.

• Questions: Please provide an update on the status of the envisioned improvements of the computer applications the BPU uses in the management of underground utility safety programs. Please explain, from OIT’s point of view, the complications that have led to the delay in the execution of the project. What kind of priority is OIT assigning to the development of applications for the management of underground utility safety programs? Does the failure to migrate to a new system significantly endanger public safety?

RESPONSE

BPU contacted OIT in August 2003 to start discussions on identifying the need and an approach. OIT provided direction and worked with the agency for several months. BPU had some difficulty defining the scope and requirements and took longer than expected. In late 2004, OIT reviewed and approved their approach and BPU began the paperwork cycle. The approach was to engage consultants that BPU would manage for a custom development effort. OIT had some concerns over the BPU consultant selection and related qualifications. BPU proceeded with these consultants and after eight months the project experienced difficulty. OIT halted the project in June 2006 as a result of consultant personnel issues and lack of performance. After an OIT review, BPU was advised that OIT could not take over the
OLS Budget Questions

Project internally due to limited resources. The scope and complexity expanded beyond conventional body shop contract requirements and it was decided that is should be competitively bid. As a result, the BPU IT staff began compiling the initial draft of the RFP in the fall of 2007. In an effort to save additional expenditures on consultants, OIT provided in-house resources and consulting services to the BPU IT staff (at no cost) to draft a suitable RFP that would meet their needs. After reaching agreement on this issue, the BPU IT staff, working with OIT submitted a near-final draft of the RFP in February 2008. The final RFP was completed and approved by OIT in April 2009 and subsequently submitted to Treasury by BPU in late April 2009. Once approved, the RFP will be publicly advertized and potential contractors would have an opportunity to submit a bid response.
51. Addressing an OLS discussion point in the FY 2007-2008 Department of the Treasury Budget Analysis, the OIT stated that each State agency established its own policy of assigning State-issued **cellular wireless devices** (cell phones, blackberries, air cards, etc.) to its employees. Their number grew 370 percent from 3,613 devices in FY 2003 to 16,012 devices in FY 2007. OIT program data in the FY 2009 Executive Budget indicated that the office expected to support 24,000 cellular wireless devices in that fiscal year (page D-437). The FY 2010 Executive Budget no longer features information on the size of the State’s voice network.

RESPONSE
The following table identifies the total number of cellular devices.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>116</td>
<td>109</td>
<td>110</td>
<td>105</td>
<td>(5)</td>
</tr>
<tr>
<td>Banking &amp; Insurance</td>
<td>31</td>
<td>62</td>
<td>63</td>
<td>72</td>
<td>9</td>
</tr>
<tr>
<td>Chief Executive</td>
<td>166</td>
<td>145</td>
<td>157</td>
<td>160</td>
<td>3</td>
</tr>
<tr>
<td>Commerce</td>
<td>15</td>
<td>36</td>
<td>39</td>
<td>30</td>
<td>(9)</td>
</tr>
<tr>
<td>Community Affairs</td>
<td>229</td>
<td>191</td>
<td>404</td>
<td>394</td>
<td>(10)</td>
</tr>
<tr>
<td>Corrections</td>
<td>286</td>
<td>292</td>
<td>312</td>
<td>379</td>
<td>67</td>
</tr>
<tr>
<td>Education</td>
<td>101</td>
<td>109</td>
<td>117</td>
<td>104</td>
<td>(13)</td>
</tr>
<tr>
<td>Environmental Protection</td>
<td>832</td>
<td>939</td>
<td>1,691</td>
<td>1,141</td>
<td>(550)</td>
</tr>
<tr>
<td>Health</td>
<td>841</td>
<td>1,009</td>
<td>1,066</td>
<td>1,179</td>
<td>113</td>
</tr>
<tr>
<td>Human Services</td>
<td>6,671</td>
<td>1,398</td>
<td>1,426</td>
<td>1,166</td>
<td>(260)</td>
</tr>
<tr>
<td>Children &amp; Families / DYFS</td>
<td>n/a</td>
<td>5,992</td>
<td>5,660</td>
<td>5,595</td>
<td>(65)</td>
</tr>
<tr>
<td>Judiciary</td>
<td>84</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Labor</td>
<td>132</td>
<td>124</td>
<td>198</td>
<td>224</td>
<td>26</td>
</tr>
<tr>
<td>L&amp;PS - Homeland Security</td>
<td>179</td>
<td>217</td>
<td>239</td>
<td>211</td>
<td>(28)</td>
</tr>
<tr>
<td>L&amp;PS - State Police</td>
<td>n/a</td>
<td>n/a</td>
<td>1,149</td>
<td>1,887</td>
<td>738</td>
</tr>
<tr>
<td>L&amp;PS - All Other</td>
<td>3,181</td>
<td>3,230</td>
<td>1,552</td>
<td>1,600</td>
<td>48</td>
</tr>
<tr>
<td>Legislative Services</td>
<td>26</td>
<td>24</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Military &amp; Veterans Affairs</td>
<td>292</td>
<td>162</td>
<td>276</td>
<td>202</td>
<td>(74)</td>
</tr>
<tr>
<td>Motor Vehicle Commission</td>
<td>n/a</td>
<td>395</td>
<td>435</td>
<td>556</td>
<td>121</td>
</tr>
<tr>
<td>OIT</td>
<td>128</td>
<td>118</td>
<td>137</td>
<td>150</td>
<td>13</td>
</tr>
<tr>
<td>OIT - Emergency Loaners</td>
<td>150</td>
<td>152</td>
<td>152</td>
<td>152</td>
<td>0</td>
</tr>
<tr>
<td>Personnel</td>
<td>47</td>
<td>51</td>
<td>51</td>
<td>40</td>
<td>(11)</td>
</tr>
<tr>
<td>Public Advocate</td>
<td>10</td>
<td>27</td>
<td>68</td>
<td>90</td>
<td>22</td>
</tr>
<tr>
<td>State</td>
<td>17</td>
<td>31</td>
<td>29</td>
<td>38</td>
<td>9</td>
</tr>
<tr>
<td>State - Public Broadcasting</td>
<td>57</td>
<td>56</td>
<td>73</td>
<td>63</td>
<td>(10)</td>
</tr>
<tr>
<td>State Parole Board</td>
<td>117</td>
<td>257</td>
<td>353</td>
<td>511</td>
<td>158</td>
</tr>
<tr>
<td>Transportation</td>
<td>1,743</td>
<td>1,277</td>
<td>1,268</td>
<td>1,196</td>
<td>(72)</td>
</tr>
<tr>
<td>Treasury</td>
<td>642</td>
<td>652</td>
<td>780</td>
<td>824</td>
<td>44</td>
</tr>
<tr>
<td>TOTALS</td>
<td>16,093</td>
<td>17,055</td>
<td>17,805</td>
<td>18,069</td>
<td>264</td>
</tr>
<tr>
<td>Difference from Prior FY</td>
<td>962</td>
<td>750</td>
<td>264</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Projected for FY2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18,369</td>
</tr>
<tr>
<td>Total Expenditures</td>
<td>$7,717,036</td>
<td>$7,289,722</td>
<td>$7,688,369</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Total # of Users: 510,560

# Service Communities: 481

# Online Service Managers: 1,140

Avg logins per weekday: 22,370
Avg logins per weekend day: 5,878

<table>
<thead>
<tr>
<th>Top 20 Service Communitites</th>
<th>Primary Business Owner</th>
<th># Users</th>
<th># Service Managers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pensions Client Services</td>
<td>Treasury - Pensions</td>
<td>173,127</td>
<td>90</td>
</tr>
<tr>
<td>NJ Employee Self Service</td>
<td>Treasury - OMB</td>
<td>12,060</td>
<td>11</td>
</tr>
<tr>
<td>DEP Online</td>
<td>Environmental Protection</td>
<td>12,032</td>
<td>13</td>
</tr>
<tr>
<td>Vendor Payment Inquiry</td>
<td>Treasury - OMB</td>
<td>5,591</td>
<td>6</td>
</tr>
<tr>
<td>DCA-Firefighters</td>
<td>Community Affairs</td>
<td>4,757</td>
<td>4</td>
</tr>
<tr>
<td>DOBI Real Estate Services</td>
<td>Banking &amp; Insurance</td>
<td>3,466</td>
<td>10</td>
</tr>
<tr>
<td>NJ Premier E-Business Services</td>
<td>Office of Economic Growth</td>
<td>3,169</td>
<td>2</td>
</tr>
<tr>
<td>CTTS_USER</td>
<td>Labor</td>
<td>3,042</td>
<td>19</td>
</tr>
<tr>
<td>DOBI Annual Reports</td>
<td>Banking &amp; Insurance</td>
<td>2,865</td>
<td>4</td>
</tr>
<tr>
<td>GovExchange</td>
<td>Community Affairs</td>
<td>2,613</td>
<td>1</td>
</tr>
<tr>
<td>MVC CAIR</td>
<td>MVC</td>
<td>1,953</td>
<td>10</td>
</tr>
<tr>
<td>Agriculture FNS</td>
<td>Agriculture</td>
<td>1,888</td>
<td>3</td>
</tr>
<tr>
<td>DEP Employee</td>
<td>Environmental Protection</td>
<td>1,704</td>
<td>25</td>
</tr>
<tr>
<td>USFHEA</td>
<td>Community Affairs</td>
<td>1,698</td>
<td>43</td>
</tr>
<tr>
<td>DOT-eMail</td>
<td>Transportation</td>
<td>1,689</td>
<td>14</td>
</tr>
<tr>
<td>DOT-Employee</td>
<td>Transportation</td>
<td>1,386</td>
<td>6</td>
</tr>
<tr>
<td>Lottery Agent</td>
<td>Lottery Commission</td>
<td>1,337</td>
<td>3</td>
</tr>
<tr>
<td>NJSP email</td>
<td>State Police</td>
<td>1,300</td>
<td>29</td>
</tr>
<tr>
<td>Child Nutrition Submitter</td>
<td>Agriculture</td>
<td>1,274</td>
<td>63</td>
</tr>
<tr>
<td>Child Nutrition Certifier</td>
<td>Agriculture</td>
<td>1,263</td>
<td>52</td>
</tr>
</tbody>
</table>
Current Top 3 Portal Initiatives

