SEARCH
The National Consortium for Justice Information and Statistics
7311 Greenhaven Drive, Suite 145 • Sacramento, California 95831
(916) 392-2550 • fax: (916) 392-8440 • www.search.org

Technical Assistance Report

Ohio Department of Public Safety

Information Technology Assessment: Making More Efficient Use of IT Resources

Site Visit: January 5–8, 2010

Report Submitted: February 12, 2010

Project Team: Scott Came
Michael Jacobson
Alecia Webb-Edgington (Emergency Management SME, report review)

Contents

I. Executive Summary **1**

Summary of Findings 2

Summary of Recommendations 4

II. Introduction and Request for Assistance **6**

III. Background **7**

Ohio Department of Public Safety 7

ODPS History and IT Environment 8

IV. Observations and Analysis **11**

— *Strengths of ODPS IT Staff* *11*
— *Technology Direction* *12*
— *Informal IT Governance* *12*
— *Communications and Trust* *14*
— *Level of IT Resources* *15*
— *Network Administration Challenges* *16*
— *Unnecessary Redundancy* *16*
— *Staffing Ratios and Redundant Positions* *20*
— *Inconsistency of Core IT Support Functions* *22*

V. Recommendations **27**

— *Recommendation 1: Consolidate ODPS IT under ITO* *27*
— *Recommendation 2: Capitalize on Efficiency Opportunities* *29*
— *Recommendation 3: Consolidate Network Management under ITO* *30*
— *Recommendation 4: Manage Organizational Change* *32*
— *Recommendation 5: Reorganize ITO and Emphasize Strategy and Policy* *33*
— *Recommendation 6: Formalize IT Governance* *35*
— *Recommendation 7: Formalize Service Levels* *36*
— *Recommendation 8: Manage Performance and Accountability* *37*
— *Recommendation 9: Continue Effective Practices and Efficiency Improvements* *40*
— *Recommendation 10: Develop and Maintain a Service Catalog* *40*

VI. Conclusion **42**

Appendix A: About SEARCH, the National Technical Assistance Program, and the Project Team **43**

Appendix B: ODPS Services Inventory: Spreadsheet **49**

Appendix C: List of Documents Reviewed **50**

Appendix D: Site Visit Agenda and Participants **53**

Appendix E: Factors Influencing the Interpretation of Staffing Ratios **55**

Common acronyms used in this report

BMV ..... Bureau of Motor Vehicles

CIO ..... Chief Information Officer
CJIS ..... Criminal Justice Information Services
CSA ..... CJIS Systems Agency
CSO ..... CJIS Security Officer

DAS ..... Ohio Department of Administrative Services

EMA ..... Emergency Management Agency
EMS ..... Division of Emergency Medical Services
EOC ..... Emergency Operations Center

FBI ..... Federal Bureau of Investigation

GIS ..... Geographic Information Systems

ISO ..... Information Security Officer
IT ..... information technology
ITIL ..... Information Technology Infrastructure Library
ITO ..... Information Technology Office
ITSM ..... Information Technology Security Management

LEADS ..... Law Enforcement Automated Data System

MCA ..... Management Control Agreement
MPLS ..... Multi-Protocol Label Switching

NCIC ..... National Crime Information Center

OAC ..... Ohio Administrative Code
OCJS ..... Office of Criminal Justice Services
ODPS ..... Ohio Department of Public Safety
OHS ..... Ohio Homeland Security
OIT ..... Office of Information Technology (Ohio DAS)
OIU ..... Ohio Investigative Unit
OSHP ..... Ohio State Highway Patrol
OTSO ..... Ohio Traffic Safety Office

PMI ..... Project Management Institute
PMO ..... Project Management Office

SLA ..... Service-Level Agreements
SOCC ..... State of Ohio Computer Center

I. Executive Summary

In November 2009, the Ohio Department of Public Safety (ODPS) engaged SEARCH, The National Consortium for Justice Information and Statistics,[1] to conduct a study of information technology (IT) efficiency in the Department. This report presents the findings and recommendations resulting from this study.

The State of Ohio, like virtually every state in the country, is facing substantially lower revenue to fund government operations. The Governor and Legislature have emphasized the importance of agencies finding ways to reduce costs and improve efficiency. ODPS Director Cathy Collins-Taylor, who was appointed by Governor Ted Strickland in October 2009, has rightly placed operational efficiency among her top priorities. Given the significant share of IT spending in the ODPS budget, and the criticality of IT to the Department's mission, the decision to conduct an IT efficiency study is an appropriate and commendable step in pursuit of the overall efficiency objective.

SEARCH developed the findings and recommendations in this report following four days of interviews with the ODPS executive leadership team and staff members from the current three quasi-independent IT groups within ODPS—the Information Technology Office (ITO) within the Administrative Division, the Emergency Management Agency (EMA) IT group, and an IT group that supports the Law Enforcement Automated Data System (LEADS) and the network at the Ohio State Highway Patrol (OSHP). SEARCH appreciated the forthright cooperation and assistance of the group of dedicated individuals who participated in the interviews.

The bottom-line finding of this study is that there is strong potential for efficiency gains in ODPS' use of information technology, largely through consolidation of staff and infrastructure. Along with this consolidation, the Department should focus on maturing its approaches to IT governance, performance measurement, and accountability, and should repurpose senior-level IT positions to focus on strategic direction. The Department's executive leadership team—including the Director, Deputy Director, component agency Directors, and the Chief Information Officer (CIO)—should recognize the change-management aspects of the recommended consolidation, and as such should focus on communications and trust issues related to IT needs and services.

[1] SEARCH provides onsite, no-cost assistance to state and local jurisdictions under several grant programs administered within the Office of Justice Programs, U.S. Department of Justice. This assistance is funded by the Bureau of Justice Assistance. Background on SEARCH, the National Technical Assistance Program, and project staff is included as Appendix A.

This report will document specific findings that support this conclusion, and offer a recommended course of action for the Department's leadership to realize these efficiencies. The following lists summarize, at a high level, the principal findings and recommendations.

Summary of Findings

- Notwithstanding the other findings (and subsequent recommendations) in this report, ODPS has a strong foundation on which to build an optimal, efficient IT support function. Across the three separate and quasi-independent IT groups, there are talented, dedicated, and experienced professionals who see themselves as having a stake in the success of the Department through efficient provisioning of IT services.

- ITO has recently begun technology migration projects that, when complete, will align ODPS with industry and statewide best practices: migration off the mainframe, standardizing email and office groupware on Microsoft Exchange, and virtualizing server environments.

- While there is a backlog of IT projects, resources seem adequate to address all critical Department needs, with adequate remaining bandwidth to pursue longer-term efficiency improvements.

- Specific IT functions, such as purchasing and front-line helpdesk, are currently operating well below optimal efficiency Department-wide, and are likely areas in which a consolidated approach could realize efficiency gains in a fairly short period of time. There are areas where IT support in the Department is "one deep," putting critical functions at risk and affecting service levels.

- Recently, ITO has implemented an informal IT governance structure, through the appointment of customer relations managers who conduct regular reviews of business unit needs and priorities (called "roadmap meetings"). Business unit leaders acknowledge that these practices have improved IT service. The CIO generally enjoys the trust and confidence of the business unit leaders served by ITO.

- The lack of a formal governance structure for IT reduces transparency and communications between IT and the business units; this impedes a common understanding of business priorities and the IT services necessary to address those priorities. The level of trust and open communication between the separate IT groups is also not what it should be; this manifests in difficulty collaborating and coordinating between the groups.

- ODPS has "grown organically" over time, and as agencies have joined ODPS, much of their independent IT structures have remained. As a result, there is costly redundancy, missed opportunity for economies of scale, and (in some areas) significant risk of service interruption that could affect critical Department operations.

- Business unit leads at EMA and LEADS have identified legitimate unique IT requirements. However, these requirements in and of themselves do not justify each business unit having its own independent IT group. Service level agreements (SLAs) with ITO could satisfy these same requirements, as long as ODPS simultaneously addresses the current lack of formal IT governance and accountability mechanisms.

- While the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) security policy[2] places specific requirements on the LEADS network, nothing in the policy requires that OSHP provision the network itself. There are alternative approaches, in use in several other states, which may be more efficient and better aligned with the Department's overall IT direction.

- Reducing unnecessary redundancy across the three independent IT groups, especially in the areas of front-line support and server and application hosting, could potentially result in significantly higher service levels and an opportunity to repurpose up to five positions to more strategic objectives.

- Traditionally, specific IT positions have been funded through particular sources, such as Federal grants or explicit allocations to ODPS component agencies (such as the Bureau of Motor Vehicles [BMV]). ITO has demonstrated an ability to work successfully with business units—such as the Office of Criminal Justice Services (OCJS), Ohio Homeland Security (OHS), and BMV—to ensure proper allocation and utilization of these positions, while expanding and deepening the coverage provided by those positions.

- HB648[3] required Ohio State agencies to create rules that provide procedures for logging State employee access to confidential personal information. Each agency is also to have a single point of contact to monitor the logs, conduct audits, and interact with the Chief Privacy Officer in the Office of Information Technology, Ohio Department of Administrative Services. The separation of IT groups (combined with lack of communication and trust) makes it difficult and less efficient for ITO to fulfill this responsibility.

---

[2] Refer to the CJIS Security Policy version 4.5 from the FBI CJIS Division, available to criminal justice agencies via http://www.leo.gov/.

[3] Refer to http://www.legislature.state.oh.us/bills.cfm?ID=127_HB_0648 for the final version of HB648.

Summary of Recommendations

- ODPS should consolidate IT support and services within ITO. The CIO should be given the authority to reorganize ITO as necessary, including identifying positions made redundant by the consolidation. ODPS should not eliminate positions, but rather should repurpose redundant positions to address currently unmet needs, such as strategy, governance, and architecture.

- ODPS should, under a consolidated IT organization structure, identify and implement opportunities for process efficiency, such as streamlining the service desk process and consolidating procurement.

- ODPS should strongly consider consolidating all Department network management under ITO.[4] To satisfy the FBI CJIS requirements, the LEADS unit at OSHP should execute a management control agreement (MCA) with ITO. An MCA would ensure that the OSHP remains the final authority on access control and other network policy issues, while allowing ITO to operate the network on a daily basis.

- Management at all levels of ODPS should work together to manage the organizational change inherent in the recommended consolidation. Continued frequent and open communications with impacted staff will be important. The message SEARCH heard from ODPS Director Collins-Taylor and CIO Jeffrey Clouse at the outset of the technical assistance engagement was that they do <u>not</u> intend to reduce staffing levels; it is imperative to include this same message to staff as senior leadership begins the consolidation.

- The CIO should create a strategy and policy office managed by a Deputy CIO. This group would subsume the existing Project Management Office (PMO) but would add a strategic planning function and a technology standards or enterprise architecture function. The agency's Information Security Officer (ISO) should also be located within this group. The strategy and policy office would be responsible for supporting the new IT governance and accountability mechanisms.

- The CIO should create a second new Deputy CIO position to oversee operations; all existing ITO staff outside of the PMO would report up through the Deputy CIO of Operations. The creation of the two Deputy CIO positions would allow the CIO to focus on his or her role as a member of the ODPS executive team, maintaining a peer-to-peer relationship with the business unit leaders.

---

[4] While SEARCH believes this is the preferred option, several options are available to ODPS. These options are presented in detail in Section V below.

- ODPS should implement a formal IT governance structure that ensures open, effective communication and transparency in IT decision-making, especially with respect to the setting of priorities and establishing Department-wide technology standards. This governance structure should be based on service-level agreements between ITO and each business unit; SLAs should be enforced through a new IT accountability mechanism that ensures both parties adhere to the provisions of each SLA.

- Business unit leaders should, as part of the consolidation transition with their existing IT staffs, document clearly any specific or unique IT requirements of their respective units. These requirements should serve as a starting point for SLA negotiation with ITO.

- ODPS should continue current technology migrations from the mainframe, toward Microsoft Exchange, and toward virtualization. In doing so, ITO should reconfirm that current infrastructure will support the new environments (in particular, that the network will support consolidated email). ITO should also continue implementing best practices of project management, change management, and IT service management.

II. Introduction and Request for Assistance

The Ohio Department of Public Safety requested technical assistance from SEARCH to assess the information technology resource strategies with respect to the three information technology groups within the department and to determine if the current IT structure is the most efficient and effective structure for the agency. The results of this report are to make recommendations on how to best structure these resources within the department. The principal objectives of this technical assistance engagement include:[5]

1. Review of the IT organizational structures of the ITO, OSHP, and EMA IT groups and determine the roles and responsibilities of each IT group.

2. Document the high-level business processes that each IT group supports from a services perspective.

3. Create a functional matrix that illustrates the overlap (if any) and uniqueness of the roles and responsibilities of each IT group.

