

# **Law Enforcement Consolidation Task Force**

## **Information Technology Services Workgroup**



**DRAFT REPORT**

June 6, 2012

## CONTENTS

1. EXECUTIVE SUMMARY .....	3
2. WORKGROUP CHARTER .....	5
3. TECHNOLOGY NEEDS OF LAW ENFORCEMENT.....	6
4. CHALLENGES OF CURRENT CONSOLIDATION FRAMEWORK.....	7
5. LE TECHNOLOGY SERVICE CENTER – THE VISION .....	10
6. LE TECHNOLOGY SERVICE CENTER - PHASED IMPLEMENTATION .....	11
7. LE TECHNOLOGY SERVICE CENTER - HOST SITE SELECTION.....	12
8. CRITICAL SUCCESS FACTORS .....	12
9. RECOMMENDATION AND CONCLUSION .....	14

## 1. EXECUTIVE SUMMARY

The Law Enforcement Consolidation Task Force established this workgroup to provide additional information and recommendations related to a dedicated state law enforcement IT service center to assure the security and operational integrity of critical law enforcement (LE) systems and data, to promote public safety services across the state, and enhance officer safety through secure and reliable technology service delivery throughout Florida. The workgroup consisted primarily of LE information technology (IT) staff and non-IT staff with experience in technology issues. The workgroup findings focused on four major areas: the technology needs of law enforcement, challenges of the current consolidation framework, consideration for the establishment of a dedicated LE Technology Service and Support Center (Center), and critical success factors for establishing such a Center.

Today, law enforcement relies heavily on individual officers and supporting personnel having 24 hour access to computer systems, network connectivity and data sharing repositories. Immediate and remote identification and data access, geospatial functionality, digital video technologies, and remote records access have all become critical 24x7x365 technologies. Support systems such as computer aided dispatch (CAD), records management systems (RMS), state and federal criminal history data (FCIC/NCIC), and radio and telephone systems, are all critical components of the law enforcement infrastructure. Temporary loss of access to any one of these systems or subsystems may hinder law enforcement and jeopardize officer and public safety.

The current effort to consolidate the numerous Florida state government data centers is justified from a financial perspective. However, it is the general consensus within the LE IT community that the current Data Center Consolidation (DCC) initiative introduces unacceptable risk for law enforcement and the citizens of the state of Florida.

The workgroup identified many potential sources of risk that exist in the current state data center system, as evidenced by experiences such as extended downtime, insufficient security management, insufficient backup of servers, and operational schedules inconsistent with the needs of law enforcement IT.

One alternative to the current approach is the establishment of a dedicated LE Technology Service and Support Center, hosted and managed by a law enforcement agency. Beyond a “data center”, this Center would ultimately host centralized systems and shared data, as well as support all of the devices and technology critical to the core mission of law enforcement. It would also provide co-location services to law enforcement agencies, to allow them to house non-LE systems that are not centrally hosted and managed, but that need ongoing support of the participating LE agency. The scope of participation, or nonparticipation, by an agency with an LE function would be considered and determined during the initial planning phase of the project to determine if participation is warranted. Implementation of the Center would be phased and carefully managed, with consideration for critical success factors including but not limited to those identified by the workgroup.

The workgroup makes the following recommendations:

1. Postpone any further data center consolidation of LE agencies.

2. Proceed with initiation of a project to establish a Law Enforcement Technology Service Center as described in this report.
3. Commit upfront and ongoing resources needed to ensure the mission of law enforcement is not compromised, even if the ultimate result of the consolidation does not achieve maximum cost savings.

We strongly support the efforts to consolidate data centers across the State as an effective way to decrease costs and improve service in some agencies. However, given the unique level of service required by LE agencies, and the high level of risk that currently exists in the data center consolidation model, we believe it is prudent for the State to move forward with the above recommendations.

## 2. WORKGROUP CHARTER

In 2011, Senate Bill 2160 created the Law Enforcement Consolidation Task Force (LECTF or Task Force). One of the teams established by the LECTF was the Information Technology (LECIT) Team, whose original charter was to review and assess the existing law enforcement (LE) information technology (IT) environment and to identify possible efficiency and consolidation opportunities. The Team membership included all state agencies with a law enforcement component.