GeoLearning Rollout:
Primary Client: HRDI / Treasury
# of Users: 50,000
Affected Departments - All (initially DEP, DOT, MVC, BPU)
Target Date: 5/5/09

Streamlined Registration:
Primary Client: DEP
# of Users: 12,000+
Affected Departments - DEP & Premier Business Services
Target Date: 6/1/09

Redesigned Access Management:
Primary Client: MVC
# of Users: 1 million
Affected Departments - All
Target Date: Q2 2010
Action Council for the Economy
Administrative Office of the Courts Business Intelligence
Advisory Commission on the Status of Women
Agency Strategic Planning Evaluation Team
Agriculture FNS
American Recovery and Reinvestment Act Information Technology Coordinators
Appeals Computerized Entry System
Asset Database
Background Investigator
Background Questionnaire
Beach Monitoring
Best Management Practices
Board of Health Survey
Board of Public Utilities Administrator
Board of Public Utilities Terminal Services
Business Incubator Administrator
Business Portal
Casino Control Commission Documents
Casino Control Commission Employee
Child Fatality and Near Fatality Review Board
Child Nutrition Certifier
Child Nutrition Submitter
Civil Service Commission Email
Commerce Commission Email
Commerce Commission Intranet
Commerce Commission Netstorage
Commerce Commission Travel Guide Administrator
Commission on Cancer Research Grant Review
Commission on Higher Education Email
Communications Service Requests
Communicator
County Environmental Health Act
County Finance Officer
County Freehold Board Clerk
County Tax Boards
Criminal Justice Conferences
CTTS_USER
Daily Leads
DCA-Firefighters
Delaware River Basin Commission Email
DEP Employee
DEP Online
Dept of Agriculture Child Nutrition Program
Dept of Agriculture County Animal Response Team
Dept of Agriculture Documents
Dept of Agriculture Email
Dept of Agriculture Food and Nutrition Administration
Dept of Agriculture Food Distribution Programs
Dept of Agriculture Mainframe Access
Dept of Agriculture Reportable Animal Disease System
Dept of Agriculture State Agriculture Development Committee
Dept of Agriculture Wholesale Buyers Guide
Dept of Banking and Insurance Banking Services
Dept of Banking and Insurance Complaint Officer
Dept of Banking and Insurance Documents Approved for Public
Dept of Banking and Insurance Email
Dept of Banking and Insurance Horizon Submissions
Dept of Banking and Insurance Individual Health Coverage Board
Dept of Banking and Insurance Mainframe Access
Dept of Children and Families Bull Mainframe Access
Dept of Children and Families Fiscal Operations
Dept of Children and Families Human Resources Business Portal
Dept of Children and Families Office Facilities and Space Planning Projects
Dept of Community Affairs Business Intelligence
Dept of Community Affairs Council on Affordable Housing
Dept of Community Affairs Council on Affordable Housing, Municipalities
Dept of Community Affairs Division of Fire Safety
Dept of Community Affairs Division of Fire Safety Citrix
Dept of Community Affairs Division of Fire Safety Fire Officials
Dept of Community Affairs Division of Fire Safety National Fire Academy Training Programs
Dept of Community Affairs Division of Local Government Services Staff
Dept of Community Affairs Email
Dept of Community Affairs Gartner RFP Review
Dept of Community Affairs Housing Registration Inspection Management System
Dept of Community Affairs Local Government Services Authorities
Dept of Community Affairs Local Government Services Housing Authorities
Dept of Community Affairs Local Unit Alignment Reorganization and Consolidation
Dept of Community Affairs Mainframe Access
Dept of Community Affairs Municipal Permits
Dept of Community Affairs Municipal Permits Training
Dept of Community Affairs NJ Historic Trust
Dept of Community Affairs Office of Smart Growth
Dept of Community Affairs Registration Inspection Management System
Dept of Community Affairs Shared Services
Dept of Community Affairs Sussex - Wantage Working Group
Dept of Community Affairs Taskforce on Housing
Dept of Community Affairs Technology Coordinator
Dept of Community Affairs Terminal Services
Dept of Community Affairs Uniform Construction Code Emergency Inspection Program Mutual Aid
Dept of Community Affairs Uniform Construction Code information
Dept of Community Affairs Universal Service Fund Home Energy Assistance Documents
Dept of Community Affairs Urban Enterprise Zone
Dept of Corrections Citrix
Dept of Corrections Citrix 2
Dept of Corrections Email
Dept of Corrections Mainframe Access
Dept of Corrections Mainframe Access 2
Dept of Corrections Medical
Dept of Education Business Intelligence
Dept of Education Email
Dept of Education Program Activity Review System
Dept of Education School Safety and Security Administrator
Dept of Education School Safety and Security Non-Public Schools
Dept of Education School Safety and Security Reporting
Dept of Education Terminal Services

Revised 5/14/2009
Dept of Environmental Protection Child Care Coordination
Dept of Environmental Protection Drinking Water Security Training
Dept of Environmental Protection Email
Dept of Environmental Protection Endangered and Non-game Species Program
Dept of Environmental Protection Enforcement Documents
Dept of Environmental Protection Mainframe Access
Dept of Environmental Protection Natural and Historic Resources Land Management
Dept of Environmental Protection NJEMS Citrix
Dept of Environmental Protection Passaic River Group
Dept of Environmental Protection Permit Efficiency Task Force
Dept of Environmental Protection Policies
Dept of Environmental Protection Recycling and Planning Communications
Dept of Environmental Protection RGGI Documents
Dept of Environmental Protection Stewardship
Dept of Environmental Protection Sustainability Action Group
Dept of Environmental Protection Water Supply Council
Dept of Health and Senior Services Aging and Disability Resource Connection Admin
Dept of Health and Senior Services Aging and Disability Resource Connection Editor
Dept of Health and Senior Services Animal Population Control
Dept of Health and Senior Services Area Agency on Aging
Dept of Health and Senior Services Board of Health Backup
Dept of Health and Senior Services Calendar Administrator
Dept of Health and Senior Services Calendar Editor
Dept of Health and Senior Services Cancer Resources Administrator
Dept of Health and Senior Services Care Givers
Dept of Health and Senior Services Communicable Disease Service
Dept of Health and Senior Services Division of Aging and Community Services
Dept of Health and Senior Services Email
Dept of Health and Senior Services File Storage
Dept of Health and Senior Services Flu Clinics
Dept of Health and Senior Services Forms Administrator
Dept of Health and Senior Services Health Professional
Dept of Health and Senior Services Health Professional Backup
Dept of Health and Senior Services Internal Review Board
Dept of Health and Senior Services Local Health Evaluation Report
Dept of Health and Senior Services Local information Network Communication System
Dept of Health and Senior Services Nurse Staffing Administrator
Dept of Health and Senior Services Nurse Staffing Reports
Dept of Health and Senior Services Nursing Home Licensing Board
Dept of Health and Senior Services Office of the Public Guardian
Dept of Health and Senior Services Refugee Health Tracking System
Dept of Health and Senior Services Right to Know Administrator
Dept of Health and Senior Services Right to Know Employee
Dept of Health and Senior Services Right to Know External
Dept of Health and Senior Services West Nile Virus
Dept of Human Services 1099 Adjustment
Dept of Human Services Access Control Facility Maintenance
Dept of Human Services Business Intelligence
Dept of Human Services Child Support
Dept of Human Services Division of Disability Determination Mainframe Access
Dept of Human Services Division of Youth and Family Services Change Management
Dept of Human Services Electronic Timesheets
Dept of Human Services Eligibility