4. Analyze and document the business reasons that currently justify the need for three separate IT groups.

5. Document the impact to the agency of having three separate IT groups (lack of leveraged IT procurements, software licenses, duplicate training, etc.).

6. Prepare a written recommendation to ODPS as to the suggested structure of the ODPS IT organization and justify that recommendation accordingly.

ODPS provided SEARCH staff with relevant and current documentation regarding the Department's policies and procedures, organization structure, major projects, budgets and other topics relevant to this technical assistance.[6]

SEARCH developed the findings and recommendations in this report following review of this material, as well as four days of interviews with the ODPS executive leadership team and staff members from the three quasi-independent ODPS IT groups[7]—the Information Technology Office within the Administrative Division, the Emergency Management Agency IT group, and an IT group that supports the Law Enforcement Automated Data System and the network at the Ohio State Highway Patrol. SEARCH appreciated the forthright cooperation and assistance of the dedicated individuals who participated in the interviews.

---

[5] IT Resource Efficiency Study Statement of Work, October 29, 2009.

[6] Appendix C: List of documents provided.

[7] Appendix D: Agenda of site visit meetings and participants.

III. Background

Ohio Department of Public Safety[8]

The ODPS is comprised of the following nine divisions, which work together to serve and protect the safety and security of Ohioans:

- **Bureau of Motor Vehicles:** BMV provides motor vehicle-related services, such as driver's licenses, vehicle registration and titling, insurance industry oversight, and dealer oversight.

- **Emergency Management Agency**: EMA is responsible for coordinating activities to mitigate, prepare for, respond to, and recover from disasters.

- **Division of Emergency Medical Services**: EMS is responsible for the education, certification, and investigation of all emergency medical service and fire service providers in the State of Ohio.

- **Office of Criminal Justice Services**: OCJS is responsible for the administration and evaluation of State and Federal grants for law enforcement, victim assistance, juvenile justice, crime prevention, and courts and corrections programs.

- **Ohio Homeland Security**: OHS is responsible for coordinating the State's overall efforts to prevent, respond to, and recover from major homeland security incidents. Duties also included providing oversight for State and local coordination of infrastructure protection and leading Ohio's homeland security and domestic preparedness efforts.

- **Ohio Investigative Unit**: OIU is committed to providing quality enforcement of State, Federal, and local laws with emphasis on liquor, food stamp, and tobacco offenses, further offering educational guidance and professional assistance to law enforcement agencies and the general public.

- **Ohio State Highway Patrol**: OSHP is an internationally accredited agency whose mission is to protect life and property, promote traffic safety, and provide professional public safety services with respect, compassion, and unbiased professionalism. The OSHP provides statewide traffic services to keep Ohio's roadways safe; statewide emergency response services and support services to the public and the criminal justice community; investigation of criminal activities on State-owned and -leased property throughout Ohio; and security for the Governor and other dignitaries.

---

[8] Department and Division information from: http://publicsafety.ohio.gov.

- **Ohio Traffic Safety Office**: The mission of OTSO is to save lives and reduce injuries on Ohio's roads through leadership and partnering efforts with others interested in traffic safety, utilizing the most innovative and efficient methods possible of managing State and Federal resources. OTSO coordinates and funds the efforts of DUI Task Forces, local law enforcement, and safety partners around the State to combat impaired and unsafe driving. OTSO also promotes educational programs, coalition-building efforts, and campaigns focused on highway safety. It also houses the State's Motorcycle Ohio program, its Driver Training program, and the Department's Traffic Statistics Division.

- **Administrative Division**: The Division provides Department-wide services, such as human resources, accounting, and IT services.

ODPS Director Cathy Collins-Taylor, who was appointed by Governor Strickland in October 2009 and serves in the Governor's cabinet, is the chief executive official in the Department.

ODPS History and IT Environment

Over time, ODPS was formed from the gradual consolidation of formerly independent State agencies. In 1933, the Legislature created the Ohio State Highway Patrol, Bureau of Motor Vehicles, and the Department of Highways. The Department of Highway Safety was formed in 1954 to include the BMV, OSHP, and an administrative division. In 1992, the department was renamed to the Department of Public Safety, and other divisions relating to public safety were added to the department. At this time, IT services were very much decentralized across the divisions. EMA joined ODPS as a division in 1996, bringing an additional IT group to the Department.

In 1998, ODPS co-located its divisions to the Charles D. Shipley Building in Columbus, and attempted to consolidate as many administrative functions as possible at the same time. As part of this consolidation, several formerly independent IT functions were combined into the ODPS Information Technology Office; however, IT support for LEADS and EMA have remained separate entities with only very loose accountability to ITO.

Like any IT operation that supports a large operation, the three ODPS IT groups provide a wide range of standard services to the business units they support. These services include:

- Network connectivity
- Data storage and file/document management
- Email
- Telephony (desktop and mobile telephones, voicemail)

- Desktop/Workstation support
- Application hosting and server maintenance/support
- Enterprise applications
- IT support services, such as service desk, project management, procurement, planning, and policy

Other than leveraging network services (e.g., the metropolitan Ethernet backbone in the Columbus area) and data center space provided by the Ohio Department of Administrative Services' (DAS) Office of Information Technology (OIT), and purchasing software and equipment off the State's term contract, ODPS provisions virtually all of its own IT services.

During this technical assistance engagement, SEARCH prepared an IT services catalog that documents all current ODPS IT services. The catalog has been delivered electronically to ODPS along with this report.

ODPS maintains three networks:

- **ODPS:** One network connects ODPS locations, including the Shipley Building, deputy registrar sites, and OSHP posts.

- **LEADS:** The second network connects law enforcement users of the Law Enforcement Automated Data System to LEADS applications and services in Columbus.

  The LEADS network also provides Ohio law enforcement agencies with access to the FBI National Crime Information Center (NCIC) and Nlets—The International Justice and Public Safety Network.

  OSHP manages the ODPS and LEADS networks, coordinating with business units and ITO as necessary when making network changes.

- **EOC:** The third network is a local-area network operating within the EMA's Emergency Operations Center (EOC).

  EMA staff maintain the network inside the EOC.

OHSP network service technicians provide 24/7 monitoring and support of the network infrastructure, which includes over 2,100 network devices, from routers and switches to firewalls and network access control appliances, as well as more than 940 data circuits.

OSHP network administration staff stated during site visit interviews that their top priority is operation and maintenance of the LEADS network.

ITO provides support for over 220 applications used across all ODPS divisions.

The three IT groups host these applications on numerous mainframe and server environments. ODPS hosts some servers at the State of Ohio Computer Center (SOCC) managed by the DAS OIT, additional servers at the Shipley Building, and a few servers at the EOC for EMA applications. The Department also currently maintains a network of around a dozen Novell file, print, and email (post office) servers across ODPS locations, including OSHP posts.

As with many state government agencies nationwide, ODPS has a long history of providing applications on a mainframe platform. A current project, called Exodus, aims to migrate all Department applications off the mainframe and onto server platforms. The Department's strategic development platform is Microsoft .NET.

OSHP currently provides telephony services for all of ODPS, except for EMA. Voicemail is provided by OIT and coordinated through OSHP. EMA currently provides its own telephony services.

ITO provides most of the core IT support functions for the department; however, both front-line IT support (i.e., help desk) and second-tier support functions are distributed across the three IT groups. EMA and OSHP provide all support functions with agency staff, while ITO provides support using a mix of agency staff and an outsourced support provider, Sarcom.[9]

As is typical for state public safety agencies, the ODPS IT groups are funded by a variety of sources:

- ITO is primarily funded through the Department's general fund.
- OSHP IT is funded from a combination of LEADS user fees and OSHP general fund allocations.
- EMA IT is funded mostly from Federal grants, which the Department generally matches through title and drivers record abstract fees.

[9] See http://www.sarcom.com.

IV. Observations and Analysis

This section provides SEARCH project staff's observations and analysis based on review of project materials, discussions, and meetings. **Section V** provides recommendations based on these findings.

— Strengths of ODPS IT Staff

Staff within the three ODPS IT groups are highly dedicated, experienced professionals who largely have the skills necessary to perform their job functions. The Department employs a wide range of technologies, including state-of-the-art technologies such as Multi-Protocol Label Switching (MPLS) in the network and server virtualization in the data center. The skills of the staff who work with these technologies seem to be adequate to manage them effectively. Generally speaking, staff do not seem reluctant to adopt new technologies and expand their skills, as evidenced by the current migration to Microsoft Exchange for email and groupware services. ODPS IT will face a significant challenge in the near term as applications transition from the mainframe to a Microsoft .NET platform, necessitating the adoption of new programming languages and object-oriented design skills. Department IT managers properly recognize the learning curve associated with this technology migration, and recognize that it will likely represent a very difficult transition for many staff.

Interviews with staff across the IT groups (principally at the management level) indicated that there is strong support for the organization and its objectives. While communications between the IT groups are not as open and effective as they could be, within each IT group there is very good communication and a strong sense of cohesion. Generally speaking, managers have worked at ODPS for a long time and are committed to the organization.

While staff expressed some understandable concern and uncertainty regarding where Department IT support is headed, the managers interviewed generally seemed willing to support the decisions of executive management and to work within the roles assigned to them. This overall attitude will provide an important foundation if the Department should decide to improve efficiency—through adoption of this report's recommendations, or otherwise.

ODPS has dedicated staff that is supportive of department leadership. It was stated more than once during our site visit: "Provide a direction and we'll do our best to work toward it," which translates to a staff that is ready to support Department leadership and work toward common goals and objectives.

— Technology Direction

ODPS has recently established a direction for enterprise technology that will provide significant benefit to the Department in the end. These migrations serve to align the Department with industry best practices and state-of-the-art technical capabilities.

Like many organizations of its age and size, ODPS has traditionally deployed mission-critical business applications on a mainframe platform. While the right choice two decades ago, mainframe platforms now offer less functionality and higher overall cost of ownership than alternatives based on distributed server platforms. Mainframes tend to rely on proprietary, vendor-specific components and programming languages, reducing competition and increasing prices. It is also generally more difficult to find and retain skilled system administrators and programmers for mainframe platforms. To address this issue, ITO has initiated a mainframe migration project that will, over the next biennium, migrate most (if not all) applications to commodity server platforms.

ITO has also begun migrating from a Novell network and groupware application to a Microsoft Windows network and Exchange. This aligns ODPS with the direction of most Ohio State agencies and most government agencies nationwide. It also consolidates licensing and technology to a large extent, since ODPS already leverages Windows for the enterprise desktop and office applications. ITO is seeking to reduce the cost of managing email and groupware by consolidating the Department onto a single Exchange environment. While SEARCH believes there are potential risks in this approach (especially regarding network bandwidth), those risks are manageable if known and documented. The potential savings from email consolidation are worth the investment in architecture and risk mitigation that consolidation entails.

SEARCH finds that these technology migrations have great potential to save ODPS money while improving reliability and flexibility. As such, the Department has already begun making important improvements in efficiency.

— Informal IT Governance

IT governance is an approach to making decisions about the deployment of technology in an organization. Effective IT governance structures ensure that decisions are made by the appropriate people, at the right level in the organization, and in a timely and efficient manner. IT governance generally offers approaches to hold both the provider(s) and consumers of IT services accountable for the obligations they must make to one another for IT to work effectively in support of the organization's business.

Typical categories of decisions addressed by an enterprise IT governance mechanism are:

- Allocation of IT resources to projects and infrastructure investments
- Setting of policies for the use of IT resources, especially in the areas of appropriate use and security
- Long-term and strategic planning
- Measuring the performance of IT
- Ensuring appropriate reuse of IT assets such as enterprise data and applications.

ODPS currently employs an informal IT governance structure. ITO has appointed customer relations managers, who work in the IT Project Management Office (PMO) and are assigned one or more ODPS divisions. They are responsible for meeting regularly with senior staff of their assigned divisions to review IT performance, prioritize projects, and identify critical needs or issues. The customer relations managers maintain a "roadmap" for each division; the roadmap lists ongoing projects and IT investments for that division, and can be used by IT and the division leadership to manage and prioritize projects.

Both ITO and division leaders report that the roadmap process works well for its intended purposes.

ITO has also implemented a change control process, with a change control board that is notified of all pending application or infrastructure changes and disseminates information about pending changes as appropriate. However, the ITO, EMA IT, and OSHP IT groups have a difference of opinion regarding the level of commitment to the change control process and the degree to which it is regularly and consistently used.

IT governance across divisions is largely missing, and as a result significant IT decisions with Department-wide impact are often not made at all, or are significantly delayed. A recent example is the OSHP proposal to create a separate network from the OSHP-managed LEADS network for the remainder of ODPS. An effective IT decision-making structure would escalate this proposal to the proper level and ensure that the right decision is made in a timely fashion. Instead, the OSHP proposal has gone unanswered for more than a year.