The LECIT Team Report identified ways that the LE community has proactively worked to achieve efficiencies of centralization and consolidation of technology services. The Team documented success stories as well as additional opportunities for service consolidation, primarily through consolidation of application systems and the related business processes. The report also included major critical success factors for consideration in future consolidation initiatives, including assessment of the current Data Center System. The LECIT Team Report dated November 7, 2011 summarizes the Team's findings.

To identify further efficiencies and economies, the Task Force subsequently established the Law Enforcement IT Services (LEITS) Workgroup. The workgroup consisted primarily of LE IT staff or non-IT staff with experience in technology issues, and focused on the perspective of the LE IT community regarding data center consolidation.

### **Scope:**

The scope of the LEITS workgroup is to identify additional enterprise efficiencies related to LE information technology. The primary objective is to provide the Task Force with additional information and recommendations related to a dedicated state law enforcement IT service center to assure the security and operational integrity of critical LE systems and data, to promote public safety services across the state, and enhance officer safety through secure and reliable technology service delivery throughout Florida.

Specifically, the LEITS Workgroup considered:

1. The technology needs specific to the law enforcement functions within state agencies
2. Challenges to meeting these needs under the current technology consolidation framework
3. Consideration of a technology service center whose mission would be focused solely on the management, support and security of law enforcement systems and data
4. Critical success factors in establishing such a service center

The scope of the Workgroup did not include development of a project planning document or project charter, and this resulting report is not intended as such.

### Out of Scope:

The Florida Department of Law Enforcement has been exempted from state data center consolidation and is not within the scope of the law enforcement technology service center being considered by this workgroup. FDLE Information Technology staff did participate as members of the workgroup.

## 3. TECHNOLOGY NEEDS OF LAW ENFORCEMENT

Technology has become an essential integrated component of law enforcement operations, critical to the success of the mission of public safety, public service, and enforcement of state and federal laws. The use of technology extends and multiplies the capabilities of our law enforcement officers and agencies, improving their ability to promote public safety, enforce laws, maintain order, educate, protect and serve the citizens of Florida.

Today, law enforcement relies heavily on individual officers and supporting personnel having access to computer systems, network connectivity and data sharing repositories 24 hours a day, every day of the week (24x7x365). Support systems such as computer aided dispatch (CAD), records management systems (RMS), state and federal criminal history data (FCIC/NCIC), and radio and telephone systems, are all critical components of the law enforcement infrastructure. Temporary loss of access to any one of these systems or subsystems may hinder law enforcement and jeopardize officer and public safety.

Examples of the myriad of ways that technology aids LE in achieving their mission and saving lives are:

- **Remote Identification and Data Access:** Online access to driver license photos, roadside biometric identification via fingerprint and facial recognition systems, and digital license plate reader systems enable rapid identification of individuals and vehicles. Officers in the field also have immediate access to information such as: active wants/warrants, criminal history, stolen articles/vehicles, sexual predators, US Marshalls most wanted, and DHS terrorist watch list. These technologies enable the rapid identification of fugitives from justice, apprehension of criminals, combating identity fraud and the effective anticipation and mitigation of situational risks when facing potential criminals.
- **Geospatial functionality:** Officers use GPS systems to map addresses for quick response, even in unfamiliar territory, as well as to provide a public service to citizens in unfamiliar surroundings. Dispatchers in our consolidated dispatch centers are able to see the location of state law enforcement officers in the event an officer needs immediate assistance and to be able to dispatch the closest officer, regardless of the LE agency, to provide immediate assistance.
- **Digital video technologies:** In-car video technology is used to document criminal activity, increase officer safety, reduce frivolous law suits, reduce officer court time, and assist with officer training.
- **Remote Records Access:** Ability to access and maintain electronic records from any location promotes efficiency and saves travel and administrative costs.