Revised 5/14/2009
Dept of Human Services GLink
Dept of Human Services Mainframe Access
Dept of Human Services Medicaid
Dept of Human Services Tax Offset Program
Dept of Human Services Training Academy
Dept of Human Services TSO Mainframe Access
Dept of Labor and Workforce Development Auditor Database Access
Dept of Labor and Workforce Development Business Intelligence
Dept of Labor and Workforce Development Database Access
Dept of Labor and Workforce Development Email
Dept of Labor and Workforce Development Employee
Dept of Labor and Workforce Development GWeb
Dept of Labor and Workforce Development Mainframe Access
Dept of Labor and Workforce Development Tax Web-Enabled System
Dept of Law and Public Division of Law Repository
Dept of Law and Public Safety ACE Data Warehouse
Dept of Law and Public Safety Communication
Dept of Law and Public Safety Criminal Justice Email
Dept of Law and Public Safety Division of Consumer Affairs Email
Dept of Law and Public Safety Division of Criminal Justice Brimage
Dept of Law and Public Safety Division of Criminal Justice Domestic Violence Working Group
Dept of Law and Public Safety Division of Criminal Justice Evidence Tracking System
Dept of Law and Public Safety Division of Criminal Justice Insurance Fraud Prosecutor
Dept of Law and Public Safety Division of Criminal Justice Laboratory Information Management System
Dept of Law and Public Safety Division of Criminal Justice Megan's Law information
Dept of Law and Public Safety Division of Criminal Justice Sexual Assault Nurse Examiners
Dept of Law and Public Safety Division of Criminal Justice Victim Witness Advocacy
Dept of Law and Public Safety Division of Gaming Enforcement Email
Dept of Law and Public Safety Division of Gaming Enforcement Mainframe Access
Dept of Law and Public Safety Division of Law Email
Dept of Law and Public Safety Division of Law Intranet
Dept of Law and Public Safety Division of Law Timekeeping
Dept of Law and Public Safety Domestic Violence
Dept of Law and Public Safety Emergency Phone Service
Dept of Law and Public Safety Ethical Standards Email
Dept of Law and Public Safety Frequency Management System
Dept of Law and Public Safety General Email
Dept of Law and Public Safety Intranet
Dept of Law and Public Safety Juvenile Prosecutors
Dept of Law and Public Safety Mainframe Access
Dept of Law and Public Safety Office of State Medical Examiner
Dept of Law and Public Safety Prescription Blank Printers
Dept of Law and Public Safety Program Management Office
Dept of Military and Veterans Affairs Citrix
Dept of Personnel Classification Support System
Dept of Personnel Email
Dept of Personnel IT Mainframe Access
Dept of Personnel Local
Dept of Personnel Mainframe Access
Dept of State Division of Archives and Records Management Archives Administrator
Dept of State Division of Archives and Records Management Archives User
Dept of State Division of Archives and Records Management Member
Dept of State Email
Elections
Electronic Catalog
Electronic Catalog Development
Electronic Catalog Support
Electronic Cost Accounting and Timesheets
Electronic Cost Accounting and Timesheets Steering Committee
Electronic Payment Logs
Electronic Payment Systems Initiative
Emergency Management Coordinator
Emergency Phone Service
Emergency Phone Service Consolidation
Emergency Phone Service Instructor
Emergency Response Official
Emergency Services
Empirix Support
Employee Directory
Employee Directory Administrator
Enterprise Architecture Documents
Enterprise Vulnerability Management Group
Federal Communications Commission Region 8 Interoperability Subcommittee
Fire District Representative
Fort Monmouth Base Closing Forum
Gang Survey
Government Records Council
Governor's Communication Office
Governor's Office Email
Governor's Office Planning
GovExchange
Grants
Grants Test
Group Meeting Calendar
Hazard Advisory Group
Hazardous Materials Right-to-Know
Higher Education Mainframe Access
Higher Education Student Assistance Authority Employee
Highlands Commission Geographic Information Systems
Highlands Council
Highlands Council Email
Housing Solutions
Housing and Mortgage Finance Agency Green Homes
Human Resources Development Institute eLearning
Human Resources Development Institute eLearning Account Administrator
Human Resources Development Institute eLearning Accounts Receivable
Human Resources Information System
Identity Management
Identity Management Provisioning
Information Resources Management Council
Information Security Representative
Information Technology Transformation
Infoshare
Infrastructure Protection
Interagency Agreements
Interagency Records Legal Discovery
Intergovernmental Cooperative Purchasing
Internal Revenue Service Mainframe Access
Juvenile Justice Commission Automated Management System
Juvenile Justice Commission Citrix
Juvenile Justice Commission Detention Information System
Juvenile Justice Commission Electronic Medical Record
Juvenile Justice Commission Email
Juvenile Justice Commission Information Management System
Juvenile Justice Commission Mainframe Access
Katzenbach School Mainframe Access
Legacy File Transfer
Legislature Mainframe Access
Local Health Annual Report
Local Procurement Discussion Group
Lottery Agent
Lottery Chain Managers
Mainframe General Access
Motor Vehicle Commission Agent Operations
Motor Vehicle Commission Auditor-Investigator
Motor Vehicle Commission Business Intelligence
Motor Vehicle Commission Business User
Motor Vehicle Commission Employee
Motor Vehicle Commission Employee Menu
Motor Vehicle Commission eMVC
Motor Vehicle Commission External
Motor Vehicle Commission Field Monitor
Motor Vehicle Commission Government User
Motor Vehicle Commission IMS Manager
Motor Vehicle Commission Information Retrieval User
Motor Vehicle Commission Intranet
Motor Vehicle Commission Inventory Counting Clerk
Motor Vehicle Commission Mailroom
Motor Vehicle Commission Manager
Motor Vehicle Commission Sending-Receiving Clerk
Motor Vehicle Commission Use Manager
Motor Vehicle Website Vendor
Multiagency Business Intelligence
Municipal Clerk
Municipal Clerk File Submissions
Municipal Finance Officer
Municipal Health Officers
Municipal Tax Assessor
Municipal Tax Collector
MVC CAIR
Network Planning Administrators
Network Planning Committee
Network Service Center
New Jersey Lottery Email
New Jersey Lottery Employee
New Jersey Lottery Input
New Jersey Lottery Tester
New Jersey Network Email
Newsline
NJ Employee Self Service (Online Pay Stub)
NJ Premier E-Business Services
NJSP email
Non-Urban Area Security Initiative
Office of Administrative Law Case Management System
Office of Administrative Law Employee
Office of Administrative Law Library
Office of Child Advocate CIMIS
Office of Economic Growth Business Opportunity Administrator
Office of Economic Growth Business Opportunity Liaison
Office of Homeland Security and Preparedness Email
Office of Information Technology Application Infrastructure Applications
Office of Information Technology Application Infrastructure Technical Team
Office of Information Technology Automated Server Application Inventory
Office of Information Technology Billing Rates
Office of Information Technology Business Intelligence
Office of Information Technology Center of Excellence
Office of Information Technology Collaborative Services
Office of Information Technology Cost Allocation Recovery
Office of Information Technology Data Management Services Database Administrator
Office of Information Technology Data Management Services Term Contract Evaluation
Office of Information Technology E-Government
Office of Information Technology Email
Office of Information Technology Email Upgrade
Office of Information Technology Employee
Office of Information Technology Geographic Information Systems Terminal Services
Office of Information Technology Information Security Group
Office of Information Technology Integrated Planning
Office of Information Technology Mainframe Access
Office of Information Technology Motor Vehicle Facilities Administrator
Office of Information Technology Network Administrators
Office of Information Technology Operational Fusion
Office of Information Technology Operational Leadership
Office of Information Technology Platform Availability
Office of Information Technology Print-Forms Consolidation
Office of Information Technology Procurement Tracking
Office of Information Technology Request for Proposals Review
Office of Information Technology Security Oversight Group
Office of Information Technology Security Working Group
Office of Information Technology Senior Staff
Office of Information Technology Strategic Planning
Office of Information Technology Strategic Planning Evaluation Team
Office of Information Technology Taxation and Revenue Developers
Office of Information Technology Webtrends
Office of Legislative Services Business Intelligence
Office of Legislative Services Mainframe Access
Office of the State Auditor
Offsite Availability and Recovery
Open Public Records Act
Operation Management System
Oracle User Group
Parole Board Whats Up
Pensions Client Services
Phone Number Administrator
Pinelands Commission Email
Pinelands Commission Employee
Police Academy Directors
Police Standards Committee Email
Police Training Commission
Preparedness College
Prevention Health Education Network
Project Management Improvement Advisory Group
Public Defender Case Management
Public Defender Pool Attorney
Public Employment Relations Email
Public Employment Relations Mainframe Access
Public Key Infrastructure Pre-Registration
Publications
Rate Payer Authority Email
Redevelopment Authority Email
Regional Evacuation Plan
Resource Directory Database
Risk Management
Role Manager
Role Manager Email
Rowan University Mainframe Access
Secure File Transfer Administrator
Secure File Transfer Technician
Secure File Transfer User
Secure Motor Vehicle
Security Officer Forum
Selective Assistance Vendor Information
South Jersey Transit Authority Mainframe Access
State Auditor Mainframe Access
State Commission on Investigation Email
State Employee Intranet
State Ethics Commission Administrator
State Parole Board EGuide
State Parole Board Email
State Parole Board Netstorage
State Police ITB Mainframe Access
State Sentencing Commission
Statewide Print Consolidation Study
Statewide Radio Interoperability Project
Statewide Strategic Planning
Statewide Technology Asset Reporting and Tracking
Strategic Planning Coordinator
Task Force One Search and Rescue
Tax Software Vendor
Telephone Billing
Telephone Billing Documents
Turnpike Authority Email
Uniform Crime Reporting
USFHEA
Vendor Payment Inquiry
VPN Client Documents
Web Content Management
Web Content Management 2
Web Developers
Web Media Documents
Workforce Investment Board and One-Stop
### Appendix C - Projects Under Review of the OIT System Architecture (SAR) Review Process

<table>
<thead>
<tr>
<th>Agency</th>
<th>Affinity Group</th>
<th>Initiative</th>
<th>CSAR Held</th>
<th>LSAR Held</th>
<th>PSAR Held</th>
<th>CSAR Scheduled</th>
<th>LSAR Scheduled</th>
<th>PSAR Scheduled</th>
<th>In the Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGR</td>
<td>Business &amp; Community</td>
<td>Agriculture Crystal Rpts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGR</td>
<td>Business &amp; Community</td>
<td>Online Organic Registration</td>
<td>9/29/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Business &amp; Community</td>
<td>Sexual Assault Incident Reporting System</td>
<td>4/14/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Business &amp; Community</td>
<td>RIMS</td>
<td>12/15/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Business &amp; Community</td>
<td>APEX Budget Connection</td>
<td>1/26/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Business &amp; Community</td>
<td>Urban Enterprise Zone</td>
<td>2/2/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCF</td>
<td>Health &amp; Social Services</td>
<td>RFP for Children's System of Care</td>
<td>6/16/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEP</td>
<td>Business &amp; Community</td>
<td>Campground Registration System</td>
<td>3/17/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEP</td>
<td>Business &amp; Community</td>
<td>Migration of eNode to EE environment</td>
<td>8/28/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHI</td>
<td>Health &amp; Social Services</td>
<td>Regulatory Services Portal (4.0)</td>
<td>8/14/2008</td>
<td>1/8/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHI</td>
<td>Health &amp; Social Services</td>
<td>DOV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CSAR</td>
</tr>
<tr>
<td>DHI</td>
<td>Health &amp; Social Services</td>
<td>OMEGA-Union Dues</td>
<td>2/5/2008</td>
<td>2/14/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHISS</td>
<td>Health &amp; Social Services</td>
<td>CompuTrust</td>
<td>11/17/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHISS</td>
<td>Health &amp; Social Services</td>
<td>Food and Drug Safety Licensing</td>
<td></td>
<td>12/11/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHISS</td>
<td>Health &amp; Social Services</td>
<td>Go To Meeting</td>
<td>3/30/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHISS</td>
<td>Health &amp; Social Services</td>
<td>IBIS-PH</td>
<td>6/26/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHISS</td>
<td>Health &amp; Social Services</td>
<td>Licensing and Tracking System</td>
<td>5/19/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHISS</td>
<td>Health &amp; Social Services</td>
<td>Pandemic Influenza Awareness Program</td>
<td>8/18/2008</td>
<td>11/13/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHISS</td>
<td>Health &amp; Social Services</td>
<td>WIC</td>
<td>2/9/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMAVA</td>
<td>Public Safety</td>
<td>IIS Web Hosting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CSAR</td>
</tr>
<tr>
<td>DOE</td>
<td>Health &amp; Social Services</td>
<td>Criminal History</td>
<td>9/11/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOS</td>
<td>Administrative Services</td>
<td>State Museum Scheduling and Event Mgmt.</td>
<td>8/4/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOS</td>
<td>Administrative Services</td>
<td>Candidate Registration and HAVA inventory System</td>
<td>6/30/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOS</td>
<td>Administrative Services</td>
<td>Travel and Tourism Booking Engine RFP</td>
<td>1/12/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT</td>
<td>Business &amp; Community</td>
<td>Environmental Data Management System</td>
<td>9/25/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT</td>
<td>Business &amp; Community</td>
<td>GIS Application Toolkit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CSAR</td>
</tr>
<tr>
<td>DOT</td>
<td>Business &amp; Community</td>
<td>HMMS - Maintenance Management System</td>
<td>7/24/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT</td>
<td>Business &amp; Community</td>
<td>Outdoor Advertising (DOT, ADV)</td>
<td>5/15/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT</td>
<td>Business &amp; Community</td>
<td>SAGE</td>
<td>1/14/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT</td>
<td>Business &amp; Community</td>
<td>TELUS - Transportation Economic Land Use System</td>
<td>7/14/2008</td>
<td>11/13/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT</td>
<td>Business &amp; Community</td>
<td>Tm2Go 2009</td>
<td>3/9/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td>Not Aligned</td>
<td>SAGE</td>
<td>10/9/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td>Not Aligned</td>
<td>Ecats v 5.0</td>
<td>1/22/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gov. Office</td>
<td>Not Aligned</td>
<td>Travel Approval System</td>
<td>8/11/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWD</td>
<td>Not Aligned</td>
<td>Family Leave Insurance Web Filing</td>
<td>1/22/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWD</td>
<td>Not Aligned</td>
<td>TDI-FL1-IVR</td>
<td>3/23/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWD</td>
<td>Not Aligned</td>
<td>Temporary Disability Benefits Web Inquiry</td>
<td>1/22/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWD</td>
<td>Not Aligned</td>
<td>Web Direct Deposit</td>
<td>6/2/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWD</td>
<td>Not Aligned</td>
<td>Web Change of Address</td>
<td>6/2/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CSAR=Conceptual System Architecture Review  
LSAR= Logical System Architecture Review  
PSAR=Physical System Architecture Review
### Appendix C - Projects Under Review of the OIT System Architecture (SAR) Review Process