The lack of a formal IT governance structure has reduced the transparency of IT decisions and affected communications between divisions. During site visit interviews, IT staff noted that they have occasionally been surprised about changes to infrastructure or configuration, and that some planned projects or investments have also not been communicated effectively to the right stakeholders. There is also no formal mechanism to hold ITO accountable for adhering to promised service levels.

It is important to note that recently ODPS, under the leadership of ITO, has begun implementing service-level agreements with business units, starting with EMS and OIU. These SLAs set appropriate expectations regarding the services that ITO provides, and add a measure of accountability to the business unit's relationship with ITO. Formalizing and documenting expectations are important aspects of effective IT governance.

ITO has also established a PMO that, in addition to providing customer relations managers, oversees application of project management best practices to IT projects within ITO. The PMO has standardized on the Project Management Institute (PMI) body of knowledge,[10] as the overall set of practices and techniques for project management.

— Communications and Trust

The current three IT groups do not have the level of trust and openness of communication that are required for effective collaboration and cooperation. During interviews during the site visit, when asked to name an aspect of ODPS IT that needed to change, communications and trust issues were among the first topics mentioned across the board.

As an example, when one group asked another group what the plans were for a particular project or pending infrastructure change, the reaction from the other group was to ask why the requestor needed to know. This indicates a questioning of intentions and in general a lack of trust. While members of the groups spend a good deal of time working together, they do not seem always to be forthcoming about upcoming projects or changes. Members of each group expressed frustration with having to spend so much of their time teaching or mentoring staff from the other groups in their areas of expertise. Staff feel like other groups have projects underway that will significantly affect them, yet are unable to learn what the plans for those projects are.

There is not a sense of common purpose or shared priorities across the groups. Because of the lack of communication and trust, the groups are missing opportunities to cross-train employees and collaborate with each other to accomplish major tasks or get through a crisis.

Formal IT governance, if adopted, would address these concerns to a certain extent. Other recommendations that appear in Section V of this report would also naturally incline the groups to communicate more directly. However, the issue of communications and trust requires attention from ODPS senior management, regardless of the organizational structure or approach that the Department chooses for the future.

---

[10] For details, see http://www.pmi.org/Pages/default.aspx.

— Level of IT Resources

The question of whether ODPS IT, across the board, is adequately staffed is complex, with a different answer depending on the area of IT under examination.

Staff from the Computer Operations group within ITO reported during interviews that they currently have a significant amount of spare "bandwidth" on their teams—meaning that they could take on additional levels of work without expanding staff. They believe—and SEARCH concurs—that their groups could easily absorb the server and desktop support needs of EMA and non-LEADS support needs at OSHP without needing to add staff positions.

On the other hand, the OSHP network administration group reported during interviews that it is currently operating at full capacity, and is often stretched in fulfilling its current responsibilities. Should ODPS be in a position to add or repurpose IT positions, the network administration group could make effective use of them.

One of the primary factors in an organization's ability to provide adequate support is the degree to which functions are "one deep" in terms of personnel. In smaller organizations that can afford only one support person for a particular application or function, service levels and support tend to suffer when that person takes vacation or, in the extreme, separates from the organization. Approaches in which staff who are expert in another function provide "secondary coverage" do not work as well, since they can preclude the development of deep expertise and customer engagement.

The OSHP network and ITO support groups generally have adequate coverage for their support functions, without going "one deep" in critical areas. EMA IT, however, involves generalist staff providing coverage for one another, but primary support roles are staffed with only a single person. While EMA has done an admirable job making this work, it is not an optimal support strategy. Anecdotal reports indicate that service and support levels have often been below the desired level during EOC activation exercises, with workstation setup and logon support tasks taking from several minutes to hours to resolve.

ITO and OHS have recently demonstrated success at using focused business unit funds (i.e., grant funding) to augment ITO staff with outside contractors for specific projects. This capability allows ITO to be responsive to business unit needs while not disrupting other project commitments.

— Network Administration Challenges

In January 2008, OSHP proposed to then-Director Henry Guzman that ODPS separate the OSHP and ODPS networks, and that OSHP build its own separate server hosting capability for LEADS applications.[11] The justification for this proposal is to allow ODPS to control and manage the Department's network (outside of LEADS) without the constraints of the FBI CJIS Security Policy.

SEARCH agrees with the overall motivation to provide ODPS with the greatest possible flexibility while simultaneously complying with FBI CJIS requirements. However, SEARCH finds that creating a completely separate network and a separate server hosting facility at OSHP runs counter to the Department's overall objective of reducing IT complexity and costs. Based on observation of other states' architectures, as well as SEARCH's own reading of the FBI CJIS Security Policy, there are options short of complete network separation that allow the Department to comply with the policy while enabling flexibility on the non-law enforcement segments of the network. These other options should be assessed against the OSHP proposal, and the most efficient option chosen; SEARCH will offer its recommendation in **Section V, Recommendations**.

— Unnecessary Redundancy

As noted in **Section III, Background**, ODPS has grown "organically" over time, as legislative and executive policy have consolidated public and traffic safety agencies within the Department. In most cases, the IT functions of the formerly independent agencies have been folded into the ITO. However, in two cases—EMA IT and OSHP IT—significant IT functions have remained independent.

The Department's leadership has continued to separate the IT groups based on a perception of unique business requirements, and a belief that consolidating IT functions would jeopardize fulfillment of those requirements. In the case of OSHP, the Department's understanding of FBI requirements for State networks that connect to the NCIC compelled ODPS to place both the Department's network and the statewide LEADS network under OSHP control. In the case of EMA, the Department has concluded that its emergency response role and particular business continuity requirements necessitated having a separate IT staff located at the State's Emergency Operations Center.

SEARCH finds that OSHP and EMA do indeed have specific, unique IT requirements. The FBI CJIS Security Policy does indeed involve specific rules about the management control of State networks that connect to NCIC. However, those rules do not require that a law enforcement agency actually provision and manage the network itself. Several State law enforcement agencies, operating within the FBI policy, have delegated network provisioning and management to

[11] Source: LEADS Separation Interoffice Communication dated January 29, 2008.

another party (generally, a State technology agency), and have implemented an agreement[12] with that party to fulfill the requirements of FBI policy. The FBI has given the States great latitude to determine an organizational structure and network management strategy that are efficient and appropriate for each State's environment. At the same time, they have ensured law enforcement control over the network by requiring a standard agreement between the law enforcement agency and the network provisioner. Such an approach is available to Ohio, and in SEARCH's opinion, is appropriate for ODPS.

EMA has legitimate requirements for immediate IT support in the event of a natural disaster or other crisis that requires EOC activation. It also legitimately requires that critical applications be available even if network connectivity is unavailable between the EOC and the Shipley Building. While SEARCH saw no evidence during the site visit of formal documentation of these requirements in detail, it certainly should be possible to articulate these requirements in an SLA between EMA and ITO. As such, SEARCH finds that the known requirements are not adequate justification, in and of themselves, to justify an independent EMA IT group.

There is significant potential for reducing redundancy in the provisioning of IT services across the Department. Table 1 illustrates where there are overlapping service areas between the three IT groups.[13]

---

[12] These agreements, called "management control" agreements, or MCAs, can be in the form of a memorandum of understanding (MOU) that specifies all the CJIS requirements (e.g., staff background checks, physical security of servers, etc.) and other provisions that ensure the law enforcement unit maintain "in control." Once that agreement is in place, the delegated party can directly run the network (manage routers and switches, coordinate telephone company circuits, patch and program devices, etc.). This approach complies with the FBI CJIS Security Policy as long as the accountability and ultimate decision-making reside with a criminal justice agency designated by the FBI as the controlling agency for the state.

[13] The services spreadsheet included as Appendix B further describes these overlaps by outlining who provides each service, the functionality of the service, and the estimated cost of the service in full-time employees (FTE).

Service	ITO	OSHP	EMA
Email	X	X	X
BlackBerry Services	X		
File Services			
LAN-based (e.g., Novell or Windows network file systems)	X	X	X
FTP	X		X
Database hosting	X	X	X
Document management	X	X	
File storage / backup / data retention / open records requests	X	X	X
Print Services			
Local / LAN printer support	X	X	X
Acquisition	X	X	X
Special Printer	X	X	
Batch/Bulk printing	X		
Telephony			
Desktop		X	X
Voicemail		X	X
Mobile		X	X
Desktop/Workstation			
Acquisition	X	X	X
Configuration/Deployment	X	X	X
Support	X	X	X
Network			
Internet connectivity		X	X
Business partner connectivity		X	
Inter-agency (within ODPS) connectivity		X	
Intra-agency connectivity		X	
LAN provisioning		X	X
Network security	X	X	

Service	ITO	OSHP	EMA
Other Security			
Access management	X	X	X
Desktop/Workstation	X		
Directory services	X	X	X
Hosting			
Web applications – external	X	X	X
Web applications – internal	X	X	X
Server provisioning (including virtualized)	X	X	X
Mainframe hosting	X		
Enterprise Application Provisioning			
HMS Web	X		
Peoplesoft	X		
Central repository	X		
Listserv	X		
CIMS – critical information management system	X		
Phone directory application	X		
Policies and procedures	X		
IT project tracking	X		
BASS	X		
Service Management / Support Capabilities			
Service desk	X	X	X
Strategic planning	X	X	X
Project management	X	X	X
Business analysis	X	X	X
Policy audit/compliance	X	X	X
IT procurement	X	X	X
Application Development (Programming)	X	X	X

Table 1: Duplication of IT Functions Based on Services Spreadsheet (Appendix B)

— Staffing Ratios and Redundant Positions

It is useful to quantify the findings of two prior Finding sections (**Level of IT Resources** and **Unnecessary Redundancy**) in terms of two key measures: The ratio of IT staff, by function, to the number of supported users; and the number of redundant IT positions across the three IT groups.

Staffing Ratios

Note that "redundant position" does not necessarily mean a reduction in overall ODPS IT staffing levels, or the elimination of any positions. ODPS executive management made clear to SEARCH that the intent is not to reduce IT headcount through this efficiency exercise, but rather to repurpose redundant positions to more efficient and effective uses. As addressed in **Section V, Recommendations,** SEARCH finds that—absent a reduction in the ODPS IT budget, or a legislative or executive mandate to reduce staffing levels—it makes sense for ODPS to leverage the opportunity of redundant positions to address currently unmet needs.

Staffing ratios are a useful measure of efficiency, as they measure the number of IT staff that are used to meet the needs of a defined number of users or customers. As such, they represent a measure of productivity that is easy to compute. At the same time, comparisons of an organization's staffing ratios to industry "benchmarks" must be interpreted properly and with full context of the situation underlying the measures. In particular, services that are less mission-critical, or where user/customer expectations of service levels are lower, require less intensive staff ratios; for these services, a higher IT staff/user ratio would be appropriate. Industry benchmarks are aimed at the largest possible audience, and therefore may over-state or under-state the ratio required for a particular organization's operations. Appendix E lists some key factors in adjusting industry benchmarks to the appropriate levels.

Ultimately, established service levels and direct measures of user satisfaction with IT services are much better tools for assessing productivity. For example, if IT and business units agree that password resets should be completed within one hour of helpdesk contact, or that printer repairs should be completed within one business day, then IT should track performance against these stated service levels and assess whether current staffing and procedures are consistently hitting the targets. IT can supplement these measures with basic customer satisfaction surveys or interviews to get a complete picture of whether the service is meeting expectations.

None of the IT groups at ODPS measures service provisioning at this level currently (a topic to be addressed in the **Recommendations** section). However, SEARCH interviews with business unit leaders indicated, for the most part, that IT support is meeting user expectations. During the site visit, SEARCH found no evidence to discount this general perception among the division leaders who were

interviewed. As such, regardless of comparisons to industry "benchmarks," IT support staffing levels at ODPS are, generally speaking, adequate to meet expectations. The exception to this general rule is in the area of application development, where some division leaders expressed a concern that the ITO backlog for application development is too long.

Across all divisions, ODPS has approximately 6,000 users of IT services. This includes staff in the Shipley Building (headquarters), OSHP posts, BMV deputy registrar facilities, and other field offices. Sixteen IT staff provide front-line, tier-one support to these users (11 OSHP service desk staff, four outsourced service desk staff that ITO provides via Sarcom, and one primary support full-time employee (FTE) at EMA). In addition, 17 OSHP network administrators provide on-site support at locations outside Columbus. Thirty-three staff that support 6,000 users results in a staffing ratio of approximately 180:1, which is higher than the standard industry benchmark of 75:1 – 100:1.