The LE community's access to these services MUST be 24x7x365; with minimal downtime, either scheduled or unscheduled. LE systems are specifically designed and maintained to minimize planned, as well as unplanned, downtime. Additional redundancy and failover capability is used for the critical 24x7x365 systems, to drastically minimize or even eliminate downtime related to scheduled maintenance. Any technological downtime could mean the loss of lives, either citizen's lives or those of the law enforcement and first responder community. The unique needs of the law enforcement community mandate that considerations related to law enforcement technology not be driven solely by cost savings. The least expensive technological solution may ultimately result in unacceptable risk to the lives of LE officers and the public.

While LE technology needs to be functional, reliable and available, another major benefit that technology can bring to LE is data sharing. Because the multiple levels and branches of law enforcement perform similar functions, including frequently encountering and dealing with the same criminal factions, the sharing of data provides an opportunity for efficiency and effectiveness. The state law enforcement community has already recognized this opportunity and has demonstrated many "success stories" where data and systems are shared. Many of these success stories are summarized in the Law Enforcement Consolidation Task Force IT Team Report dated November 7, 2011. However, as discussed in that report, more can be done toward gaining efficiencies and increasing effectiveness through consolidation and centralization of services, systems, and data.

#### 4. CHALLENGES OF CURRENT CONSOLIDATION FRAMEWORK

Technology consolidation, when done correctly, can achieve cost savings, efficiencies, and advances in functionality and capability. However, if not done correctly, technological consolidation can substantially increase business risk and, in the area of law enforcement, can have disastrous and life-threatening consequences.

It is the general consensus within the LE IT community that the current Data Center Consolidation (DCC) initiative introduces unacceptable risk for law enforcement and the citizens of the state of Florida.

The current effort to consolidate the numerous Florida state government data centers is justified by the long-term potential for significant cost savings across the enterprise. However, without thorough planning, significant capital investment and careful management of functional, skilled personnel, the current consolidation model is fraught with risk for the State's LE functions.

To reduce the risk of downtime and to enable effective security, governance and prioritization of LE systems, several states have opted to exempt law enforcement systems, and those systems and data streams that support them, from consolidation initiatives. Mississippi, Texas, Oregon, and California have all removed law enforcement from consolidation requirements. Iowa has attempted to consolidate some of their LE systems and has in every instance reversed the changes. Michigan identified prerequisites for successful law enforcement consolidation, including data center facility upgrades to achieve Tier 3 standards and establishment of strong processes through adoption of Information Technology Infrastructure Library (ITIL) standards.

As Florida proceeds with Data Center and IT consolidation, it is critical that risks to LE be identified and mitigated. The workgroup identified multiple sources of risk as well as indicators that give evidence that these risks are not currently being mitigated successfully and are already having a negative impact on LE operations.

**Potential Sources of Risk:**

Risk factors exist in all areas of the current Data Center Consolidation Model: Facilities, Processes, Staffing, Disaster Recovery/Preparedness, and Prioritization/Governance. Some of the risks are greater in certain Primary Data Centers than in others. The Workgroup identified the following potential sources of risk; however, this list may not be comprehensive.

1. Data Center System Maturity - The maturity of the current data center system, including facilities and staff, is not fully equipped to handle the special needs of LE. Therefore, there is a tendency for the data centers to treat all agencies (both LE and non-LE) essentially the same, regardless of mission. The consolidation process is rigid and prescriptive, and has little flexibility for agencies to tailor their migrations and operations to meet the needs of the agency and the public they serve. Necessary facility upgrades are incomplete; facility upgrades identified in previous studies have not been completed to the level appropriate for LE needs. Operational monitoring, change management processes, and problem escalation procedures and tools have proven insufficient. Many policies and processes are not fully documented, or are not documented specific to certain agencies or systems.
2. Governance and Prioritization - Data Center personnel and services are not dedicated to the LE mission or under the direction and control of a law enforcement agency, resulting in potential competition for prioritization of resources. This is especially problematic during emergency situations and disaster recovery.
3. Loss of Business-specific IT Expertise – The current Data Center consolidation model promised near-immediate cost-savings primarily through immediate staff reduction. Terminated staff or staff fearful of being terminated departed state government, often taking extensive institutional and technical knowledge critical to the successful operation of the systems being consolidated. This will continue to occur with each agency consolidation, resulting in the loss of essential agency-specific and system-specific expertise being lost upon or prior to consolidation.
4. Reduced Efficiency and Response – Lack of LE-specific IT knowledge prevents the Data Center staff from effectively managing and resolving problems with the LE systems. Consolidated agencies continue to have to rely on internal agency expertise for problem resolution, with involvement of Data Center staff becoming in many situations, simply an added layer, reducing efficiency and slowing the response to incidents and restoration of services.
5. Lack of enterprise Disaster Recovery – The current consolidation model assumes that the agency will continue to be responsible for DR; however, due to technical infrastructure changes and loss of staff, this is not always feasible.
6. Security and Cyberwarfare – The State’s Primary Data Centers meet current CJIS security requirements. However, there is some justification for a higher standard of security to be