<table>
<thead>
<tr>
<th>Agency</th>
<th>Affinity Group</th>
<th>Initiative</th>
<th>CSAR Held</th>
<th>LSAR Held</th>
<th>PSAR Held</th>
<th>CSAR Scheduled</th>
<th>LSAR Scheduled</th>
<th>PSAR Scheduled</th>
<th>In the Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVC</td>
<td>Public Safety</td>
<td>DARTSS</td>
<td>3/10/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVC</td>
<td>Public Safety</td>
<td>EDDL</td>
<td>2/15/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVC</td>
<td>Public Safety</td>
<td>MATRIX</td>
<td>9/15/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVC</td>
<td>Public Safety</td>
<td>MVC Organ Donor</td>
<td>3/12/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PSAR</td>
</tr>
<tr>
<td>MVC</td>
<td>Public Safety</td>
<td>MVC, SAC</td>
<td>8/14/2008</td>
<td>9/25/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVC</td>
<td>Public Safety</td>
<td>MVC, VEHRKPT</td>
<td>8/14/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVC</td>
<td>Public Safety</td>
<td>Point of Sale (POS) MVC Modernization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8/29/2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NISP</td>
<td>Public Safety</td>
<td>JSR</td>
<td>12/22/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NISP</td>
<td>Public Safety</td>
<td>E-Team Consolidation</td>
<td>3/30/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAL</td>
<td>Administrative Services</td>
<td>Case Management System</td>
<td>3/2/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHSP</td>
<td>Public Safety</td>
<td>Special Needs</td>
<td>3/12/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Certified Mail Process (NJ KIDS)</td>
<td>12/18/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Data Stage Upgrade</td>
<td>CSAR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>DCA - COAH Data Mart</td>
<td>4/21/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Employee Intranet</td>
<td>2/9/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Express Server</td>
<td>4/14/2008</td>
<td>7/24/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Frequency Management System</td>
<td>4/24/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Manager File Transfer System</td>
<td>CSAR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Microsoft SQL Server Refresh</td>
<td>4/24/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>NJ GEO TOOLS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>NJ HRIS</td>
<td>4/10/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>OIT Management Integration System</td>
<td>10/20/2008</td>
<td>2/5/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Statewide Document Facility (Carroll Street)</td>
<td>LSAR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIT</td>
<td>Not Aligned</td>
<td>Telephone Billing</td>
<td>3/14/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPB</td>
<td>Public Safety</td>
<td>SPB-Offenders</td>
<td>2/28/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>BusEnd</td>
<td>9/22/2008</td>
<td>12/5/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>Check Register</td>
<td>9/25/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>COARS</td>
<td>2/14/2006</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>Data Warehouse (QDS) LMIS and SAMS systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>Development Subsidy Job Goals Accountability Tracking System (Turner Law)</td>
<td>5/15/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>IRS Link</td>
<td>4/24/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>MACSE Emptoris</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>Online Check Register</td>
<td>12/5/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>OTT Alternative Benefit Program (ABP)</td>
<td>3/27/2008</td>
<td>6/26/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>SPR Automation</td>
<td>5/22/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>State Health Info Processing (SHIPS)</td>
<td>3/19/2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>TYTR_FairHousing Non-Residential Devel. Fee</td>
<td>7/24/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td>Administrative Services</td>
<td>USPS Web Service - Pay stubs on the web</td>
<td>4/24/2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- CSAR = Conceptual System Architecture Review
- LSAR = Logical System Architecture Review
- PSAR = Physical System Architecture Review
State of New Jersey
IT Circular
Title: 130 – Information Asset Classification Control Policy

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The purpose of this policy is to provide a mechanism to ensure the proper classification of all information assets. This policy establishes the criteria for complying with federal and local regulations regarding privacy and confidentiality of information by ensuring an appropriately risk managed Information Technology infrastructure through proper classification. This policy further establishes the prioritization of confidential and personal information and/or to identify the most significant risks to the Executive Branch of New Jersey State Government’s systems. The purpose is also to ensure access to information that is processed, stored, and/or transmitted across the Executive Branch of New Jersey State Government’s systems is properly controlled. This policy further establishes requirements to ensure that all data, applications and systems are inventoried for security control purposes and to assist in fiscal, strategic and risk management planning requirements. The criteria for classification are identified in Information Asset Classification and Control Standard 08-04-S1-NJOIT. The process for classification is identified in Information Asset Classification and Control Procedures 08-04-S1-P1-NJOIT.

II. AUTHORITY

This policy is established under the authority of State of New Jersey P.L.2007.c.56.

OIT reserves the right to change or amend this circular to comply with changes in Agency policies.

III. SCOPE

This policy applies directly to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracting entities, and
others who develop and administer information systems and resources for those systems.

The scope of this policy includes the following:

- Information assets used by the Executive Branch of New Jersey State Government for external and client operations.
- Physical assets that process, store, or transmit information for the Executive Branch of New Jersey State Government.

IV. POLICY

All departments and agencies have a responsibility to protect the confidentiality, integrity, and availability of information generated, accessed, modified, transmitted, stored or used by the Executive Branch of New Jersey State Government, irrespective of the electronic or digital medium on which the information resides and regardless of format.

Accountability for all Information Assets will be maintained through an inventory management process that will align with and support fiscal, strategic and risk management planning.

The following are information asset classification and control requirements that must be implemented across Executive Branch of New Jersey State Government systems.

A. All departments and agencies must be aware of, determine classification of, and maintain an inventory of all information assets of which they are either Owners or Stewards according to the Information Asset Classification and Control standard and procedures.

B. All information and data assets shall be classified in terms of criticality, sensitivity, and potential loss impact on departments and/or agencies should that information become unavailable.

C. All physical assets shall be classified in terms of criticality and potential loss impact on departments and/or agencies should that information become unavailable. Systems will inherit a sensitivity classification based on the highest level of classification of the data that it processes or stores.

D. Classifications shall be used for security control decisions including access control and authorization, risk mitigation, application development and maintenance decisions, architectural design decisions, and fiscal and strategic planning decisions.

E. It is the responsibility of the Data Steward to classify their information assets and mark their respective media accordingly.
F. All departments and agencies physical systems used to house the information must be adequate to protect said information according to its classification.

G. Information assets and associated classifications shall be maintained by OIT in the centralized automated Application/Server Asset Inventory application. This applies to all assets currently owned or managed by OIT. During agency consolidation, all information assets shall be incorporated into this inventory. Prior to consolidation, agencies shall maintain their own asset inventory list.

V. DEFINITIONS

A. Information Assets

Information Assets are defined as all categories of electronic devices that process and/or contain digital information including but not limited to the following: databases, records, files, electronic documents, stored data, applications, and other software that is required to support business processes such as application software and system software.

B. Physical Assets

Physical assets are defined as all computing, telecommunication and other devices that process and contain digital information including but not limited to, processors, monitors, laptops, modems, hand-held wireless devices, communications equipment (routers, switches, firewalls, etc.), magnetic media (tapes and disks), and other technical equipment.

C. Data Owner

A Data Owner is the authority, individual or organization that has legal rights to the data and those rights are protected by law. The legal rights of a Data Owner include copyright and intellectual property rights as well as the rights to exploit and/or destroy the data. The rights of the Data Owner apply even when the owned data is collected by a third party and/or combined with data owned by others.

D. Data Steward

A Data Steward is the authority, individual, or organization responsible for the use of data within his/her functional areas. The Data Steward is responsible for developing decisions specifically related to the use of the data. Data Stewards follow and/or approve policies, procedures, and guidelines that pertain to the data during the lifecycle of that data entrusted to their stewardship. Data Stewards specify procedures for the access, processing, maintenance, storage, protection, and/or destruction
of data on behalf of the Data Owner. The Data Steward may also be the Data Owner.

E. Data Custodian

A Data Custodian is the authority, individual, or organization responsible for implementing Data Steward-defined requirements while protecting the rights of the Data Owner for the access, processing, maintenance, storage, protection, and/or destruction of data and electronic records. Information/Data Custodians are responsible and accountable for the management and care of the data under their control.

VI. RESPONSIBILITIES

A. Data Stewards

1. Identify the potential loss impact, criticality, and sensitivity levels of their information being processed, stored, or transmitted by information resources according to any identified prioritization schedule as defined in the procedure document.

2. Maintain timely updates and maintain a cognizance at all times of the values of the information assets within their ownership and/or stewardship.