However, it is important to understand the 180:1 staffing ratio in the context of second-tier support at ODPS.[14] Most of the 46 staff in Computer Operations within ITO assume some second-tier support responsibilities. EMA has five staff (in addition to the one primary support staff noted above) in Network Administration Support, and nine staff in Telecommunications Support (excluding staff assigned to radiological device support). OSHP has eight additional network administration staff at headquarters, plus 11 staff in Telecommunications Support. Thus, at the second-tier support level, ODPS has 59 staff in operations or network administration roles, with another 20 in telecommunications support roles, giving second-tier support ratios of 100:1 and 300:1 for operations/network and telecommunications, respectively. These ratios bring ODPS close to industry benchmarks.

Redundant Positions

It was not an objective of SEARCH's technical assistance engagement to provide a detailed, precise analysis of redundant positions. The following analysis is SEARCH's best assessment, given the information available. ODPS should conduct a focused follow-on analysis to confirm this assessment, and potentially to identify other opportunities to repurpose positions to more strategic goals.

SEARCH assumes, based on current information, that ODPS will not reduce direct support positions, as doing so would likely reduce the Department's ability to continue meeting users' support expectations. Thus, the identification of redundant positions focuses on management-level positions:

[14] Source: Organization charts provided by ITO, OSHP, and EMA.

- **Front-line support staff.** Management of 33 front-line (tier-one) support staff currently occupies 3.5 FTEs across the Department: two in ITO, one at OSHP, and .5 at EMA. SEARCH finds that ODPS could reduce this management function to one FTE without a loss in service level, assuming that the Department could organize the existing 33 staff into functional groups and move 1–2 of those staff into a line management role.

- **Administrative staff.** Similarly, management of 59 network administration staff occupies four FTEs across the Department: two in ITO, 1.5 at OSHP, and .5 at EMA. SEARCH finds that ODPS could reduce this management function to one FTE, assuming that the Department could organize the existing 59 staff into functional groups (e.g., LEADS, wide-area, and local-area network support) and move 2–3 of those staff into a line management role.

- **Telecommunications staff.** Finally, management of 20 telecommunications staff (not including OSHP radio and mobile data support) occupies two FTEs across ODPS: one at OSHP and one at EMA. SEARCH finds that ODPS could reduce this management function to one FTE without a loss in service level.

To summarize, without considering redundancies in direct support (i.e., non-management) roles, ODPS could likely identify 4–5 IT management positions as redundant in the current structure.

— Inconsistency of Core IT Support Functions

The "low-hanging fruit" of IT efficiency is in streamlining the core IT support functions of help desk/service desk and desktop support, procurement, application hosting/server provisioning, and security. The "organic" growth of IT at ODPS has prohibited the establishment and enforcement of consistent approaches to these core processes. As a result, ODPS is experiencing inefficiencies due to lack of economies of scale, diminished reuse and cross training of staff across IT groups, and reduced service levels.

Help Desk/Service Desk and Desktop Support

The diagram (Figure 1)[15] depicts the user support process at ODPS, from initial contact by a user, through front-line and tier-two support functions, to resolution.

[15] Source: Keith Albert, ITO.

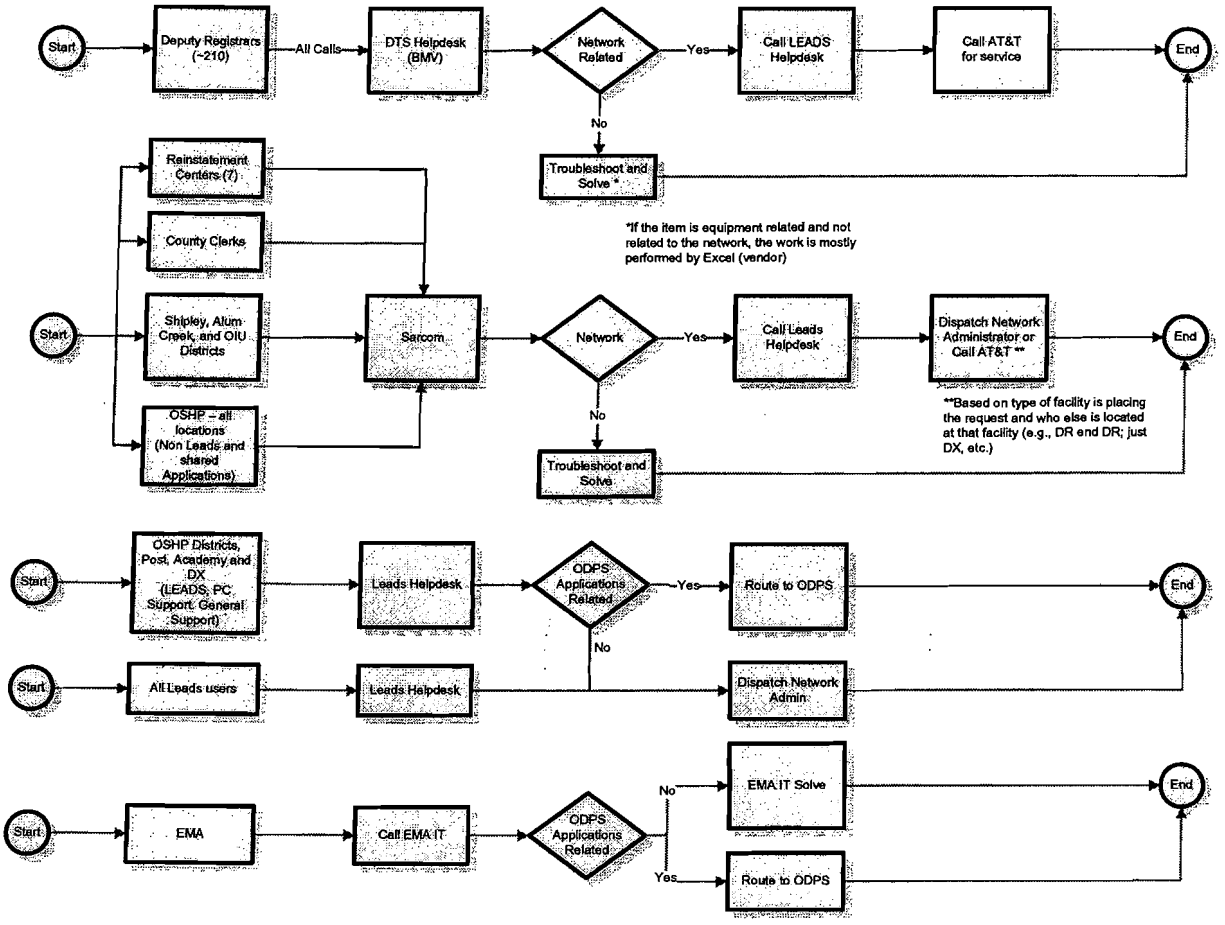

Figure 1: ODPS User Support Process

This support process is inefficient in the following ways:

1. Users have varied paths for support, depending on the nature of their support request and/or where they are working. For users that work in multiple areas of the Department, this causes confusion, lack of transparency, and lack of accountability.

2. The Department is unable to track requests, and measure the performance of request fulfillment, consistently across divisions.

3. Support requests that require collaboration between groups rely on informal "bridges" between the paths in this process, rather than a consistent streamlined approach. Often technicians are dispatched or solutions implemented without collaborators in other IT groups being aware.

4. Each IT group is using a mix of internal processes and tools and Department-wide tools (e.g., Remedy for ticket tracking). This prohibits the development of Department-wide best practices and consequent efficiency improvements.

5. OSHP network administrators perform a wide range of functions, but make regular visits to remote sites as their primary means of delivering support. There is no significant use of remote support capabilities (such as using Remote Desktop or other remote access technologies), nor is there policy or procedure in place to determine when such capabilities are appropriate rather than sending a technician to a remote site. As a result, it is likely that OSHP administrators are spending more time traveling, and incurring more travel expenses, than is necessary or ideal.

Procurement

IT staff across the three existing groups all purchase equipment via the State term contract and otherwise follow State procurement practices. As a result, the IT groups are taking advantage of the volume buying and economies of scale provided by these mechanisms. However, it is common for vendors to offer prices and terms more favorable than those offered in the State term contract. ODPS is often missing these opportunities because each IT group currently has its own separate purchasing authority.

Lack of purchasing coordination across ITO, EMA, and OSHP is likely resulting in purchases of equipment and software products that at best are difficult to integrate, and at worst incompatible. As a recent example, ITO has established a direction for geographic information systems (GIS) software based on a suite of Microsoft products, while EMA continues to procure products from ESRI, Inc. Staff throughout ODPS noted during site visit interviews that a significant portion of the Department's equipment is at or beyond end-of-life, without a clear refresh path in sight. Yet in other areas, equipment is refreshed on schedule. This inconsistency fails to ensure that new equipment is deployed for the highest-priority and -criticality applications, and complicates the provisioning of support.

Application Hosting and Server Provisioning

Each of the three IT groups manages some number of application servers in various locations. ITO manages the majority of the Department's servers; these host the ODPS "enterprise" applications (such as PeopleSoft, HMS Web, etc.), as well as applications on behalf of business units. OSHP manages several server environments for LEADS and other OSHP or law enforcement systems (e.g., warrants, hot files, license plate reader, etc.). These servers reside in the Shipley Building, in the main ODPS data center, but are managed directly by OSHP staff. EMA maintains its own data center at the EOC, where it maintains several servers to host EMA applications. ITO has begun moving aggressively in the direction of server virtualization, which aligns the Department with industry best practices and significantly increases flexibility and scalability while reducing power consumption. OSHP and EMA have not begun leveraging server virtualization; in OSHP's case, the principal application vendor (CPI) has advised against it, and in EMA's case, staff have determined that virtualization would not make sense given the relatively small number of servers under EMA's management.

Another example of inconsistencies in application hosting is the current approach to support and maintenance of the Department's Novell GroupWise[16] email post offices. This diagram (Figure 2) depicts the current email architecture and the email servers across the department.

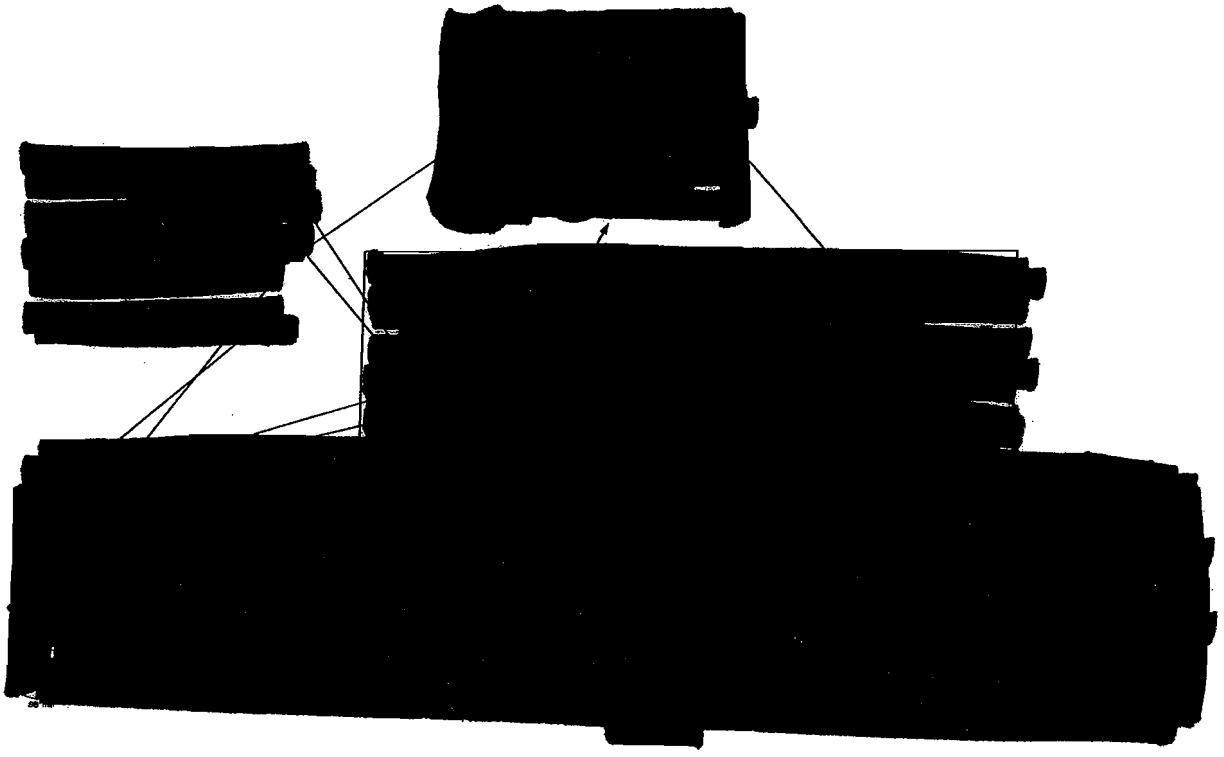

Figure 2: Current ODPS Email Architecture and Servers

In this approach, IT staff from each group are responsible for maintenance and support of the servers on which the post offices reside. This responsibility includes determining the backup approach for each post office, which includes ensuring that records are available for retrieval under state law. Often the level of record retention in each remote location is determined by the available resources at that location, rather than by a consistent Department-wide policy. As ODPS implements the provisions of HB648, which includes rules concerning records retention, this could present challenges (though the project to migrate the entire Department to Microsoft Exchange should address these challenges).