required for the consolidated data center model. Consolidated data centers, housing multiple critical systems and extensive confidential data, create an especially attractive target to individuals and organizations, both domestic and international, who wish to engage in cyberwarfare. Insufficient logging and intrusion detection processes could result in an increased risk of data breach. The security programs within the State's data centers are progressing, but they currently lack the maturity needed by a consolidated LE environment. A fully developed and fully implemented Security Program is essential.

7. High availability – LE systems are specifically designed and maintained to minimize planned, as well as unplanned, downtime. Additional redundancy and failover capability, including power and cooling, is needed for the critical 24x7x365 systems, to drastically minimize or even eliminate downtime related to scheduled maintenance. This is not the case for many non-LE systems, nor for the data centers supporting them. Data center “availability” statistics are generally calculated based on unscheduled downtime, which may not adequately represent a data center’s ability to meet the LE requirements for minimal scheduled downtime. Additionally, change management processes and maintenance schedules must be tailored to LE needs, avoiding critical times such as weekends and holidays, which are often the preferred maintenance windows for non-LE operations.
8. Lack of LE “culture” – IT staff working directly for LE agencies have a complete understanding of the needs of the LE mission and a very high level of loyalty and dedication to their role in that mission. For critical LE systems, this drives the IT staff toward a goal of not only “high availability”, but “continuous, uninterrupted availability”. Critical LE systems are considered the very highest of priorities, and do not have to compete with non-LE systems in terms of IT support and service. The importance of the LE culture should not be underestimated.

### **Indicators of Risk:**

Evidence of the types of risk that have already been experienced by agencies involved in data center consolidation:

1. Downtime was recently experienced by customers of Northwood Shared Resource Center (NSRC) when an emergency power-off button was accidentally pressed.
2. 72 hours of downtime for Commercial Motor Vehicle Enforcement troopers related to the data center not doing database backups per the contract which resulted in the log files filling up on the system. This outage resulted in the inability to issue electronic commercial motor vehicle citations resulting in lost revenue for the state.
3. FWC’s entire website was erased from the servers at the SSRC resulting in significant down time and loss of data. SSRC staff was unable to identify how or who had deleted this data due to inadequate procedures and a lack of appropriate logging tools.
4. Consolidated agencies have experienced incidents of insufficient security management and backup of servers not being performed in a timely fashion, in some cases over a week behind schedule.

5. Operational schedules do not address the needs of LE, with maintenance windows scheduled during weekends and holidays, which are the worst times for LE to experience downtime, even scheduled. Alternate maintenance windows, if possible, are provided at an added charge.

**Options for Risk Mitigation:**

- Continue on Current Path (not recommended)
- Bringing entire Data Center System up to level required by LE
- Dedicate a Technology Service Center to LE (public or private)

## 5. LE TECHNOLOGY SERVICE CENTER – THE VISION

The long-term vision for the Law Enforcement IT Service and Support Center (Center) would be that of an IT organization dedicated to the needs of the state law enforcement community. Beyond a “data center”, this Center would ultimately host centralized systems and shared data, as well as support all of the devices and technology critical to the core mission of law enforcement. It would also provide co-location services to law enforcement agencies, to allow them to house non-LE systems that are not centrally hosted and managed, but that need ongoing support of the participating LE agency. The scope of participation, or nonparticipation, by an agency with an LE function should be considered and determined during the initial planning phase of the project to determine if participation is warranted.

