

Law Enforcement Consolidation Task Force

Information Technology Team



FINAL REPORT

November 7, 2011

CONTENTS

1. EXECUTIVE SUMMARY	3
2. BACKGROUND	4
2A. Team Charter	4
2B. Team Approach	6
2C. Current Environment	7
3. PRIOR LAW ENFORCEMENT IT CONSOLIDATION INITIATIVES	8
3A. Success Stories	8
3B. Lessons Learned	12
4. DATA CENTER CONSOLIDATION.....	14
4A. Law Enforcement Data Center Consolidation Workgroup	14
4B. Gartner Data Center Consolidation Study	15
5. I.T. STAFFING AND RETENTION	15
6. EFFICIENCY AND CONSOLIDATION OPPORTUNITIES.....	16
6A. Law Enforcement Application Systems	16
6B. Consolidation Critical Success Factors	18
7. RECOMMENDATIONS	19
APPENDIX A – LE DATA CENTER CONSOLIDATION RECOMMENDATIONS	21
APPENDIX B – LE DATA CENTER REQUIREMENTS WORKGROUP CHARTER.....	25
APPENDIX C – CRIMINAL & JUVENILE JUSTICE INFORMATION SYSTEMS COUNCIL.....	34
APPENDIX D – GLOSSARY OF ACRONYMS & ABBREVIATIONS	34

1. EXECUTIVE SUMMARY

Background

The goal of the Law Enforcement Consolidation Information Technology Team (Team) was to review and assess the existing law enforcement (LE) information technology (IT) environment and to identify possible efficiency and consolidation opportunities. The Team included membership representing all state agencies with a law enforcement component.

The Team considered all areas of information technology, but focused primarily on the area of law enforcement application systems. The Team developed a high level inventory of law enforcement applications used by all participating agencies. The Team reviewed and discussed each application from the perspective of whether it would likely be a good candidate for consolidation based on several factors.

One notable finding was the degree to which the law enforcement community has successfully engaged in, and completed, initiatives toward consolidation, centralization, and efficient sharing of data and processes. Many examples of such success stories are included in this report. Based on prior consolidation experience, the Team was also able to identify major critical success factors for consideration in future consolidation initiatives.

Critical Success Factors

General consolidation Critical Success Factors identified by the Team are summarized below (Section 6B contains a full discussion of these Critical Success Factors).

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 recommended.
4. Comprehensive IT Assessment – When any consolidation is being considered, a comprehensive IT assessment should include applications, infrastructure, desktops, data, support and staffing.
5. IT Staffing – When consolidations are planned, careful consideration must be given to the full range of skill sets, duties and institutional knowledge required for system maintenance / 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.
6. Primary Data Center Coordination - Complications and complexities are multiplied once systems are centrally located in a Primary Data Center.
7. Primary Data Center Budgeting – current Primary Data Center funding methodology of Zero Balance provides no funding for additional hardware, software, or other expenses that may be necessary to the success of the project.

Recommendations

The Information Technology Team recommends the following:

1. Consider the following application systems for possible centralization or consolidation, which are used similarly by most law enforcement units: **Training Management, Policy Management, Evidence Management, Records Management, and Property Management Systems.**

However, comprehensive analysis of agency-specific business requirements, processes, and interfaces is warranted prior to any final decision.

2. Any potential consolidation of law enforcement should include comprehensive and effective planning, business analysis, coordination and communication, addressing all areas of information technology and utilizing accepted practices in project management. LE consolidation may impact and be impacted by the Agency for Enterprise Information Technology Data Center Consolidation and other Enterprise Consolidation efforts currently underway, and such potential impacts should be considered during analysis and planning of any proposed LE consolidation.
3. Interagency workgroups made up of both business (LE) and IT personnel should be established for detailed study and business process analysis of any recommended area of consolidation or major efficiency initiative. It is critical that the services and business processes of all agencies must be analyzed from an operational perspective prior to any attempt to consolidate any IT supporting those business processes.
4. The importance of retaining skilled and knowledgeable IT staff should not be underestimated. The State should make every attempt to retain IT staff throughout the consolidation process, during which time agency-specific technical and institutional knowledge is especially critical. No reduction in IT staff should be attempted until well past the successful completion of consolidation, and even then reduction should only be through normal attrition.
5. The Agency for Enterprise Information Technology should be given the necessary resources and authority to take action to implement and comply with requirements and recommendations from the Law Enforcement Data Center Requirements Workgroup. Specifically, Data Center facilities MUST comply with federal Criminal Justice Information Systems (CJIS) Security Policy and MUST meet all requirements for high availability, including sufficient failover and disaster recovery to geographically dispersed locations.
6. The state should undertake a comprehensive assessment of the Primary Data Center system with specific focus on facilities, security, staffing, tools, processes, controls and transparency.
7. Any future recommendations to address the consolidation of IT functionality across state criminal justice and law enforcement agencies should comply with standards as adopted by the Criminal and Juvenile Justice Information Systems (CJJIS) Council in accordance with its duties stated in Florida Statute 943.08 and be reviewed by the Council as necessary. (See Appendix C for additional information on the CJJIS Council)

2. BACKGROUND

The goal of the Law Enforcement Consolidation Information Technology Team (Team) was to review and assess the existing law enforcement (LE) information technology (IT) environment and to identify possible efficiency and consolidation opportunities.