EMA also manages its own Microsoft Exchange server, which provides redundant external email connectivity to the Internet, for use in emergencies when the main ODPS email service is unavailable.

[16] For more information on Novell GroupWise, refer to: http://www.novell.com/products/groupwise/.

Security

The implementation of IT security is also spread across the three IT groups:

- **OSHP:** Network security is almost exclusively the responsibility of OSHP; its staff directly manage and control all network devices, including firewalls and routers. OSHP staff also currently perform all auditing and monitoring of the network; ensure conformance with the FBI CJIS Security Policy; manage network accounts (including email accounts) for OSHP staff; and manage user credentials for LEADS users.

- **EMA:** EMA monitors network device configurations, but delegates actual management of the devices to OSHP. EMA provisions its own user network access, manages email accounts for EMA users, and manages application-level security for EMA applications.

- **ITO:** ITO manages user credentials and email accounts for all ODPS users outside of EMA and OSHP, and provisions application-level security for applications that it hosts.

The current structure has been effective at ensuring the security of the Department's data, applications, and network. Staff reported that there have been no recent major security breaches or issues. However, the current structure presents a number of challenges to ODPS from an efficiency standpoint.

The State's IT policy, ITP-B.1, "Information Security Framework,"[17] requires each State agency to identify a "Security Point of Contact" who is "responsible for coordinating the information technology functions within the agency, and for implementing the information technology security management plan." ODPS has complied with this policy, designating an agency ISO within ITO. However, ITO staff indicated that the ISO does not have full access to resources and information at OSHP necessary to fulfill these responsibilities. OSHP staff indicated that they feel they have provided all requested access and information. SEARCH is not in a position to determine which of these points of view is correct; what is clear is that the dispersion of security responsibilities across the IT groups introduces a level of coordination and communication that consumes resources, and introduces a potential lack of accountability as to who is in charge of security.

HB648 places additional security-related requirements on State agencies. Agencies are required to log and monitor access to confidential personal information, and to retain logs for a period of time. In the current structure, demonstrating compliance with these requirements will be significantly less efficient than if security functions and records retention responsibilities were not distributed across the Department's three IT groups.

---

[17] State of Ohio, IT Policy ITP-B.1, at http://www.das.ohio.gov/LinkClick.aspx?fileticket=n%2FoeaOM9RXE%3D&tabid=107.

V. Recommendations

Based on the observations and analysis documented in **Section IV**, SEARCH staff recommends the following actions to improve IT efficiency throughout ODPS:

Recommendation 1	Consolidate ODPS IT under ITO
Recommendation 2	Capitalize on Efficiency Operations
Recommendation 3	Consolidate Network Management under ITO
Recommendation 4	Manage Organizational Change
Recommendation 5	Reorganize ITO and Emphasize Strategy and Policy
Recommendation 6	Formalize IT Governance
Recommendation 7	Formalize Service Levels
Recommendation 8	Manage Performance and Accountability
Recommendation 9	Continue Effective Practices and Efficiency Improvements
Recommendation 10	Develop and Maintain a Service Catalog

— Recommendation 1: Consolidate ODPS IT under ITO

ODPS should consolidate all Departmental IT functions under ITO, with a single streamlined reporting structure to the CIO.

To achieve this consolidation, ODPS should bring the current EMA IT and OSHP LEADS network administration and support groups into the appropriate groups that currently exist within ITO. SEARCH estimates that this would make redundant 4–5 management-level positions, which ODPS should repurpose to address currently unmet needs (see **Recommendation 5: Reorganize ITO and Emphasize Strategy and Policy** for details on the recommended new positions). SEARCH concurs with ODPS senior management's statement at the outset of this technical assistance engagement that it does not make sense to reduce overall IT staffing levels.

ODPS' first step to effect the consolidation should be to charter a consolidation project and appoint an experienced project manager to lead and coordinate the effort. Ideally, this project manager should be familiar with State government IT operations and, if possible, public safety agencies. Experience with organizational change management would be beneficial as well. The project should have the CIO and ODPS Director (or Deputy Director) as co-executive sponsors. The project manager's first task should be to develop a detailed plan for implementing this recommendation that prioritizes avoiding disruption to ongoing projects, IT support needs, and operations.

Rationale

This recommendation would likely produce the following benefits for ODPS:

1. It would achieve efficiencies in the management structure, allowing 4–5 positions to be repurposed by the organization to meet critical needs

2. It would create economies of scale that the Department does not achieve (and could not easily achieve) in the current structure. For example, positions (especially in EMA) that are "one deep" in terms of coverage could now have more substantial backup for emergencies, staff absences, etc. The organization could afford to develop staff expertise in new technical areas, as fewer staff would need to be generalists. In addition, purchasing and procurement could be consolidated across the Department, to take advantage of volume buying beyond what the State term contract can achieve.

3. It would streamline communications and decision-making authority across the currently separated IT functions. For example, communications between network administrators and computer operations staff would no longer be seen as cross-division or cross-agency communications; the managers of those groups, working under the same structure, would have common lines of authority and a closer organizational relationship. Communications could occur more frequently, and escalated issues could reach a final decision more quickly and efficiently.

4. It would streamline IT policy and procedure, and provide greater transparency and authority for policy enforcement, since direction and authority for policy would now be consolidated in the CIO.

5. It would likely improve the overall IT user/customer experience across the Department, as user-facing processes like service desk and desktop support are streamlined and consistent, and as economies of scale create the potential for improved service levels (e.g., response times). Realization of this benefit, however, requires adoption of other recommendations presented in this section, such as formalization of governance and implementation of service level agreements.

In addition to these benefits, ODPS should recognize the costs of consolidation, especially in the short term. Consolidation brings considerable organizational change and potential displacement of staff, both of which will require the attention of executive-level staff and the commitment of IT managers and business unit directors throughout the organization. There will also be costs in effecting the transition itself, such as engaging a project manager, training staff, and implementing business process changes. Subsequent recommendations propose some mitigation strategies for these issues, but the short-term costs will be real and tangible. ODPS should consider the consolidation, in the short term, as an investment in the future.

— Recommendation 2: Capitalize on Efficiency Opportunities

Assuming ODPS adopts a consolidated IT structure, as recommended, the Department should identify some "quick-win" efficiency gains and implement them within the first 6–12 months. These opportunities include:

- Consolidated procurement and volume buying.
- Streamlining the service desk and desktop support processes.
- Accelerating and reducing risk of the migration from Groupwise to Microsoft Exchange.

The CIO should be responsible for identifying tangible benefits, measuring results, and demonstrating achievement of results in the 6- to 12-month time horizon. Progress toward short-term results should be a regular topic on the agenda of the IT governance group(s), discussed in **Recommendation 6: Formalize IT Governance.**

As the three separate IT groups are consolidated into a single group, there will likely be opportunities for simplification of platforms and technologies. ODPS should utilize the services catalog (see **Recommendation 10: Develop and Maintain a Service Catalog**) to analyze what servers, databases, and other infrastructure IT should virtualize or consolidate to simplify support and maintenance.

Note that implementation of this recommendation relies on adoption of **Recommendation 8: Manage Performance and Accountability**.

Rationale

Because of the level of organizational change ODPS will experience through the consolidation, it will be important to demonstrate and communicate the benefits of consolidation to the organization. Ultimately, IT users—and especially division directors—generally see IT as a set of services, and they evaluate those services based on cost and performance. It is likely, during the consolidation, that there will be (hopefully minor) disruptions to service or changes in process that are visible to users. If costs decrease and performance increases, the perception will be that the initiative is successful, even considering the disruptions to service or current process.

It will also be important for users to understand that, while most of the benefits of consolidation will accrue in the medium- to long-term, there are some short-term benefits. Communicating these benefits will demonstrate that executive management and the IT organization are committed to service delivery and impact on users.

Additionally, aiming for quick wins will allow management to identify potential additional opportunities for efficiency improvements. For example, streamlining

the service desk and desktop support processes may identify additional redundant positions that can be repurposed to more strategic uses.

— Recommendation 3: Consolidate Network Management under ITO

ODPS should bring the OSHP and EMA network administration functions under the control of ITO.

The FBI CJIS Security Policy,[18] as well as good network security practices, require that the LEADS network (that is, the connections between LEADS users, including OSHP posts, and LEADS applications) remain separated from all other networks. A common mechanism for achieving this is to deploy a firewall between the LEADS network and the rest of the ODPS network; this firewall should control traffic between the networks, and in particular should ensure that there is no unauthorized access to LEADS applications, including NCIC, from ODPS.

To comply with the FBI CJIS Security Policy, OSHP and ODPS should jointly establish a "management control agreement," or equivalent policy,[19] which ensures OSHP remains the final authority on management and configuration of the LEADS network, while allowing ITO staff to perform configuration or other equipment changes. Under this approach, the CJIS Security Officer (CSO) at OSHP would control the access, security, and any changes of the CJIS network in cooperation with ITO. The FBI CJIS Security Policy determines what is required of a management control agreement (MCA); ODPS management should consult Ohio's copy of the policy (held by OSHP) for details. SEARCH would be pleased to place ODPS staff in touch with counterparts in other states that have implemented agreements, as well as appropriate officials at FBI CJIS should questions arise.

---

[18] Statements in this section about the FBI CJIS Security Policy represent SEARCH's best professional assessment of ODPS's options, based on SEARCH's reading of the Security Policy and the information provided during this technical assistance engagement. The FBI CJIS Division is the final authority on compliance with the Security Policy, and SEARCH urges ODPS to receive independent confirmation of any change in network configuration or architecture (including network control and management) with the FBI CJIS Division.

[19] The ODPS Chief Legal Counsel, in an interview, expressed concern with implementing "agreements" between component agencies of ODPS. As an alternative, the ODPS Director could issue a policy (with input from both ITO and OSHP) that accomplishes the same ends.

Rationale

The rationale for this recommendation is as follows:

1. By its very nature, a network is closely linked to virtually every other aspect of IT. Deploying applications, upgrading or relocating servers, installing desktops, and troubleshooting problems are only a few examples of basic IT support activities that touch the underlying network. Because of its interconnectedness with the rest of IT, network support must be closely coordinated with all other support activities.

   This requires a close collaboration between network administrators and other IT support staff, including computer operations, desktop support, and application developers. In the current ODPS environment, this collaboration is not working effectively, as indicated by nearly unanimous views of the staff interviewed during the site visit. Poor communications and lack of trust underlie the collaboration problems, but lack of clear direction and priorities from upper management is a contributing factor. Bringing network administration into ITO will give the CIO the authority and power to address the critical need for coordination between the IT support functions.

2. OSHP's and EMA's core missions are law enforcement and emergency management, respectively—not information technology. The trend in IT management across industries, and including the public sector, is for organizations to focus on their core mission and outsource non-core business processes to service providers that specialize in those processes. In interviews with ODPS executives, it became clear to SEARCH that this trend is consistent with the goals of ODPS as well.

   Clearly, OSHP continues to have a critical role in the oversight, policy-making, and control of the LEADS network. However, an alternative model that lets OSHP fulfill this oversight role while delegating the technical management of the network to ITO is not only allowed under the FBI CJIS Security Policy, but more efficient.

3. Other recommendations in this report urge ITO to continue adopting best practices of IT management, such as performance measurement and management, IT Service Management (ITSM), project management, and formalized governance. These best practices often demonstrate value only after achieving economies of scale; it is unlikely, given current staffing, that OSHP or EMA could adopt many of these best practices in isolation. Thus in the current environment, network administration may begin to fall behind in terms of best practice adoption. However, if brought into ITO, network administration could take advantage of economies of scale and leverage new practices established by the Department.

4. The recommended approach requires much less of an initial investment and significantly lower long-term costs than the January 2008 OSHP proposal to implement completely separate networks and server hosting capabilities. Among the alternatives, bringing network administration under ITO would be the quickest way to resolve current uncertainties and issues across the Department.

5. The recommended approach would allow ODPS to comply with the requirements of HB648 and State IT policy ITP-B.1 more efficiently, through closer coordination (and common authority, in the CIO) for security monitoring and auditing. Specific monitoring and auditing expectations should be detailed in the MCA—or equivalent policy—between ITO and OSHP.