3. Be aware of and specify, as needed the functional security requirements for the information or physical assets needed to protect those assets.

4. Approve all access and restriction requirements to their information/data and maintain current access control lists for such information/data.

5. Specify procedures for the access, processing, maintenance, storage, protection, and/or destruction of information/data.

6. Review any security reports of the processing environment provided by the Data Custodian to ensure an acceptable level of risk is established to guard against the loss of information/data confidentiality, integrity, or availability.

7. Provide classification inventory of their information and physical assets to Data Custodian as required.
8. Be cognizant of all regulatory compliance requirements for data in their stewardship and provide information about regulatory compliance to data custodians.

9. Ensure all employees and business partners understand the classification values of information assets being used and are informed of procedures for protecting and releasing that information.

B. Data Custodian

1. Maintain and update information in the enterprise Application/Server Asset Inventory.

2. Recommend and/or implement security controls that satisfy the security requirements specified by the Data Steward.

3. Ensure that the controls in place are adequate to meet the asset classification requirements.

4. Administer the Data Steward-defined access requirements to the information, software, and/or physical assets.

5. Ensure all employees and business partners understand the classification values of information assets being maintained or accessed and are informed of procedures for protecting and releasing that information.

VII. EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

Failure to comply with this policy may result in disciplinary action. A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with Policy 08-02-NJOIT (111 - Information Security Managing Exceptions).
<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>07-31-2008</td>
<td>Changed to a Statewide IT Circular</td>
</tr>
<tr>
<td>2.0</td>
<td>07-31-2008</td>
<td>Revised and Changed to a Statewide IT Circular</td>
</tr>
</tbody>
</table>

Adel Ebeid, Chief Technology Officer  
NJ Office of Information Technology
State of New Jersey
IT Circular

Title: 130-01 Information Asset Classification and Control Standard

Standard: 08-04-S1-NJOIT

DATE PUBLISHED: 07-31-08

VERSION: 2.0

EFFECTIVE DATE: IMMEDIATELY

FOR INFORMATION CONTACT:
Elizabeth Caldwell, Office of Policy and Planning
(609) 633-0429

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

This standard establishes security classification categories for both information and information systems. This standard supports the Executive Branch of New Jersey State Government’s ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individual’s information.

Note: Any Federal or State legislation, regulations or mandates to classify data in a manner that requires tighter controls than articulated in this standard shall take precedence.

The procedures for maintaining inventories of asset classification will be deferred to 08-04-S1-P1-NJOIT (130-00-01 Information Assets Classification and Control Procedures).

II. AUTHORITY

This standard is established under the authority of State of New Jersey P.L.2007.c.56 and under the authority of Policy 08-04-NJOIT – Information Assets Classification and Control.

Office of Information Technology (OIT) reserves the right to change or amend this circular to comply with changes in State standards.

III. SCOPE

This standard applies directly to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracting entities, those who develop and administer information systems and resources, and
others tasked to implement Policy 08-04-NJOIT (130 ~ Information Assets Classification and Controls).

IV. STANDARD

Security classification categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization, as well as for fiscal and strategic planning. Information assets shall be classified by the Data Steward and entered into OIT's Application/Server Asset Inventory (ASAI) database.

A. Sensitivity classification identifies information in terms of what it is and how access, processing, communications, and storage must be controlled. Information assets shall be classified in terms of sensitivity. All information stored, processed, or transmitted by information resources shall be identified by one of four levels of sensitivity: Public, Secure, Confidential, and Personal. If more than one sensitivity level could apply to the information, the highest level (most restrictive) will be selected.

1. Public – Information that is authorized for release to the public. The disclosure, unauthorized access, or unauthorized use of Public information would not adversely impact OIT, the state, and/or the public. Examples include: List of New Jersey municipalities and cabinet officials.

2. Secure – Information that is available to business units and used for official purposes but would not be released to the public unless requested. The disclosure, unauthorized access, or unauthorized use of secure information would have a limited adverse impact on OIT, the state, and/or the public. Examples include: Financial accounting information and department projects such as Department of Transportation bridge maintenance records.

3. Confidential – Information of a sensitive nature that is available only to designated personnel. The disclosure, unauthorized access, or unauthorized use of confidential information would have a significant adverse impact on OIT, the State, and/or the public. Confidential information would be undisclosable under the Open Public Records Act (OPRA). Examples include: Criminal investigation for fraud and Homeland Security planning and support.

4. Personal – All personally identifiable information pertaining to individuals that is protected by Federal or State law shall be labeled as Personal. The disclosure, unauthorized access, or unauthorized use of Personal information would have a significant adverse effect on OIT, the State, and/or the public and the individuals whose
information was disclosed. Examples include: Personal financial information, social security number, and medical conditions.

Note: Sensitivity classifications shall attach to and follow the information to which it applies until the classification is changed by the Data Steward.

B. Criticality classifies the importance of specific information to operations in terms of the impact that loss of use of the information would have on the organization. Criticality ranks the significance of the information to the organization's mission. Most often, the criticality value assists in determining recovery priorities during a disaster with the most critical systems being recovered first.

Information shall be classified by one of four criticality levels: Derived, Non-Essential, Essential, or Public Safety.

1. Derived – Information/data that is derived from other systems and is dependent upon that system and the restoration of that data. The loss of Derived data and/or its processing platforms would be minor and would not impact operations. Examples include: Data warehousing (data downstream from source) and internal reporting databases created to supply reports.

2. Non-Essential – Data that is not mission essential to the business unit and can be restored after all essential data is made available. The loss of Non-Essential data and/or its processing platforms would have a minimal impact on operations. The acceptable loss of Non-Essential information would typically be expressed in days. Examples include: Correspondence tracking systems and project management data.

3. Essential – Data that is essential to the mission of the business unit and must be restored as quickly as possible. The loss of Essential data and/or its processing platforms would adversely affect operations. The acceptable loss of Essential information would typically be expressed in hours. Examples include: Motor vehicle licensing and benefit checks.

4. Public Safety – Data to support life and property safety, which must be available at all times. The loss of Public Safety data and/or its processing platforms could be catastrophic to operations. Public Safety information is typically redundant and are the first systems to be recovered during a disaster. The acceptable loss of Public Safety information or an information resource that processes this data would typically be expressed in minutes. Examples include:
State Criminal Information Center (SCIC) data and critical infrastructure data (e.g., telecommunications, utilities, 911).

Note: If more than one criticality level could apply to the information when aggregated, the highest level (most critical) will be selected.

C. Information assets shall be classified in terms of low, moderate, or high impact of loss on each of the following: availability, integrity, and confidentiality of the assets with the higher the impact the greater the security control required. The loss classification should have some correlation to both the sensitivity and criticality levels.

1. Low Impact – Loss of availability, integrity, and confidentiality could have a limited adverse effect on organizational operations, organizational assets, or individuals. Public information is often categorized as having a low impact.

2. Moderate Impact – Loss of availability, integrity, and confidentiality could have a serious adverse effect on organizational operations, organizational assets, or individuals. Secure data would be categorized as having a limited impact.

3. High Impact – Loss of availability, integrity, and confidentiality could have a severe and/or catastrophic adverse effect on organizational operations, organizational assets, and/or individuals. Confidential and/or personal information should be categorized as having a high impact.

D. Physical assets shall inherit the highest criticality value of the information they process, store, and/or communicate. Physical assets must not contribute to the degradation of the classification of the information. Wherever and whenever practicable, information assets shall be segregated according to like classification.

E. Classifications shall be used for security control decisions, risk management, fiscal, and strategic planning as well as to aid in application and system development and implementation.

Sensitivity and impact values shall be used to establish data protection requirements. (e.g., information classified as Confidential would require more security controls than information classified as Public.) Only those security controls that fulfill the defined protection requirements and are acknowledged as providing an acceptable level of risk will be implemented.
Criticality values shall be used to ensure that platform/application specifications and implemented controls are sufficient to meet the availability requirements of the asset.

Classification values (potential loss impact, sensitivity, and criticality) shall be an input to:

- Authentication and authorization decision makers to ensure appropriate access control is established and maintained for all users and systems are provisioned and deprovisioned in an accountable fashion.

- Developers, in support of the New Jersey Data Management Framework and Common Data Architecture.

- Disaster Recovery/Business Continuity planners to ensure recovery priorities are appropriate.

- Fiscal Planning to provide decision making input support of the yearly Appropriations act as it relates to IT purchasing.

- Strategic Planning and Development.

V. DEFINITIONS

A. Confidentiality—A measure of the ability of the system to protect its data and the means of preserving authorized restrictions from access and disclosure. A loss of confidentiality is the unauthorized disclosure of information.

B. Integrity—The assurance that data is consistent and correct. A loss of integrity is the unauthorized modification or destruction of information.

C. Availability—The assurance of timely and reliable access to and use of information. A loss of availability is the disruption of access to information or an information system.

VI. RESPONSIBILITIES

All responsibilities shall be delegated as stated in 08-04-NJOIT (130 – Information Assets Classification and Controls).

VII. EXCEPTIONS AND NON-COMPLIANCE
Departments and Agencies shall comply with this standard within 90 days of its effective date.

Failure to comply with this standard may result in disciplinary action. A compliance exception must be requested if there is an inability to comply with this standard because of a business reason or system constraint. Exceptions and non-compliance with this standard shall be managed in accordance with Policy 08-02-NJOIT (111 – Information Security Managing Exceptions).

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>07-31-2008</td>
<td>Changed to a Statewide IT Circular</td>
</tr>
<tr>
<td>2.0</td>
<td>07-31-2008</td>
<td>Revised and Changed to a Statewide IT Circular</td>
</tr>
</tbody>
</table>

Adel Ebeid, Chief Technology Officer
NJ Office of Information Technology
State of New Jersey
IT Circular

Title: 130-00-01 – Information Assets Classification and Control Procedure

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

This procedure establishes a statewide classification method to be used when inventorying all information assets and establishes the use of Application Server Asset Inventory (ASAI) as the repository.

II. AUTHORITY

This procedure is established under the authority of State of New Jersey P.L.2007.C.56 and Policy 08-04-NJOIT (130 – Information Assets Classification and Control).

OIT reserves the right to change or amend this circular to comply with changes in OIT or other agency policies.

III. SCOPE

This procedure applies to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracted entities, and others who are authorized to access enterprise information resources.