1. The Center would be administratively housed within or managed by an existing LE agency. That LE agency would be fully responsible for the day-to-day operations of the Center.
2. Governance of the Center must be carefully designed to empower the LE community to ensure that the mission of the Center is committed to meeting the needs of law enforcement.
3. Initially, facilities would be consolidated, with each participating agency migrating their IT equipment and systems to the selected host facility in a co-location model, and continuing to manage their own IT resources as planning and implementation of the consolidation proceeds.
4. Systems and processes would be carefully consolidated and provided as centrally-hosted services. IT knowledge transfer would be ongoing and shifting of IT staff would be well-planned and coordinated to ensure sufficient support at all times for both consolidated and unconsolidated systems. This process would ultimately result in the majority of IT support functions and staff being consolidated. Any efficiencies gained in IT support staffing would allow for shifting of staff to optimize system support, and to possibly invest staffing resources in adoption of new technologies.
5. Ultimately, all IT systems and services essential to the core mission of law enforcement would be hosted by the consolidated Center, under the control of an LE agency.

In order to successfully achieve this vision, a well-planned phased approach is needed.

## 6. LE TECHNOLOGY SERVICE CENTER - PHASED IMPLEMENTATION

As previously stated, a well-planned and managed phased approach is recommended:

1. **Project Planning** (also repeated within each subsequent phase) – During this initial phase, the scope and objectives of the project would be defined and clarified, enabling establishment of a proposed timeline. The scope of participation, or nonparticipation, by agencies with an LE function would be considered and determined during this phase to determine if participation is warranted. Most importantly, a project team would be assembled, including an experienced project manager and necessary support staff, including resources provided by participating agencies. Preliminary information gathering would include (for all participating LE agencies) an updated inventory of LE systems and IT resources, and (for possible host sites) data center facility and capacity data. This information would be used to solidify options and create a high level plan, which would be refined and revised as the project proceeds. Results of prior studies related to the data center system and facilities should be taken into consideration.
2. **Host Site Selection** – Potential sites would be further analyzed to determine any upfront capital investment needed to ensure LE business requirements are met. Selection and preparation of host site must be completed before moving to the next phase. The most likely options for consideration as Host Site are:
  - a. An existing Primary Data Center
  - b. An existing LE agency data center
  - c. A private-sector data center

See section 7 for further discussion.

3. **Facility Consolidation** – In this phase, equipment and systems supported by participating LE agencies would be physically moved into the shared facility in a co-location model. All IT staff would be retained throughout this phase, to ensure the stability and reliability of all layers of the technology infrastructure. Some cost reduction would be achieved through elimination of duplication of facility and data center infrastructure and environmental systems. Agency Disaster Recovery (DR) plans should be assessed, revised, and tested by agency staff as needed to ensure there is no reduction in DR preparedness.
4. **System and Process Consolidation** – The goal of this phase would be the identification of similar applications, collapsing redundant systems, eliminating or reducing “stovepipes” and “data silos”, increasing data sharing, reducing costs of software licensing, hardware, infrastructure, and support. LE “common” systems and processes should be considered and prioritized for consolidation. Such systems or “process areas”, as identified in the previous team report dated November 7, 2011, may include: **Training Management, Policy Management, Evidence Management, Records Management, and Property Management Systems**, as well as **Computer Automated Dispatch** which has already been extensively consolidated.

Consolidation of these process areas is not necessarily sequential; some overlap could occur; however, coordination and resource availability will be critical. Each process area consolidation should be carefully managed as a project. (See Critical Success Factors below.)

- 5. Full IT Consolidation** – The ultimate vision for the LE Service Center would be for all LE systems and technologies to be consolidated and centrally hosted. After agency-specific LE systems have all been replaced by centralized, hosted LE systems, any support services and IT staff that have not yet been consolidated should be considered for possible consolidation. This could include mobile device support, desktop support, and remaining support for non-LE systems.

## 7. LE TECHNOLOGY SERVICE CENTER - HOST SITE SELECTION

All potential sites must be analyzed to determine any upfront capital investment needed to ensure LE business requirements are met. Agency technology inventory data would be used to analyze capacity requirements and the ability of a given site to meet these requirements. Facility, staffing, and processes should be considered to identify changes or improvements needed.