While the recommendation stated above is, in SEARCH's opinion, the best option for ODPS, SEARCH recommends that ODPS review the recommendation in light of other options, such as:

- Bring network administration into ITO, but instead of implementing an MCA (or equivalent policy), change the Ohio Administrative Code (OAC) to designate ODPS as the State's CJIS systems agency (CSA) rather than the OSHP. This approach would allow ITO to administer the LEADS as the CSA's IT provider.

- Continue current OSHP management of the Department's network and LEADS. Implement an SLA between ITO and OSHP to ensure that both parties communicate and coordinate effectively, and that there is agreement on network administration service levels (such as response times for configuration changes, break/fix tasks, notification of pending changes, etc.).

- Separate the LEADS network from the rest of the ODPS network, essentially creating two duplicate networks: one for LEADS users and applications, and the other for other ODPS traffic.

— Recommendation 4: Manage Organizational Change

ODPS executive management should recognize the significant organizational change inherent in the other recommendations in this report, and as a result should work toward an environment of trust and open communication, especially with impacted staff.

As noted earlier in **Section III, Observations and Analysis**, there is currently less trust and open communication between the separate IT groups than there needs to be for effective, efficient overall IT operations. Placing the three IT groups under one management structure will not automatically solve that problem. ODPS managers, from Director Collins-Taylor to line managers, should ensure a consistent message and approach designed to break down old

interpersonal or organizational barriers and create a new, common organizational culture. With the support of the project manager engaged to plan and coordinate the transition, the ODPS IT management team (i.e., the ODPS Director, ODPS Deputy Director, CIO, and all managers in IT) should meet regularly to address organizational change issues and work together to solve problems that arise.

Firm and consistent decision-making is also important to an effective transition. Recently, executive management sometimes delayed making decisions that affect organizational boundaries (such as a decision on OSHP's network separation proposal). Regardless of the chosen path forward, managers at the appropriate level should make informed, consistent, and firm decisions that set a direction and then marshal the Department's resources behind executing them.

Rationale

The rationale for this recommendation is straightforward: Without effective management of the organizational change inherent in ODPS's future, the Department could fail to realize the benefits through reduced morale, loss of capable staff, and reduced productivity.

— Recommendation 5: Reorganize ITO and Emphasize Strategy and Policy

ODPS should reorganize ITO to accommodate the consolidation of functions and to emphasize strategy and policy.

The consolidated ODPS IT organization will employ nearly 200 staff, with the potential for 4–5 direct reports to the CIO. Given SEARCH's observation that the CIO could productively spend more time on strategic and customer-relations matters, if he had the time, it makes sense to introduce a Deputy CIO layer of two managers whose responsibility is to manage ITO, in both an operational and personnel sense, on a day-to-day basis.

SEARCH recommends that ODPS adopt a traditional IT organizational structure with Deputy CIOs for policy/strategy and operations, with these responsibilities:

- The **Deputy CIO for Operations** would focus on IT service provisioning: network administration, operations (server, storage, etc.), application development, data and information systems, service desk, desktop support, and communications.

- The **Deputy CIO for Policy and Strategy** would focus on IT policy, strategic planning, enterprise architecture, performance management, service documentation and management, project management, and customer relations and communications.

SEARCH recommends that ODPS repurpose redundant management positions to establish the Deputy CIO positions.

Figure 3 depicts a candidate[20] organizational structure for the consolidated ITO:

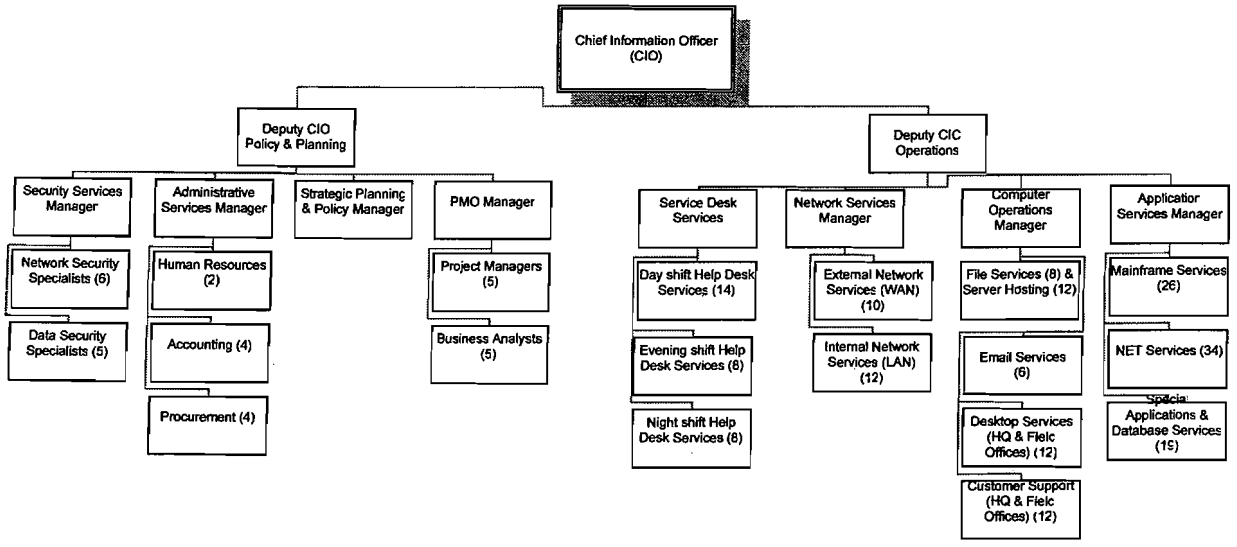

Figure 3: Candidate Organizational Structure for a Consolidated ITO

ODPS should consider maintaining a balanced organizational structure below the Deputy CIO level. When the Department combines staff from the three current groups, there will likely be opportunities to create functional groups under line managers. For example, in the organization structure shown in Figure 2, the service desk (which includes both tier-one and tier-two support) is segmented along a traditional three-shift approach, while computer operations units are organized to address specific services. A balanced approach allows grouping of staff into appropriate teams focused on a functional or service-oriented area, while also keeping the number of reports for any given manager to a reasonable level.

Rationale

The rationale for this recommendation is as follows:

1. It would free some of the CIO's time to focus more on:
   a. Direct customer contact at the division director level
   b. Effective participation in the IT governance process
   c. Greater involvement with peer agency CIOs from other State agencies (if appropriate)
   d. Setting strategic objectives for ITO
   e. Effective participation in the ODPS executive management team

[20] ODPS should consider the depicted structure below the Deputy CIO layer as an illustration of a possible structure, rather than a strong recommendation. ODPS should conduct follow-on research to determine the best management structure below the deputies.

f. Pursuing objectives, such as statewide justice information sharing, as strategic objectives for the Department.

2. It establishes IT strategy and policy as a top priority for the Department, ensuring ODPS identifies long-term efficiency measures and, where appropriate, implements them.

3. It provides explicit resources for managing and enforcing policy and procedure across the Department, including implementing the new IT governance and accountability mechanisms.

— Recommendation 6: Formalize IT Governance

ODPS should formalize IT governance by creating a committee, chaired by the Director or Deputy Director, and including the ODPS division directors as members, to oversee IT decision-making.

Generally speaking, current IT decision-making at ODPS is informal and tactical. ITO has begun to implement formal service level agreements with its customers, and has also implemented the concept of "roadmaps" that document and prioritize each customer's needs. A project manager (also known as a customer relationship manager) from ITO meets with the designated customer representative (often the division director) on a regular basis to review that division's projects and objectives, as stated on the roadmap.

In EMA, because IT reports directly to the division leadership, governance is more streamlined in the form of priorities and direction from upper management.

While the current roadmap process (supplemented by SLAs where they exist) gives ITO's customers input into prioritization of IT resources, there is currently no mechanism for Department-wide IT decision-making—especially as it relates to strategy. A committee of business unit leaders, under the overall leadership of the Department executives, would provide more formal strategic guidance and a forum for addressing issues of Department-wide concern.

It is important that the ODPS IT governance committee remain focused on strategic, Department-wide objectives, rather than directly impacting or influencing the business operations within a division. The IT governance committee should also not be a mechanism for dictating to the CIO how he or she operates the IT function. The committee should include on its agenda strategic topics, such as the following:

- Establishing baseline or standard service levels for IT services consumed across the department
- Determining funding models for Department-wide IT services
- Reviewing planned changes to Department-wide IT services and assisting the CIO in assessing the impacts of changes

- Establishing priorities and resolving tradeoffs between competing division priorities
- Advising the CIO on Department-wide IT policy and standards issues
- Reviewing and contributing to the Department's IT strategic plan
- Supporting the IT accountability process (**Recommendation 8: Manage Performance and Accountability**).

Rationale

The rationale for this recommendation is as follows:

1. It provides a forum in which business unit leaders have a formal voice in setting IT strategy. This benefits the CIO by providing direct input from his customers, in a forum where competing priorities are recognized and resolved. It creates a sense of joint accountability for the strategic direction of IT—as a partnership between the CIO and business units.

2. It focuses the Department's leadership, even for a few hours each month, on how they are collectively using IT, and how they could be using it more efficiently.

3. It tends to improve trust, accountability, and transparency in making significant IT investment and policy decisions.

— Recommendation 7: Formalize Service Levels

ODPS should continue recent initial efforts to establish service level agreements—SLAs—for IT services.

The objectives of an SLA are to define, document, measure, and report service levels with the goal of continued improvement of services and customer satisfaction with the quality of the services. It is through the SLA that a business unit leader can express specific requirements and hold ITO and the CIO accountable for delivering services that meet those requirements. SLAs generally include measurable, objective criteria of satisfactory performance, so that it can be objectively clear whether ITO is meeting the required levels or not.

As noted in **Section IV, Observations and Analysis**, SEARCH found during this engagement that EMA and OSHP do indeed have unique requirements. While not a specific focus of investigation, it is likely that each business unit at ODPS has similar unique requirements. However, all ODPS business units share common needs and requirements as well, thus justifying the pooling of resources and economies of scale that centralized IT provides.

As a first step in moving toward ubiquitous SLAs at ODPS, each division director should meet with his or her staff to begin documenting specific needs and requirements for IT. These requirements will form the core of each division's

SLA with ITO. It is important that these requirements specify what the division needs, not how the service should be provided. Functional requirements—what the service does—as well as non-functional requirements—supporting characteristics of the service, such as reliability, availability, location/deployment requirements, etc.—should be included.

Over time, as divisions complete their own SLAs, it will become clear that some services have common, baseline service level requirements and consistent functionality across the Department. Email and telephony are perhaps good examples—with a few exceptions, these services have mostly the same requirements everywhere. As these "common" or "shared" services are identified, the IT Governance Committee can officially designate them as such, and the Department can migrate to a shared or common SLA for those services.

As ODPS begins to implement SLAs, the IT Governance Committee should begin regular reviews of performance against service levels. See **Recommendation 8: Manage Performance and Accountability** and **Recommendation 6: Formalize IT Governance**.

Rationale

The rationale for this recommendation is as follows:

- SLAs are a key component of accountability and ensuring that business unit leaders remain in control of IT requirements. SLAs allow business unit leaders to specify what they need, while allowing ITO to determine how to fulfill that need in the most efficient manner possible.
- SLAs allow ODPS to recognize, through a formal process, which services are truly shared and common.
- SLAs provide business unit leaders with a formal process for articulating the unique aspects of their business and how IT must support those needs.
- SLAs can streamline communications and build trust and confidence.

— Recommendation 8: Manage Performance and Accountability

ODPS should improve its ability to measure the performance of IT services and use the resulting data to demonstrate adherence to promised service levels.

It is a well-known adage of management that "you have to measure it to manage it." This is as true for IT as for any other area of a business. Throughout these recommendations, SEARCH is suggesting that ODPS implement a more formal, structured approach to IT, with negotiated and established service levels for well-defined IT services. This mechanism, through which business unit leaders can be assured of receiving the IT services they need to fulfill their missions, is a foundational premise of consolidation. Without measurable and meaningful

accountability, division directors could hardly be faulted for viewing consolidation as a risky loss of control.

Considerable literature exists on the measurement of IT performance, and this report will not attempt to summarize this literature. As part of the consolidation project, ITO should task a project manager with conceiving and leading a project to identify and implement performance measures, starting with the most critical IT services. This project should be provided with adequate resources to complete the task, and should receive the support of the CIO in instrumenting or even adjusting IT processes to ensure that service levels can be measured.