IV. PROCEDURE

The asset classification information will be collected and maintained in the following manner:

A. The Statewide Office of Information Security (SOIS) will provide each agency with an inventory spreadsheet (Attachment A) to use for the collection of the required asset classification information.
B. As the Data Steward, each agency must develop a mechanism for classifying their data and populating the inventory spreadsheet and must ensure that the asset classification information is updated through a recurring review process. Agencies must complete the provided spreadsheet (Attachment A) within 120 days of notification and submit it to SOIS.

C. SOIS will maintain a comprehensive list of all information asset classifications, which includes all Executive Branch agencies. The compiled list will be used to populate the ASAI as applicable.

D. Any system in the planning and development stages must include detailed classification information for all information assets. This information will be required and included in the System Architecture Review (SAR) process and will be added to the ASAI.

E. At the time of consolidation agencies shall provide an asset inventory list, which will be added to the ASAI in a manner that will be defined by the consolidation process.

F. All exceptions must be requested within 90 days of notification.

V. RESPONSIBILITIES

All responsibilities shall be delegated as acknowledged in policy 08-04-NJOIT (130 – Information and Physical Assets Classification and Controls).

VI. EXCEPTIONS AND NON-COMPLIANCE

A compliance exception must be requested if there is an inability to comply with this procedure because of a business reason or system constraint. Exceptions and non-compliance with this procedure shall be managed in accordance with Policy 08-02-NJOIT (111 – Information Security Managing Exceptions).

Adel Ebeid, Chief Technology Officer
NJ Office of Information Technology
<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>08-22-2008</td>
<td>Revised and Changed to a Statewide IT Circular</td>
</tr>
</tbody>
</table>
State of New Jersey
IT Circular

Title: 203 – Information Security Payment Card Industry (PCI) Data Security Policy

ATTN: Directors of Administration and Agency IT Directors

I. PURPOSE

The purpose of this policy is to safeguard sensitive credit card data and to achieve compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.1. This policy establishes technical and non-technical security controls to be employed on systems used for the purpose of conducting credit card transactions. The following are the specific names of the Payment Card Industry programs:

MasterCard's Site Data Protection (SDP)
Visa's Cardholder Information Security Program (CISP)
American Express Data Security Operating Polices (DSOP)
Discover Information Security Compliance (DISC)

II. AUTHORITY

This policy is established under the authority of Policy 06-2004 – Information Security Program.

OIT reserves the right to change or amend this circular to comply with changes in OIT or other agency policies.

III. SCOPE

This policy applies to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracting entities, and others who store, process, or transmit credit cardholder data.
IV. POLICY

The current Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.1 is comprised of twelve requirements organized in six logically related groups designed to enhance payment account data security. In order to achieve compliance with these requirements, all departments and agencies have the responsibility of securing the confidentiality of credit card information transmitted, stored, or used by the State of New Jersey.

Policy requirements are as follows:

Build and Maintain a Secure Network

A. Install and maintain a firewall configuration to protect cardholder data

1. Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

2. All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

B. Do not use vendor-supplied defaults for system passwords and other security parameters

1. Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

Protect Cardholder Data

A. Protect stored cardholder data

1. Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating
cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

B. Encrypt transmission of cardholder data across open, public networks
   1. Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

Maintain a Vulnerability Management Program

A. Use and regularly update anti-virus software or programs
   1. Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

B. Develop and maintain secure systems and applications
   1. Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and security coding techniques.

Implement Strong Access Control Measures

A. Restrict access to cardholder data by business need-to-know
   1. This requirement ensures critical data can only be accessed by authorized personnel.

B. Assign a unique ID to each person with computer access
   1. Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

C. Restrict physical access to cardholder data
1. Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

Monitor and Test Networks

A. Track and monitor all access to network resources and cardholder data

1. Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

B. Regularly test security systems and processes

1. Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

Maintain an Information Security Policy Program

A. Maintain a policy program that addresses information security for employees and contractors

1. A strong security policy program sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

V. EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

Failure to comply with this standard may result in disciplinary action. Requests for exceptions for non-compliance with this policy shall be processed in accordance with Policy 08-02-NJOIT (111 - Information Security Managing Exceptions).

Adel Ebeid
Chief Technology Officer

203 Information Security Payment Card Industry (PCI)
Data Security Policy
ATTN: Directors of Administration and Agency IT Directors

I. PURPOSE

The purpose of this standard is to safeguard sensitive credit card data and to achieve compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.1. This standard establishes technical and non-technical security controls to be employed on systems used for the purpose of conducting credit card transactions. The following are the specific names of the Payment Card Industry programs:

- MasterCard’s Site Data Protection (SDP)
- Visa’s Cardholder Information Security Program (CISP)
- American Express Data Security Operating Policies (DSOP)
- Discover Information Security Compliance (DISC)

II. AUTHORITY

This standard is established under the authority of Policy 06-2004 Information Security Program.

OIT reserves the right to change or amend this circular to comply with changes in OIT or other agency standards.

III. SCOPE

This standard applies to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracting entities, and others who store, process, or transmit credit cardholder data.
IV. STANDARD

Compliance with PCI Data Security Standard Version 1.1 is required of all merchants and service providers that store, process, or transmit credit cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. The confidentiality of credit card information must be responsibly secured during transmission and storage when in use by State of New Jersey departments and agencies.

To achieve compliance set forth in the PCI DSS Version 1.1, the following applies as a standard:

1. **Build and Maintain a Secure Network.**

   1.1 Establish a firewall configuration that includes:

   1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration.

   1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks.

   1.1.3 Requirements for a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and the Intranet.

   1.1.4 Description of groups, roles, and responsibilities for logical management of network components.

   1.1.5 Documented list of services/ports necessary for business.

   1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN).

   1.1.7 Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented.

   1.1.8 Annual review of firewall/router rule sets.

   1.1.9 Configuration standards for routers.

   1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment:

   1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:

   1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters)
1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ.
1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (only "established" connections are allowed into the network).
1.3.4 Placing the database in an internal network zone, segregated from the DMZ.
1.3.5 Restricting outbound traffic to that which is necessary for the payment card data environment.
1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted), should have the same, secure configuration.
1.3.7 Denying all other inbound and outbound traffic not specifically allowed.
1.3.8 Installing perimeter firewalls between any wireless networks and the payment card data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes).
1.3.9 Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization's network.

1.4 Prohibit direct public access between external networks and any system component that stores cardholder information (e.g., databases, logs, trace files).

1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic.

1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.

1.5 Implement Internet Protocol (IP) masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as Port Address Translation (PAT) or Network Address Translation (NAT).

2. **System passwords and other security parameters.**

2.1 Always change the vendor-supplied defaults before you install a system on the network (e.g., passwords, SNMP community strings, and elimination of unnecessary accounts).
2.1.1 For wireless environments attached to cardholder data or transmitting cardholder data, change wireless vendor defaults, including but not limited to, default service set identifier (SSID), passwords, and SNMP community strings. Enable WIFI Protected Access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry best-accepted system hardening standards as defined by System Administration Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

2.2.1 Implement only one primary function per server (e.g., web servers, database servers, and DNS should be implemented on separate servers).

2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).

2.2.3 Configure system security parameters to prevent misuse.

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."

3. Protect Cardholder Data.

3.1 Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

3.2 Do not store sensitive authentication data subsequent to authorization (not even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 2.1 through 2.3:
3.2.1 Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.).

3.2.2 Do not store the card-validation code (Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data)) used to verify card-not-present transactions.

3.2.3 Do not store the Personal Identification Number (PIN) or the encrypted PIN block.

3.3 Mask Primary Account Numbers (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed).

*Note that this does not apply to those employees and other parties with a specific need to see full credit card numbers.*

3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data or portable digital media, backup media, in logs and data received from or stored by wireless networks) by using any of the following approaches:

- Strong one-way hashes (hashed indexes)
- Truncation
- Index tokens and PADs, (pads must be securely stored).
- Strong cryptography with associated key management processes and procedures.

*The MINIMUM account information that must be rendered unreadable is the PAN. If for some reason, a company/agency is unable to encrypt cardholder data, refer to Appendix B: "Compensation Controls for Encryption of Stored Data."

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (e.g. by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

3.5 Protect encryption keys against both disclosure and misuse.

3.5.1 Restrict access to keys to the fewest number of custodians necessary.

3.5.2 Store keys securely in the fewest possible locations and forms.
3.6 Fully document and implement all key management processes and procedures, including:

3.6.1 Generation of strong keys.
3.6.2 Secure key distribution.
3.6.3 Secure key storage.
3.6.4 Periodic changing of keys.
   - As deemed necessary and recommended by the associated application (e.g. re-keying) preferably automatically
   - At least annually.

3.6.5 Destruction of old keys.
3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).
3.6.7 Prevention of unauthorized substitution of keys.
3.6.8 Replacement of known or suspected compromised keys.
3.6.9 Revocation of old or invalid keys (mainly for RSA keys)
3.6.10 Requirement for key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.

4. **Encrypt transmission of cardholder and sensitive information across public networks.**

4.1 Use strong cryptography and security protocols such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and, and Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over open public networks.

4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on Wired Equivalent Privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

   - Used with a minimum 104-bit encryption key and 24 bit-initialization value.
   - Use ONLY on conjunction with WiFi protected access (WPA or WPA2) technology, VPN or SSL/TLS
   - Rotate shared WEP keys quarterly (or automatically of the technology permits)
• Rotate shared WEP keys whenever there are changes in personnel with access to keys
• Restrict access based on media access code (MAC) address.

Note: New implementations of WEP are not allowed after March 31, 2009. Current implementations must discontinue use of WEP after June 30, 2010

4.2 Never send unencrypted PANs by e-mail.

5. Maintain a Vulnerability Management Program.

5.1 Deploy anti-virus software on all operating systems.

Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all forms of malicious software, including spyware and adware.

5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

6. Develop and maintain secure systems and applications.

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

6.2 Establish a process to identify newly discovered security vulnerabilities (e.g. subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.

6.3 Develop software applications based on industry best practices and include information security throughout the software development life cycle.

6.3.1 Testing of all security patches and system software configuration changes before deployment.
6.3.2 Separate development, test, and production environments.
6.3.3 Separation of duties between development, test, and production environments.
6.3.4 Production data (live PANs) are not used for testing or development.
6.3.5 Removal of test data and accounts before production systems become active.
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.