2A. TEAM CHARTER

Information Technology Team

Executive Sponsor: Emery Gainey, Attorney General's Office

Executive Co-Sponsor:

Senior Leadership Team Leader: Deborah Stevens, Attorney General's Office

Senior Leadership Team Co-Leader(s): Penny Kincannon, FDLE

Team Members:

Emery Gainey, Attorney General's Office
Mark Zadra, FDLE
Deborah Stevens, Attorney General's Office
Penny Kincannon, FDLE
Mike Russo, AEIT
Larry Coffee, FDLE - CJIS
Major Steve Williams, HSMV - FHP
Joey Hornsby, FDLE – IRM
Mitch Golloher, DEP
Robert Fields, HSMV
Brett Norton, FWC
Kevin Patten, FWC
Lynn Dodson, FDLE
Chuck Murphy, FDLE
Pati Lytle, DOACS
Terry Kester, DFS (Invited)
Benita Williams, DJJ
Jackie Suttle, DJJ
Doug Smith, DOC
Tammy Crumel, DOC
Joseph Martin, DBPR
Team Resource: Lisa Hopkins, FDLE

Issue:

Senate Bill 2160 created the Law Enforcement Consolidation Task Force (LECTF). The mission of the Task Force is to review all state law enforcement functions, evaluate duplicate efforts, and identify functions appropriate for possible consolidation.

The Task Force designated Teams to perform detailed research on specific topics and report back to the Task Force. The Law Enforcement Information Technology Team will provide information and recommendations dealing specifically with information technology (IT) issues, including but not limited to the consolidation of LE data centers.

Scope:

The scope of the Law Enforcement Consolidation Task Force Information Technology Team is to address the information technology (IT) aspects of law enforcement consolidation to provide information related to the feasibility and effectiveness of such consolidation. A primary area of focus will be law enforcement application systems currently in use, which will be reviewed, categorized and assessed to determine possible duplicative systems and to help identify opportunities for consolidation, centralization, or sharing of these systems. Additionally, the Team will consider the potential impact of data center consolidation efforts on LE operations, and prior attempts and successes relating to LE IT consolidation, centralization, and sharing initiatives to identify and document best practices toward ensuring the success of future such initiatives.

With the potential consolidation of law enforcement personnel, opportunities exist for consolidating, centralizing and streamlining of business processes. Such changes will drive associated IT changes

and consolidation. However, it is important to note that proper analysis, assessment and planning of IT consolidation is dependent upon and driven by the business decisions. Costs, benefits, risks, and critical success factors of IT consolidation can only be fully determined after business decisions are made as to consolidation of staffing and business processes.

Team Goals:

The overall goal of this Team is to provide information and recommendations related to potential LE consolidation, with respect to the area of information technology, including LE data centers, application systems, desktop support, and other areas of information technology.

Specific goals include:

1. Review and assess existing LE applications, to identify possible opportunities for consolidation, including but not limited to duplicative systems.
2. Review and assess previous successful LE consolidation initiatives, to determine and document applicability to current initiative, including best practices for successful IT consolidation.
3. Review the LE Data Center Requirements and Recommendations produced by the CIO Council Law Enforcement Data Center Consolidation Workgroup, to determine applicability to current initiative.

Work Product:

The IT Team Report will include:

1. Overview of previous and existing consolidation initiatives, including lessons learned and best practices
2. Identification of additional areas for consideration, such as duplicative IT systems and services
3. Identification of other IT considerations or recommendations applicable to possible LE consolidation initiatives

Timeframe for Completion:

October 31, 2011 or as needed for completion of Task Force Report, December 2011.

2B. TEAM APPROACH

The Information Technology Team included membership representing all agencies with a law enforcement component. Many of the team members had previously participated in the Chief Information Officers Council (CIO Council) Agency for Enterprise Information Technology Advisory Committee Law Enforcement Workgroup (Workgroup), which had identified data center requirements and recommendations specific to the needs of law enforcement. The Team discussed and included the work of the prior CIO Council initiative, but attempted to avoid duplication of effort.