As a guideline, the IT Infrastructure Library (ITIL) suggests the following steps to the effective measurement of IT service performance:[21]

- **What should you measure?** – Define what ideally should be measured.
- **What can you measure?** – Define what can be measured. These are the business requirements.
- **Gather data** – Verify whether the goals and objectives are being met.
- **Process data** – Translate the data into a depiction of the service performance set by the business.
- **Analyze data** – Understand the area for improvement.
- **Present and use information** – Report the information so that it can be used to make strategic, tactical, and operational decisions.
- **Implement corrective action** – Set priorities that align with the organizational goals and start the process over for continued improvements.

Two examples of the need for better measurement became clear during the site visit:

- Across the three existing IT groups, managers do not account for personnel time as a billable resource. Accounting for staff time spent on projects and tasks allows managers to calculate labor costs and can show exactly where within a project staff are spending time. An analysis of actual time required to complete the various tasks in a project proves very useful in improving future project estimations.

[21] *Foundations of IT Service Management Based on ITIL® V3*, published by Van Haren Publishing and part of the ITSM library.

- There does not seem to be systematic analysis of the data in Remedy, the Department's ticket/issue tracking system. The data in this system could provide a wealth of information regarding service desk responsiveness, as well as information on where events and incidents are manifesting as persistent problems. Talented and attentive staff can often sense these issues without formal data analysis, but diagnosis of systemic problems and understanding the performance of the service desk become much easier with formal data analysis and reporting.

In addition to monitoring performance, ODPS should adopt a formal accountability process. Since for the foreseeable future ODPS will not (and, in SEARCH's view, should not) implement a fee-for-service model for IT, the Department should implement an alternative mechanism to hold ITO accountable for IT performance. The Department should implement such a mechanism in a spirit of teamwork and collaboration, recognizing that everyone has a stake in successful IT services, but at the same time recognizing that the CIO's job is to ensure that IT services are available and performing in accordance with promised service levels.

SEARCH recommends that ODPS leverage the IT Governance Committee (see **Recommendation 6: Formalize IT Governance**) to provide a forum for regular review of IT performance. The CIO and Deputy CIO for Policy and Strategy should prepare for each meeting of the committee by compiling data on service-level performance. Business unit leaders know well in advance which services are to be examined at any given meeting. Based on the data analysis, the CIO and business unit leaders engage in a dialogue concerning performance—whether the measures still make sense, what the numbers (good or bad) indicate, and what mitigating factors exist (extraordinary circumstances, funding changes, staffing issues, etc.). The committee would then use the forum to work together on problem solving to address any performance shortfalls or changes to the performance management mechanism itself.[22]

Rationale

The rationale for this recommendation is straightforward. Accountability based on objective, measured performance is a key element of establishing trust and confidence that the IT needs of business units will be met.

---

[22] This kind of government accountability mechanism has been implemented in several jurisdictions. For examples, see:

- http://en.wikipedia.org/wiki/Compstat
- http://baltimorecity.gov/Government/AgenciesDepartments/CitiStat.aspx
- http://www.accountability.wa.gov/.

— Recommendation 9: Continue Effective Practices and Efficiency Improvements

ODPS should continue investing in projects and practices that will improve the efficiency of IT service delivery.

ITO has initiated migration projects to move applications off the mainframe platform and consolidate email on Microsoft Exchange, the primary email platform in State government. Both of these projects will very likely reduce long-term costs and improve service levels. These projects should continue through to completion.

In addition to implementing SLAs, ITO has also introduced other known best practices of IT management. It has established a Project Management Office and staffed it with several capable project managers, who also serve as customer relations managers. ITO has established the Project Management Institute standards and certifications in the PMO, and seeks to use a consistent PMI-conformant project management approach on every project.

ITO should continue leveraging defined, disciplined approaches to project management. However, it is important to recognize that project management approaches should scale to fit the scale of the project. It is common for PMI-certified project managers to treat all projects the same, requiring the same level of formalism, documentation, and "ceremony" regardless of size. It is by no means clear that ITO has fallen into this trap, but it is an issue that requires constant vigilance. ITO should consider adding agile project management techniques and development methodologies to its toolkit. Agile methodologies focus on performing the minimum amount of project management overhead consistent with the risk and scale of the project. They also focus on maintaining intense levels of discipline across a project team, and involving business customers early and often in steering a project. Agile projects are typically smaller and more focused, allowing greater opportunity for course corrections.

Rationale

The rationale for this recommendation is straightforward: ODPS should continue with efforts aimed at improving efficiency.

— Recommendation 10: Develop and Maintain a Service Catalog

ODPS should create and maintain a catalog of IT services. The catalog should document the important features of each service, including the service's functionality, service levels, IT point of contact, current version, and expected changes to the service.

As part of this technical assistance engagement, SEARCH has provided a start at a service catalog, which ODPS is free to use as it sees fit. The catalog, in Excel format, has been attached (electronically) to this report.

Rationale

A service catalog provides the ability to contain critical information about the services in a central repository accessible by both the IT department and customer business units. It serves as a focal point for IT, users, and the IT Governance Committee when discussing services; it provides a common vocabulary and an accessible statement of current service functionality and service levels.

VI. Conclusion

This report has attempted to document the SEARCH team's observations, analysis, and recommendations regarding IT efficiency at ODPS.

This is a time of significant change for the Department, with new leadership at the very top of the organization, and renewed energy for achieving new levels of operational efficiency. One thing is very clear—to the SEARCH team and, it seems, to each ODPS staff person interviewed as part of this engagement: Technology is absolutely essential to the delivery of public safety services to the public. That essential element of the public safety mission—delivering the right information and applications to the right practitioners at the right moment, reliably, securely, and quickly—continues to be dependent on the effective and strategic use of technology.

SEARCH commends ODPS for recognizing this critical component of the public safety mission, and for challenging itself to become more efficient in its delivery.

The central recommendation of this report—the consolidation of IT services—will not be easy, on a number of levels. ODPS should not underestimate the challenge, in terms of technology, business process, personnel management, and funding. Some wins will probably come quick, but others will take time to materialize. Executive management should be patient, attentive, and consistent in the direction set and the message sent to stakeholders: Moving to a new level of efficiency is important to ODPS, the Legislature, the Governor, and the practitioners and public that the Department serves.

SEARCH has attempted to provide insights and tools that ODPS can use in effecting this transition to a consolidated IT environment. The Department should know that SEARCH is always here to assist in whatever way possible. Specifically, SEARCH would be pleased to assist with implementing some of the recommendations in this report. For example, SEARCH could assist with chartering the IT Governance Committee and facilitating its first meetings; SEARCH could also assist with developing model SLAs and performance measures, or setting up the accountability process.

Should ODPS wish to take advantage of SEARCH technical assistance in the future, feel free to contact either of this report's authors directly, or SEARCH generally at http://www.search.org.

It has been a pleasure working with the dedicated, professional staff at ODPS. Best wishes as you move forward with improving IT efficiency.

Appendix A: About SEARCH, the National Technical Assistance Program, and the Project Team

SEARCH, The National Consortium for Justice Information and Statistics

SEARCH, The National Consortium for Justice Information and Statistics, is a nonprofit membership organization created by and for the states, dedicated to improving the quality of justice and public safety through the use, management, and exchange of information; application of new technologies; and responsible law and policy, while safeguarding security and privacy.

SEARCH's primary objective has been to identify and help solve the information management problems of justice and public safety agencies confronted with the need to automate and integrate their information systems and to exchange information with other local agencies, tribes, state agencies, agencies in other states, or with the federal government.

SEARCH is governed by a Membership Group comprised of one gubernatorial appointee from each of the 50 States, the District of Columbia, Puerto Rico, and the Virgin Islands. Members are primarily state-level justice officials responsible for operational decisions and policymaking concerning the management of criminal justice information.

A staff of professionals works from SEARCH headquarters in Sacramento, California, to implement solutions identified by the Membership Group. SEARCH provides justice and public safety agencies with diverse products, services, and resources through four focus areas: Systems and Technology, Criminal History Law and Policy, High Technology Crime Investigation, and Public Safety.

SEARCH:

- Is the national provider of no-cost technical assistance to address the specific needs of operational state and local justice and public safety agencies in the process of acquiring, developing, upgrading, or integrating their computer and communications systems.
- Offers hands-on training to local, tribal, state, and federal agencies on computer technology issues with criminal justice and homeland security applications. Courses are offered on such topics as investigating computer crime, cellular device investigations, network investigations, and online child exploitation investigation.
- Prepares police, fire, and EMS agencies for successful technology projects through the Public Safety Program.
- Sponsors national conferences, symposia, and workshops for local, tribal, state, and federal justice practitioners.
- Prepares national research, analytical, and survey reports and bulletins on a range of timely issues in criminal justice information management, technology, and law and policy, which are published and disseminated by the U.S. Department of Justice and U.S. Department of Homeland Security.

- Provides a wide variety of information about justice information systems, related technologies, standards, research, and technology acquisition via the Internet. A wide range of resources can be accessed via the SEARCH home page at www.search.org.

The National Technical Assistance Program

The National Technical Assistance Program, administered by SEARCH with funding from various agencies within the U.S. Department of Justice and U.S. Department of Homeland Security, provides no-cost assistance to all components of the state and local criminal justice system with respect to the development, operation, improvement, and/or integration of all types of criminal justice and public safety information systems (for example, records and case management, computer-aided dispatch, and criminal history record systems, etc.). The Technical Assistance Program includes both in-house and on-site technical assistance:

- In-house technical assistance includes consultation with agencies via telephone, mail, and Internet. These technical assistance projects can include consultations and information about automation, integration, communications interoperability, and planning issues, as well as review of agency automation/integration planning materials, needs assessments, data modeling, and requests for proposals.

- On-site assistance helps agencies in their efforts to effectively plan for, design, develop, procure, and implement computerized information systems, and can involve the following: conducting needs assessments, identifying system requirements, and developing or reviewing site-specific planning documents; planning projects to achieve integration of information systems across functional and/or political boundaries; assistance in writing technical proposals; providing technical consultations on a wide range of operational and policy issues; proposing solutions to system problems; locating expertise and information systems for transfer; and guiding the transfer and implementation of systems and techniques to improve information management.

Project Staff

Mr. Scott M. Came is Director of Systems and Technology for SEARCH, The National Consortium for Justice Information and Statistics, where he develops and directs activities and manages staff under the National Technical Assistance Program, a multifaceted program of information technology services for the nation's justice and public safety communities to assist their efforts to develop, operate, secure, and improve information-sharing and identification systems, and to achieve interagency data exchange. These services include technical assistance, training, and conference and workshop development.

Mr. Came is a recognized expert in enterprise architecture and information sharing architecture. He has served as the editor and architecture advisor to the Global Infrastructure/Standards Working Group (GISWG) Justice Reference Architecture (JRA) initiative. He developed a service-oriented integration architecture (SOA) for state

government in Washington, and has helped several clients define and implement SOA in his position at SEARCH. His expertise focuses on the strategic planning and policy implications of technology architecture.

Mr. Came manages SEARCH's Justice Information Exchange Model (JIEM) Program, which shows practitioners how to establish a solid foundation for their information sharing projects by modeling exchange requirements—the who, what, when, and why of information exchange. Practitioners apply the JIEM methodology by using JIEM software and JIEM reference models, both of which allow for efficient modeling of complex requirements while aligning models with national best practices. Mr. Came also oversees SEARCH's justice XML initiatives, and SEARCH's role in the implementation of the National Information Exchange Model (NIEM).

Mr. Came is an experienced technology leader with over 11 years of progressive experience and a solid track record of success on more than 20 enterprise software development projects. He is experienced in planning and leading criminal justice systems integration projects; strategic planning and performance measurement; developing SOA and enterprise architecture; development with XML and Web services technologies; and software project management.

Mr. Came has extensive experience leveraging technology to improve justice information sharing. He participated in the initial beta testing of the Global Justice XML Data Model (GJXDM) and has participated in refining its overall architecture. He has provided technical assistance to state and local justice integration initiatives, has served as an instructor in national GJXDM trainings, and has spoken on GJXDM and technical architecture at conferences and symposia. He led the development of Information Exchange Package Documentation for Amber Alerts and Incident Reports, as well as the OASIS Electronic Court Filing 3.0 specification. He is a member of the GISWG and is actively involved in its effort to define a reference SOA for justice integration.

Prior to joining SEARCH, Mr. Came was Chief Enterprise Architect for the Washington State Department of Information Services. He also previously was President and Principal Consultant for Justice Integration Solutions, Inc.; Enterprise Architect and Development Manager for the Washington Administrative Office of the Courts; a technology consultant for ANZUS Technology International and Puget Sound Systems Group; and an instructor at the University of Washington–Seattle's Educational Outreach Java Certificate Program.

Mr. Came has a bachelor's degree in Economics from Georgetown University, graduating Phi Beta Kappa and summa cum laude. He is a Sun-certified Java programmer, a Certified ScrumMaster, and has achieved SEARCH JIEM Certification.