6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:
6.4.1 Documentation of impact.
6.4.2 Management sign-off by appropriate parties.
6.4.3 Testing of operational functionality.
6.4.4 Back-out procedures.

6.5 Develop all web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:
6.5.1 Unvalidated input.
6.5.2 Broken access control (e.g., malicious use of user IDs).
6.5.3 Broken authentication and session management (use of account credentials and session cookies).
6.5.4 Cross-site scripting (XSS) attacks.
6.5.5 Buffer overflows.
6.5.6 Injection flaws (e.g., structured query language (SQL) injection)
6.5.7 Improper error handling.
6.5.8 Insecure storage.
6.5.9 Denial of service.
6.5.10 Insecure configuration management.

6.6 All web-facing applications must be protected against known attacks by applying either of the following methods:
- All application code must be reviewed for common vulnerabilities via manual or automated vulnerabilities assessment tools or methods.

7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

8. Assign a unique ID to each person with computer access.

8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.

8.2 In addition to assigning a unique ID, employ at least one of the methods to authenticate all users:

- Password
- Token devices (e.g., SecureID, certificates, or public key)
- Biometrics

8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

8.4 Encrypt all passwords during transmission and storage on all system components.

8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components:

8.5.1 Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

8.5.2 Verify user identity before performing password resets.

8.5.3 Set first-time passwords to a unique value for each user and change immediately after first use.
8.5.4 Immediately revoke accesses of terminated users.
8.5.5 Remove inactive user accounts at least every 90 days.
8.5.6 Enable accounts used by vendors for remote maintenance only during the time needed.
8.5.7 Communicate password procedures and policies to all users who have access to cardholder information.
8.5.8 Do not use group, shared or generic accounts and passwords.
8.5.9 Change user passwords at least every 90 days.
8.5.10 Require a minimum password length of at least seven characters.
8.5.11 Use passwords containing both numeric and alphabetic characters.
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID.
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.
8.5.16 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.

9. **Restrict physical access to cardholder data.**

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

9.1.1 Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

9.1.2 Restrict physical access to publicly accessible network jacks.

9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.

9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.
"Employee” refers to full-time and part-time employees, temporary employees/personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

9.3 Make sure all visitors are handled as follows:

9.3.1 Authorized before entering areas where cardholder data is processed or maintained.

9.3.2 Given a physical token (e.g., badge or access device) that expires, and that identifies them as non-employees.

9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.

9.4 Use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.

9.5 Store media back-ups in a secure location preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.

9.6 Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.

9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information including the following:

9.7.1 Classify the media so it can be identified as confidential.

9.7.2 Send the media via secured courier or a delivery method that can be accurately tracked.

9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).

9.9 Maintain strict control over the storage and accessibility of media that contains cardholder information:

9.9.1 Properly inventory all media and make sure it is securely stored.
9.10 Destroy media containing cardholder information when it is no longer needed for business or legal reasons as follows:

9.10.1 Crosscut shred, incinerate, or pulp hard copy materials

9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

10. **Monitor and Test Networks**

10.1 Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.

10.2 Implement automated audit trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data.
10.2.2 All actions taken by any individual with root or administrative privileges.
10.2.3 Access to all audit trails.
10.2.4 Invalid logical access attempts.
10.2.5 Use of identification and authentication mechanisms.
10.2.6 Initialization of the audit logs.
10.2.7 Creation and deletion of system-level objects.

10.3 Record at least the following audit trail entries for all system components for each event:

10.3.1 User identification.
10.3.2 Type of event.
10.3.3 Date and time.
10.3.4 Success or failure indication.
10.3.5 Origination of event.
10.3.6 Identify or name of affected data, system components, or resource.

10.4 Synchronize all critical system clocks and times.

10.5 Secure audit trails so they cannot be altered.

10.5.1 Limit viewing of audit trails to those with a job-related need.
10.5.2 Protect audit trail files from unauthorized modifications.
10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.
10.5.5 Use file integrity monitoring/change detection software on logs to ensure that existing log data cannot be changed
without generating alerts (although new data being added should not cause an alert).

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example RADIUS).

Note: Log harvesting, parsing, and alerting tool may be used to achieve compliance with Requirement 10.6.

10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulation.

An audit history usually covers a period of at least one year, with a minimum of 3 months available online.

11. Regularly test security systems and processes.

11.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts. Where wireless technology is deployed, use a wireless analyzer periodically to identify all wireless devices in use.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Note: A scan vendor qualified by the payment card industry must perform quarterly external vulnerability scans.

11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, sub-network added to environments, or a web server added to environment). These penetration tests must include the following:

10.3.1 Network-layer penetration tests
10.3.2 Application-layer penetration test

11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modifications of critical system or content files; and configure the software to perform critical file comparisons at least weekly.

Critical files are not necessarily those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operation system. Other critical files, such as those for custom applications, must be evaluated and defined by the merchant or service provider.


12.1 Establish, publish, maintain, and disseminate a security policy program that:

12.1.1 Addresses all requirements in this specification.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.
12.1.3 Includes a review at least once a year and updates when the environment changes.

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (e.g., user account maintenance procedures, log review procedures).

12.3 Develop usage policies for critical employee-facing technologies, such as remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops, and personal data assistants, to define proper use of these technologies for all employees and contractors. Ensure these usage policies require:

12.3.1 Explicit management approval.
12.3.2 Authentication for use of the technology.
12.3.3 A list of all such devices and personnel with access.
12.3.4 Labeling of devices with owner, contact information, and purpose.
12.3.5 Acceptable uses of the technology.
12.3.6 Acceptable network locations for these technologies.
12.3.7 A list of company-approved products.
12.3.8 Automatic disconnect of modem sessions after a specific period of inactivity.
12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.
12.3.10 When accessing cardholder data remotely via mode, disable storage of cardholder data onto local hard drives, floppy disks or other external media. Also, disable cut-and-paste and print functions during remote access.

12.4 Ensure the security policy program and associated standards and procedures clearly define information security responsibilities for all employees and contractors.

12.5 Assign to an individual or team the following information security management responsibilities:

12.5.1 Establish, document, and distribute security policies and procedures.
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
12.5.4 Administer user accounts, including additions, deletions, and modifications.
12.5.5 Monitor and control all access to data.

12.6 Make all employees aware of the importance of cardholder information security.

12.6.1 Educate employees upon hire and at least annually (e.g., through posters, letters, memos, meetings and promotions).
12.6.2 Require employees to acknowledge in writing they have read and understood the company’s security policy and procedures.

12.7 Screen potential employees to minimize the risk of attacks from internal sources.

For those employees who only have access to one card number at a time to facilitate a transaction, such as store cashiers, this requirement is a recommendation only.

12.8 If cardholder data is shared with service providers, then contractually the following is required:

12.8.1 Service provider must adhere to the PCI DSS requirements.
12.8.2 Agreement that includes and acknowledgement that the service provider is responsible for security of cardholder data the provider possesses.

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create an incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (e.g., informing Acquirers and credit card associations).

12.9.2 Test the plan at least annually.

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.

12.9.4 Provide appropriate training to staff with security breach response responsibilities.

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

12.9.6 Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

12.10.1 Maintain a list of connected entities
12.10.2 Ensure proper due diligence is conducted prior to connecting an entity
12.10.3 Ensure the entity is PCI DSS compliant
12.10.4 Connect and disconnect entities by following an established process.

V. EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this standard within 90 days of its effective date.

Failure to comply with this standard may result in disciplinary action. Requests for exceptions for non-compliance with this standard shall be processed in accordance with OIT Policy 08-02-NJOIT (111 - Information Security Managing Exceptions).
State of New Jersey
IT Circular

Title: 100 Information Security Program

NO: 08-01-NJOIT
SUPERCEDES: n/a

DATE PUBLISHED: 06-18-2008

VERSION: 1.0
EFFECTIVE DATE: IMMEDIATELY

FOR INFORMATION CONTACT:
Elizabeth Caldwell, Office of Policy and Planning
(609) 633-0429

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The State of New Jersey is committed to protecting the information assets and resources of the state and its constituency. All State agencies have a responsibility of due diligence and due care to that commitment. The State of New Jersey P.L.2007.c.56 establishes Office of Information Technology (OIT) as the central authority for the state’s information technology infrastructure. Under that authority and in support of the commitment to protect information assets and resources, OIT maintains oversight for developing an Information Security Program to ensure the availability, integrity, and protect the confidentiality of those information assets and resources within the Executive Branch of State Government.

The primary objectives of this Information Security Program are to:

- Effectively manage risks associated with exposure or compromise of agency information assets.
- Define and communicate responsibilities for performing information security duties.
- Ensure the implementation of security controls, both technical and non-technical, across the enterprise.
- Provide a framework for statewide security compliance efforts.
- Increase the awareness and importance of information security in all state agencies.
II. SCOPE

This policy applies to all personnel including employees, temporary workers, volunteers, contractors, and those employed by contracted entities, and others who administer state information resources.

III. POLICY

This policy establishes that the Statewide Information Security Officer (SISO) and the Statewide Office of Information Security are responsible for directing the Information Security Program and providing leadership and coordination of information security programs and services across the enterprise. This policy also establishes the responsibilities of Agencies in securing information assets and resources.

The Information Security Program will establish and ensure that:

- Physical, technical, and administrative information security controls are implemented and maintained to protect the confidentiality, integrity, and availability of information and information resources within the state.

- Statewide information security policies, standards, procedures, and any associated guidelines are developed, maintained and promulgated across the enterprise.

- Legal, regulatory, and contractual requirements will be met in support of managing and protecting statewide information assets and resources.

- Information Security awareness and training will be provided to all.

- All employees will be held accountable for fulfilling their individual information Security responsibilities.

IV. RESPONSIBILITIES

A. Chief Technology Officer

The CTO has ultimate authority and oversight for the approval, interpretation, implementation, and enforcement of all Information Security Program specifics.