The approach taken by the Team was as follows:

1. The Team discussed the previously-developed LE Data Center Requirements and Recommendations, prepared by the CIO Council initiative, and agreed that the deliverables produced at that time are still valid and should be included by reference. Statewide Data Center Consolidation and IT Consolidation were also discussed, and related issues and efficiency opportunities were considered.
2. All areas of IT were discussed and considered, such as applications, infrastructure, desktops, data, support and staffing. Feedback received from the comprehensive Task Force survey was reviewed.
3. The Team focused primarily on the area of law enforcement applications, in light of the other Enterprise IT Consolidation initiative currently underway.
4. In assessing opportunities in the area of law enforcement applications, the Team felt that additional information was needed from participating agencies. A spreadsheet was developed, distributed and consolidated, documenting the applications used by law enforcement in each participating agency. These applications were considered for consolidation potential.
5. During the Team's review of LE applications, it was apparent that many LE applications have already been consolidated or centralized, and these "Success Stories" were documented as well.

It should be noted that, in the event that any law enforcement units are designated for consolidation, IT consolidation opportunities are possible and quite likely as a result of the consolidation of the business unit.

2C. CURRENT ENVIRONMENT

Currently, an agency's information technology services and resources primarily reside within the agency itself. Systems are shared between law enforcement and non-law enforcement staff, and the IT resources, including hardware, software and support staff, are also shared. Historically, the platforms used and supported across different agencies may vary widely, resulting in disparate applications, database platforms, and system platforms. Therefore, many of the law enforcement units utilize entirely different systems, many of which have been highly customized for the unit's specific business needs and current processes. IT service levels and business requirements vary widely given the differing missions among agencies. Some agencies operate on a mission critical 24/7 basis, whereas others may only routinely deploy law enforcement on an 8-5 weekday basis. IT support levels and resources vary drastically as well.

An important commonality among law enforcement agencies is adherence to the FBI's Criminal Justice Information Services (CJIS) requirements to protect and safeguard criminal justice information. The Florida Department of Law Enforcement (FDLE) is tasked with granting, monitoring and compliance with the CJIS requirements for all law enforcement entities in Florida. All agencies work closely with FDLE to ensure the requirements are met and address any issues when environments and systems change.

The State of Florida has embarked on an IT consolidation initiative, under the direction of the Agency for Enterprise Information Technology. As part of this initiative, agency data centers and e-mail systems are being consolidated, with other enterprise-wide services such as desktop support being planned for future consolidation. Some law enforcement data centers, such as the Department of Juvenile Justice and the Department of Corrections, have already been moved into one of the three

designated Primary Data Centers, and basic CJIS requirements have been met, but full managed-service consolidation will still take some time as FDLE and the resident criminal justice agencies wrestle with achieving compliance in an environment shared with non CJIS agencies. Other agencies with law enforcement components are being consolidated at this time, with others to follow over the next 2 years.

Any law enforcement consolidation should take into account the current diversity and complexity of the state's technology infrastructure supporting law enforcement and the possible effects by and on the Enterprise IT Consolidation initiative.

However, as described in the Consolidated Success Stories section, the law enforcement community has proactively engaged, probably more so than in any other program area, in extensive centralization and consolidation of services, applications, and data. These prior initiatives have already achieved considerable gains in efficiencies, collaboration, and data sharing.

3. PRIOR LAW ENFORCEMENT IT CONSOLIDATION INITIATIVES

As the IT Team reviewed and analyzed existing information technology applications in use by law enforcement across state agencies, it quickly became clear that many successful consolidations have already been completed. There are many systems, centralized and maintained by the Florida Department of Law Enforcement, which provide critical information to, and between, Florida's criminal justice community and also provides access to information held nationally and by other states. The Department of Highway Safety and Motor Vehicles also hosts and supports centralized applications used by multiple law enforcement entities. Additionally, some application systems, including both hardware and software, have been migrated from one agency to another to reduce overall support and provide improved service. There have also been several technology consolidations completed in support of the consolidation or realignment of law enforcement units.

3A. SUCCESS STORIES

The following provides an extensive, though not necessarily complete, overview of prior law enforcement information technology consolidation success stories.

Computer Aided Dispatch (CAD) DHSMV/FHP

In 2003, the Florida Highway Patrol, Florida Department of Law Enforcement and Florida Fish and Wildlife Commission worked collectively to develop an ITN for a single system to support law enforcement dispatch functions that could be shared. Once the vendor was selected, a single solution was developed and implemented which supported the functions of each agency. This single system is supported and managed by DHSMV and now supports 11 state agencies, 6,000 law enforcement officers and 4,000 mobile devices. Each agency participates in sessions with DHSMV related to enhancements to the system.