Mr. Michael Jacobson is a Justice Information Systems Specialist for SEARCH, The National Consortium for Justice Information and Statistics, where he provides assistance on integrated justice systems project planning and implementation. He provides training,

technical assistance, and research on automated systems development, automation planning, and justice information sharing to state, local, and tribal jurisdictions nationwide.

Mr. Jacobson has 20 years of networking, database programming, user support, administration and project management experience, with expertise in XML, business process modeling, and service-oriented architecture. Prior to joining SEARCH in 2009, he worked for the Montana Department of Justice (DOJ), most recently as an Information Technology Project Manager. In this position, he was responsible for coordinating and completing multiple simultaneous projects, including managing project scope and timelines, developing project and communications plans, providing risk assessments, developing policies, standards and procedures, conducting business process analysis, and reporting to project sponsors, stakeholders, and team members. He managed the statewide Integrated Justice Information Sharing (IJIS) Broker program, which is creating the information exchanges that allow a wide range of agencies (such as courts, jails, prisons, police, sheriffs, motor vehicle division, etc.) share real-time information quickly, securely, and accurately.

Mr. Jacobson also served as Chief of the Montana DOJ's Application Services Bureau for more than 3 years, which assists the department in planning, developing, and maintaining automated information systems. He oversaw the work of web developers, programmer/ analysts, systems analysts, and database administrators, and also participated in long-range planning and coordinating development projects. He worked with IT managers statewide on enterprisewide strategic planning, standards, and policy issues as Executive Chairman of the Montana Information Technology Managers Council, an advisory group to the state Chief Information Officer.

He also served as a System Analyst for the Montana Department of Agriculture for five years, where he was responsible for meeting its IT needs, including user support and training; network and server administration; and programming large and small database projects. He previously worked for MoreWire, Inc., as Vice President of Information Systems; Hydrometrics, Inc., as Senior Systems Specialist; and as an Information Service Specialist for state Office of Public Instruction, all based in Helena, Montana.

Mr. Jacobson has a bachelor's degree in Computer Science from Carroll College.

Ms. Alecia Webb-Edgington is a Public Safety Technology Specialist for SEARCH, The National Consortium for Justice Information and Statistics. She provides technical assistance to local, county and state public safety agencies nationwide that want to develop, improve, acquire, and achieve integration and interoperability of information technology, including radio communications, computer-aided dispatch (CAD), records management (RMS) and mobile data systems.

Ms. Webb-Edgington joined SEARCH in 2008 following a successful career of state-level leadership and experience in the public safety realm, most recently as Executive Director of the Kentucky Office of Homeland Security (OHS), a position she held from 2005–07. Prior

to that, she served in the Kentucky State Police (KSP) for 15 years, rising in the ranks from Trooper to Major for the Technical Services Division before retiring in October 2005. In between, she held such positions as Detective (child sexual abuse investigations, street-level narcotics, drug enforcement and special investigations); Executive Security; Sergeant, Operations Division; Squad Sergeant; Assistant Commander, Recruitment; Commander, Criminal Identification and Records Branch; Chief Information Officer, Technical Services Division; and as the appointed Deputy Director of Operations and Prevention for OHS. She began her career as a Deputy Sheriff in Edmonson County, Kentucky, serving from 1985–89.

While at KSP, she led various project implementations for the Commonwealth of Kentucky, including a statewide CAD, interoperable communications solutions, mobile data network and design and development of an RMS for law enforcement agencies. She has managed the full life cycles of these projects, and therefore has a deep understanding of how to utilize technology in order to deliver enhanced services for first responders.

Since January 2008, Ms. Webb-Edgington has been an elected member of the Kentucky House of Representatives, representing the 63rd District. She earned a bachelor's degree in sociology/criminology from Western Kentucky University and a master's degree in criminal justice from Eastern Kentucky University. Her post-graduate studies include the 52nd Annual National Security Seminar at the U.S. Army War College and the Executive Leadership Program at the Naval Postgraduate School, Center for Homeland Defense.

Ms. Webb-Edgington served as Kentucky's gubernatorial-appointed representative to the SEARCH Membership Group from 2002–06, and she was elected to the Board of Directors in 2004. She also served as secretary/treasurer and president of Kentucky Women in Law Enforcement, and is a past member of the National Governors' Association Homeland Security Advisory Council. She is a recipient of numerous honors and awards, including the KSP Commendation for Outstanding Achievement, and the Best of Kentucky 2007 IT Champion Award, given by the Commonwealth Office of Technology.

Appendix B: ODPS Services Inventory: Spreadsheet

Attached electronically in Excel spreadsheet form

Appendix C: List of Documents Reviewed

File name	Description
SEARCH Agenda _2.doc	Meeting agenda for the site visit (see Appendix D)
ODPS Infrastructure document.docx	Overview of ODPS services
OSHP IT Overview.doc	Overview of OSHP services
SEARCH Requested Documents -EMA.docx	Overview of EMA services
LEADS Isolation IOCs.zip	Inter-Office memos regarding LEADS
800.01.pdf	Policy from ITO - Use of Email, Internet and Other Resources
800.02.pdf	Policy from ITO - Management of Hardware and Software
800.03.pdf	Policy from ITO - Internet Security
800.04.pdf	Policy from ITO - Internet / Intranet
800.05.pdf	Policy from ITO - Security of Computer Networks
800.06.pdf	Policy from ITO - Remote Access Security
800.07.pdf	Policy from ITO - Virus Protection
800.08.pdf	Policy from ITO - Information Technology Plan
800.09.pdf	Policy from ITO - Computer Network Boundary Protection
800.10.pdf	Policy from ITO - Password and PIN security
800.11.pdf	Policy from ITO - Wireless LAN security
800.12.pdf	Policy from ITO - VPN Access
800.16.pdf	Policy from ITO - Portable Computer Security
800.17.pdf	Policy from ITO - Security Notifications
801.02.pdf	Policy from ITO - Accessing Confidential Personal Information
802.01.pdf	Policy from ITO - Computer Room Access
091208_HB648.mpp	Project Plan for House Bill 648 implementation
091208_HB648_App_List.xls	List of applications affected by HB648
Additional MS Migration Project info for SEARCH.ppt	Information regarding the project to migrate from Novell to Microsoft
ATPS 2004 RFP 0A05010 - 04-15-05 1715.pdf	RFP for the Titling system from 2004
Add_t Info on Development and Software Licenses.docx	List of software used by the ITO development team
ATPSIII.mpp	Project Plan for upgrading the ATPS (Titling System)
attachment B - EMA .pdf	EMA Network Diagram
attachment c - server list.xls	List of EMA servers
C_ODPSCodingStandards.pdf	C# coding standards

Change Control System.doc	User documentation for the Change Control application
Contracts Unit Procedures.pdf	Procedures for the contract process
Direct Purchase FlowChart.pdf	Flowchart of purchasing procedure
Direct Purchase Procedures.pdf	Purchasing procedure
DPS EA_6184046_12-1-09clean.xls	Microsoft Enterprise Agreement spreadsheet
DPS Select_3305629_12-1-09clean.xls	Microsoft Select Agreement spreadsheet
EMA Reqs for EMA Review Response by Morrill.xls	EMA Requirements for Network Administration
Exodus Phase 1.mpp	Project plan for migrating off of the mainframe
HB0648EN.pdf	Language from HB648
ITO Budget.xlsx	ITO Budget
Major Acquisition FlowChart.pdf	Major Acquisition Purchasing Procedure Flowchart
Major Acquisition Procedures.pdf	Major Acquisition Purchasing Procedures
MS Migration Project Estimated Timeline for SEARCH.ppt	Information regarding the Microsoft Migration Project Estimated Timeline
OAC123-3-1-01.pdf	Electronic signature law
ODPS MS Migration Plan Info for SEARCH.doc	Microsoft Migration Plan
ODPS Coding Standards.doc	ODPS website Coding Standards
OH org charts 20091210130303.pdf	ODPS Organization Charts
OhioOIT Policies.zip	IT Policies from the State CIO
Ohio_Interop_Appendices.pdf	Ohio Interoperability Report
OSHP Inventory of Hardware (excluding PCs).doc	Inventory of Servers, etc. that the Highway Patrol is responsible for
OSHP IT Overview of Services.ppt	Presentation of OSHP IT Services
Production Database Special Access Request.doc	Production Database Special Access Request Form
PROJ-CTL 1209.DOC	Overview of the Project Tracking system
Regular & Personal Service Contract Flow Chart.pdf	Flowchart for the Regular and Personal Service Contract
RFQ 09-122 EMS DATABASE - System Analyst 101408.doc	Request for Quote for a System Analyst for EMS
Security Technologies Used.doc	List of Security Technologies Used by ODPS
SLA EMS.pdf	Service Level Agreement between ODPS IT and EMS
SLA OIU.pdf	Service Level Agreement between ODPS IT and OIU
standards.docx	.NET development standards for ODPS
WCFRouterService.doc	Information about Windows Communication Foundation Router in an SOA environment

Appendix D: Site Visit Agenda and Participants

January 5, 2010 — *Orientation Meetings*		
8:00 – 8:30 am	ODPS Director Cathy Collins-Taylor, Assistant Director George Maier, Executive Director of Administration Larry McCartney	Director's Office
8:30 – 9:30 am	Jeff Clouse, Keith Albert, Dave Brown, Brent Rawlins	327C
10:00 – Noon	EMA – Mark Patchen, Mark Morrill	327C
Noon – 1:00 pm	LUNCH	
1:00 – 3:00 pm	OSHP – S/Lt. Jim Hamilton, Jeremy Hansford, Jeremy Ebert	327C
January 6, 2010 — *In-Depth Meetings*		
8:30 – 11:30 am	EMA – Executive Director Nancy Dragani, Mark Patchen, Mark Morrill	@ EMA
11:30 am – 1:00 pm	LUNCH	
1:00 – 4:00 pm	ITO – Brent Rawlins, Michele Croghan, George Dotson, Jeff Coffey, Rod Ehrman, Dave Brown, Jeff Clouse, Keith Albert	T3-7
January 7, 2010 — *In-Depth Meetings (Cont.)*		
8:00 – 11:30 am	OSHP – Capt. Tom Dean, S/Lt. Jim Hamilton, Jeremy Hansford, Jeremy Ebert	Centre School Conference Room
11:30 am – 1:00 pm	LUNCH	
Individual Meetings		
1:00 – 1:30 pm	ODPS Director Cathy Collins-Taylor	Director's Office
1:30 – 2:00 pm	ODPS Assistant Director George Maier	Director's Office
2:00 – 2:30 pm	ODPS Chief Legal Counsel Josh Engel	Legal
2:30 – 3:00 pm	Karhlton Moore – Executive Director, OCJS	OCJS
3:00 – 3:30 pm	Carolyn Williams – Acting Registrar, BMV	BMV
3:30 – 4:00 pm	William Vedra – Executive Director, OHS	OHS
January 8, 2010 — *Close-Out Meetings*		
8:00 – 9:00 am	Dave Brown, Chief Information Security Officer	PLAN311
9:00 – 10:00 am	Infrastructure – Brent Rawlins, Michele Croghan, George Dotson	PLAN311
10:30 – 11:00 am	OSHP – Interim Superintendent Kevin Teaford, Capt. Tom Dean, S/Lt. Jim Hamilton	PLAN311
11:00 am – Noon	Networking – S/Lt. Jim Hamilton, Jeremy Hansford, Jeremy Ebert	PLAN311
Noon – 1:00 pm	LUNCH	
1:00 – 4:00 pm	Jeff Clouse, Keith Albert	327C

Appendix E: Factors Influencing the Interpretation of Staffing Ratios[23]

[23] Source: http://coastaltech.com/hd-staff.htm.

Consideration	Support Staff Levels
Experienced support staff	Decrease
Customer handling expertise	Decrease
Large number of products to support	Increase
Multiple shifts and weekends	Increase
Support staff possesses knowledge of the organization's business	Decrease
Internal support only	Decrease
External support only	Increase
Both internal and external support	Increase
Service Level Agreements negotiated	Decrease
Budget concerns	Decrease*
Multiple platforms to support (Web, PC, Mainframe, Mac)	Increase
Automated tools in place	Decrease
Experienced support center management	Decrease
Support center has good reputation in company	Decrease
Center has bad reputation	Increase
Multiple support center locations	Increase
Quality Assurance or Quality Control responsibility	Increase
Proactive support philosophy	Increase**
Support center has additional responsibilities not listed above	Increase

** A staffing decrease may be required to meet your budget, but too small a staff can create bigger problems later on – dissatisfied customers, excessive stress, technician burnout, and high turnover to name a few.*

*** Initially, proactive support requires more staff per customer. The trend is reversed down the line, as you should see a decrease in customer problems.*