B. Statewide Information Security Officer

The SISO is responsible for the development and coordination of the Statewide Information Security Program and performs the following duties:

- Administer the program and periodically assesses whether the program is implemented effectively
• Develop and implement Security Policies, Standards and Procedures

• Review requested exceptions to Security Policies, Standards and Procedures

• Provide solutions, guidance and expertise in IT security

• Maintain awareness of security status of IT systems

• Communicate requirements of Information Security Policies and legislative mandates

• Implement Security Awareness program

• Respond to security incidents

C. Agencies

Each Agency has ultimate responsibility for the protection of its information from disclosure, loss or misuse. As such, each agency must maintain thorough knowledge of these assets and understand and manage risks associated with the use of these assets. Agencies must adhere to all information security policies and program functions. Each agency shall designate an information security point of contact(s) to address program needs, participate in enterprise information security matters as well as interact with SISO as needed. Agencies shall immediately notify SISO of any information security issues requiring attention.

VI. EXCEPTIONS AND NON-COMPLIANCE

Failure to comply with this policy may result in disciplinary action.

A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with Statewide IT Circular 08-02-NJOIT (111 – Information Security Managing Exceptions).
<table>
<thead>
<tr>
<th>Department/Agency</th>
<th>FY 2007 #</th>
<th>Amount</th>
<th>FY 2008 #</th>
<th>Amount</th>
<th>FY 2009 #</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>36</td>
<td>315,346.03</td>
<td>22</td>
<td>299,106.67</td>
<td>21</td>
<td>1,051,635.40</td>
</tr>
<tr>
<td>Banking &amp; Insurance</td>
<td>22</td>
<td>704,311.32</td>
<td>19</td>
<td>684,211.32</td>
<td>13</td>
<td>358,141.97</td>
</tr>
<tr>
<td>Board Of Public Utilities</td>
<td>2</td>
<td>5,078.43</td>
<td>2</td>
<td>5,078.43</td>
<td>1</td>
<td>10,023.00</td>
</tr>
<tr>
<td>Casino Control Commission</td>
<td>32</td>
<td>872,011.17</td>
<td>29</td>
<td>786,631.08</td>
<td>15</td>
<td>520,440.11</td>
</tr>
<tr>
<td>Children And Families</td>
<td>49</td>
<td>3,642,033.14</td>
<td>45</td>
<td>3,466,835.20</td>
<td>19</td>
<td>14,253,620.67</td>
</tr>
<tr>
<td>College of New Jersey</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>3</td>
<td>30,830.43</td>
</tr>
<tr>
<td>Commerce &amp; Economic Growth</td>
<td>5</td>
<td>81,973.58</td>
<td>5</td>
<td>81,973.58</td>
<td>7</td>
<td>187,703.29</td>
</tr>
<tr>
<td>Community Affairs</td>
<td>44</td>
<td>1,535,002.88</td>
<td>42</td>
<td>1,531,225.92</td>
<td>36</td>
<td>636,912.96</td>
</tr>
<tr>
<td>Corrections</td>
<td>77</td>
<td>1,879,226.42</td>
<td>69</td>
<td>1,734,995.61</td>
<td>131</td>
<td>2,785,609.37</td>
</tr>
<tr>
<td>Education</td>
<td>45</td>
<td>1,662,969.74</td>
<td>38</td>
<td>1,589,476.09</td>
<td>40</td>
<td>2,345,184.36</td>
</tr>
<tr>
<td>Environmental Protection</td>
<td>58</td>
<td>1,496,715.83</td>
<td>56</td>
<td>1,487,193.72</td>
<td>149</td>
<td>4,060,494.49</td>
</tr>
<tr>
<td>Health &amp; Senior Services</td>
<td>152</td>
<td>2,968,008.19</td>
<td>142</td>
<td>2,631,436.56</td>
<td>160</td>
<td>11,292,469.87</td>
</tr>
<tr>
<td>Higher Education</td>
<td>6</td>
<td>36,641.98</td>
<td>2</td>
<td>16,181.04</td>
<td>1</td>
<td>6,744.00</td>
</tr>
<tr>
<td>Human Services</td>
<td>220</td>
<td>17,923,121.61</td>
<td>206</td>
<td>17,361,017.65</td>
<td>216</td>
<td>29,164,953.75</td>
</tr>
<tr>
<td>Labor</td>
<td>108</td>
<td>8,896,122.38</td>
<td>104</td>
<td>8,262,448.64</td>
<td>111</td>
<td>22,564,458.38</td>
</tr>
<tr>
<td>Law &amp; Public Safety</td>
<td>361</td>
<td>32,274,513.61</td>
<td>344</td>
<td>29,563,707.16</td>
<td>382</td>
<td>36,554,039.13</td>
</tr>
<tr>
<td>Military &amp; Veterans Affairs</td>
<td>29</td>
<td>713,663.61</td>
<td>26</td>
<td>669,312.11</td>
<td>39</td>
<td>985,130.00</td>
</tr>
<tr>
<td>Motor Vehicle Commission</td>
<td>124</td>
<td>14,121,504.24</td>
<td>95</td>
<td>11,016,448.56</td>
<td>117</td>
<td>21,390,862.18</td>
</tr>
<tr>
<td>New Jersey Highlands Council</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>New Jersey Housing And Mortgage</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Finance Agency</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>NJ Public Broadcasting Authority</td>
<td>5</td>
<td>294,985.05</td>
<td>5</td>
<td>294,985.05</td>
<td>11</td>
<td>664,571.19</td>
</tr>
<tr>
<td>NJ State Parole Board</td>
<td>11</td>
<td>322,967.33</td>
<td>10</td>
<td>281,372.46</td>
<td>32</td>
<td>718,101.49</td>
</tr>
<tr>
<td>Office Of Homeland Security</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Office Of The Governor</td>
<td>1</td>
<td>27,100.00</td>
<td>1</td>
<td>27,100.00</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Personnel</td>
<td>17</td>
<td>838,873.39</td>
<td>12</td>
<td>609,231.91</td>
<td>27</td>
<td>5,730,664.83</td>
</tr>
<tr>
<td>Public Advocate</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Public Employment</td>
<td>1</td>
<td>6,464.22</td>
<td>1</td>
<td>6,464.22</td>
<td>3</td>
<td>33,819.22</td>
</tr>
<tr>
<td>State</td>
<td>11</td>
<td>136,586.98</td>
<td>10</td>
<td>132,852.34</td>
<td>17</td>
<td>451,312.61</td>
</tr>
<tr>
<td>State Commission Of Investigation</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>1</td>
<td>25,568.50</td>
</tr>
<tr>
<td>Transportation</td>
<td>69</td>
<td>6,654,133.42</td>
<td>66</td>
<td>6,572,363.42</td>
<td>90</td>
<td>6,880,523.19</td>
</tr>
<tr>
<td>Treasury</td>
<td>263</td>
<td>11,904,097.12</td>
<td>234</td>
<td>9,943,183.35</td>
<td>220</td>
<td>14,075,404.55</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>1,748</strong></td>
<td><strong>109,313,451.67</strong></td>
<td><strong>1,585</strong></td>
<td><strong>99,054,828.09</strong></td>
<td><strong>1,933</strong></td>
<td><strong>176,779,218.94</strong></td>
</tr>
</tbody>
</table>
Information – Centralized Payroll System

What is the cost of operating the centralized payroll system? How much could be saved if the system was to be converted to a paperless system. How much would the State save, if it no longer mailed out checks and used direct deposit instead, and if pay stubs were available online only. Please break out the system’s costs and savings by personnel, printing, mailing and direct deposit costs.

Response

OIT system operation costs to support the State’s centralized payroll system is approximately $2.1M a year. Additional supports costs would exist within Treasury OMB as well as agencies concerning its daily administration. There is currently an effort underway that would substantially automated many of the manual processes with the implementation of E-Cats (Cost Allocation and Time Reporting system). This system has been implemented in 9 agencies (DEP, DOT, MVC, DOA, DOH, LWD, CSC, DCF, DOE (scheduled May 2009)) to date and will continue a target of phased in implementation over the next 18 months to complete all executive branch agencies including in but not of’s. Statistics on overall state check printing by category are attached on page 2 as well as the percentage currently performed electronically. Opportunities exist for migrating other categories of printed checks such as Unemployment, Pension and tax rebates. Regarding payroll check printing specifically, efforts have been made to date to encourage employees to sign up for direct deposit and receiving pay check stubs on the web. Currently this program is strictly voluntary and despite efforts by OMB and agencies to encourage enrollment, progress has been slow. A cost summary is presented on page 3 which outlines the OIT related costs exclusive of agency related costs for administration of check distribution. OIT related costs for salary, materials, and equipment are outlined on page 3 which are estimated at 26 cents per check. Assuming success in mandating direct deposit and pay stubs on the web, OIT chargeback savings to agencies would be at least $343,604 annually.
# EFT and Stubs on the Web

## Number of Payments, Method, and Frequency

<table>
<thead>
<tr>
<th>Program</th>
<th>Daily</th>
<th>Weekly</th>
<th>Bi-weekly</th>
<th>Monthly</th>
<th>Other (qt/annual)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Services (see note 1)</td>
<td>1,100</td>
<td>22,200</td>
<td>2,750</td>
<td>18,250</td>
<td>248,000</td>
</tr>
<tr>
<td>Labor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unemployment Benefits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temporary Disability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pensions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retirees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (see note 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payroll</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regular payroll</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplemental</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tax Rebate Checks (2008)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non senior homeowners</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior homeowners</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenant (homestead)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Income Tax Refunds (2008)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>1,100</td>
<td>22,200</td>
<td>207,885</td>
<td>63,128</td>
<td>50,829</td>
</tr>
<tr>
<td>% Electronic</td>
<td>95%</td>
<td>23%</td>
<td>56%</td>
<td>85%</td>
<td>33%</td>
</tr>
</tbody>
</table>

Note 1 - Social Services include programs such as Family and General Assistance, Food Stamps, Child Support, REACH, USF HEA, Credit to Utilities, etc

Note 2 - Various programs under the pension system such as death benefits, loans, employer overage payments, etc

EBT - Electronic Benefit Transfer
DD - Direct Deposit
DC - Debt Card
Cost Summary (OIT related costs exclusive of Agency)

The following represents OIT’s cost of check creation, printing, and distribution. It does not represent the cost that individual agencies may incur for back office processes, customer support, problem resolution, etc.

**OIT production output cost center ($3,900,000)**
- Salary $1,800,000
- Materials & Supplies $2,100,000

**Average number of checks generated by OIT (based on 2008 data)**
- Annually – 14,971,512

**OIT cost to produce each check ($.26/check)**
- Salary portion $.12
- Materials & Supplies $.14

**Postage (pre-sort bulk rate)** $0.34 per/check