The most likely options for consideration as Host Site are:

1. An existing Primary Data Center – If an existing Primary Data Center (PDC) is selected, management and operation must be fully and completely transferred to the designated hosting LE agency. Additionally, any and all needed capital investment must be completed **prior to any migration of LE systems** to that facility. By far the best option for use of an existing Primary Data Center would be the Southwood Shared Resource Center (SSRC), which has been classified as a Tier 3 facility, with little or no up-front capital investments needed for facility upgrades. However, many non-LE agencies are already consolidated at the SSRC, requiring re-location of these systems to another PDC.
2. An existing LE agency data center – In selecting an existing LE agency data center as the host location, consideration should be given to: facility quality and capacity; facility or IT infrastructure upgrades that may be needed; ability to meet LE requirements for security and availability, maturity of data center processes; experience of data center staff; and proven experience in providing centralized, hosted systems and services.
3. A private-sector data center

## 8. CRITICAL SUCCESS FACTORS

The prior Team report dated November 7, 2011 outlined and described many of the critical success factors important to successful completion of future consolidation of law enforcement information technology. Most if not all of those critical success factors would be applicable regardless of what approach to consolidation is used or which option for a hosting facility is selected. The major critical

success factors are summarized here; this list is not intended to be complete or comprehensive, but to emphasize the factors identified by this Workgroup as most critical.

**Critical Success Factors for Host Site Selection:**

1. Managed by and dedicated to the law enforcement community.
2. Facility Infrastructure
3. Technology Infrastructure
4. Physical/Cyber Security – high level, both internal and external
5. High availability and Redundancy

**Critical Success Factors for Consolidation of Systems and Processes:**

1. **Business Process Analysis**– In all areas of consolidation, the planning should begin with an examination of the business requirements and processes necessary to perform each service proposed for consolidation.
2. **Planning** - Sufficient time for consolidation research and planning is critical to the success of the effort.
3. **Project Management** – Use of standard project management practices is strongly recommended.
4. **Comprehensive IT Assessment** – For each process area being consolidated, a comprehensive IT assessment should include applications, data, infrastructure, desktops, support and staffing.
5. **IT Staffing** – Knowledgeable and experienced staff must be maintained until it can be assured that they are no longer needed. Careful consideration must be given to the full range of skill sets, duties and institutional knowledge required for system maintenance and support in the consolidated location as well as the skill sets, duties and institutional knowledge that will continue to be needed in the agencies after consolidation. In some cases, IT staff may be shifted from agencies to LE Service Center staff; in other cases, knowledge transfer may be needed.

## 9. RECOMMENDATION AND CONCLUSION

The workgroup makes the following recommendations:

1. Postpone any further data center consolidation of LE agencies.
2. Proceed with initiation of a project to establish a Law Enforcement Technology Service Center as described in this report.
3. Commit upfront and ongoing resources needed to ensure the mission of law enforcement is not compromised, even if the ultimate result of the consolidation does not achieve maximum cost savings.

These are challenging budgetary times. The LE community is committed to our Governor's directive to find better, less costly, and more efficient ways to do business without compromising the critical mission of law enforcement to provide for the safety of our citizens and officers. We strongly support the efforts to consolidate data centers across the State as an effective way to decrease costs and improve service in some agencies. However, given the unique level of service required by LE agencies, and the high level of risk that currently exists in the data center consolidation model, we believe it is prudent for the State to move forward with the above recommendations.

The solution of a Law Enforcement Technology Service Center provides for just this type of efficiency. By consolidating like functions into one data center, cost savings will be achieved first through facility consolidation in a co-location model, quickly reducing operational costs. Subsequently, by replacing current stove-piped LE systems with centralized hosted ones, additional cost-savings and efficiencies can be realized beyond those achieved through data center consolidation alone. This approach provides for a process utilizing LE IT subject matter experts working together toward the goal of keeping our law enforcement officers safe while protecting Florida citizens and visitors. Ultimately, the State can achieve the ambitious vision of enterprise-wide LE hosted services and data sharing which is necessary for the long-term success of our law enforcement community.