Department of Environmental Protection (DEP) SmartCop

In December 2010, Department of Environmental Protection (DEP), Division of Law Enforcement made the decision to transfer the SmartCop data servers to the Florida Highway Patrol, Division of Highway Safety and Motor Vehicles (DHSMV). The decision was made to streamline data access and communication with the DHSMV Computer Aided Dispatch. The transfer of servers allowed DEP users to access the NetMotion VPN without the purchase of additional servers to house the NetMotion VPN client. Additionally, DEP users now accessing the DHSMV network experience faster processing

speed, greater reliability, and a robust server connection, as the network was built with the mobile user in mind. This transition was accomplished with minimal costs by taking advantage of the existing DHSMV network. Once the migration was completed, DHSMV consolidated DEP data into existing FHP systems and shut down the DEP hardware which further reduced costs and maintenance.

Department of Environmental Protection (DEP) CopLink and Rapid ID

In 2011, subsequent to migrating their SmartCop servers, DEP also moved their CopLink (IBox) and Rapid ID servers to the DHSMV network creating additional savings while increasing productivity, by reducing DEP support and maintenance requirements. The move to maximize available technology has created a positive impact on field level reporting while generating savings for the tax payers of Florida. Once the migration was completed, DHSMV consolidated DEP data into existing FHP systems and shut down the DEP hardware which further reduced costs and maintenance.

State Fire Marshal (SFM) SmartCop

Similarly to DEP, the State Fire Marshal migrated their mobile systems to DHSMV, creating additional savings while increasing productivity, by reducing SFM support and maintenance requirements utilizing existing systems in DHSMV.

Child Predator Cybercrime

In July 2011, the Child Predator Cybercrime Unit (CPCU) was transferred from the Office of the Attorney General, Department of Legal Affairs (OAG) to the Florida Department of Law Enforcement. The technology component of this consolidation was streamlined through the adoption of new business processes, allowing CPCU staff to utilize existing systems at FDLE going forward, while accessing their historical case data through a local copy of their OAG application and database.

CJNet

FDLE provides the backbone of Florida criminal justice telecommunications – the CJNet. The CJNet is a virtual private network providing connectivity to approximately 600 local, state, and federal criminal justice and law enforcement sites across Florida. It provides access to critical criminal justice information systems - provided by multiple agencies - to all of Florida's Criminal Justice Community statewide. Systems such as FCIC, DAVID, BIS, RapidID, and CJNet email are just a few of these systems. Additionally, over the last several years, CJNet sites have been encouraged to consolidate connectivity within their respective agencies. This internal consolidation has resulted in a reduction of the total number of physical CJNet connections by approximately 25% with no reduction in access or availability.

FCIC - Florida Crime Information Center

The FCIC system serves over 81,000 devices in approximately 1,300 federal, state and local criminal justice agencies. This system provides information on wanted or missing persons and stolen vehicles, boats and property. The FCIC system processes between 80 and 90 million data transactions per month (over 1 billion transactions during FY 10-11). This system allows criminal justice agencies virtually instantaneous access to a variety of state and federal information sources. This system serves as Florida's gateway to information held by the Federal government and other states through the NCIC (National Crime Information Center) – the central database for tracking crime-related information - and the III (Interstate Identification Index) - a national index of criminal histories (or rap sheets), maintained by the Federal Bureau of Investigation (FBI).

CCH - Computerized Criminal History

FDLE maintains the 4th largest criminal history file in the nation – receiving over 20 million arrests per year. Persons arrested throughout Florida are entered into the CCH as they are booked by the local arresting agency. CCH serves as the state repository and makes the records available to all criminal

justice agencies in Florida and across the country, other governmental agencies, and to the public (through the Internet). Criminal histories can be accessed by searching name and other identifiers or by positive fingerprint identification. Each criminal history record must be based on a fingerprint submission that is retained by FDLE and used for future identification. This system relies on several sub-applications such as the LOGAN system - used by the Florida Clerks of the Court to report dispositions to CCH.

BIS - Biometrics Identification System

The BIS is the fingerprint repository for all persons arrested in Florida and currently contains 4,937,255 10-print person records. Fingerprints (as well as identification and charge information) are entered by local agencies throughout the state through Livescan devices. This system works hand-in-hand with the CCH to provide a complete criminal history.

FALCON

The criminal history records in the systems discussed above also provides information for public use in background screening for firearm purchase authorization, employment, volunteer efforts, assorted licenses, and voter registration. In Florida, criminal history record screening for licensing and employment purposes is required for many professions. Florida also passed legislation, under the National Child Protection Act, authorizing record checks for volunteers working with children, disabled persons or the elderly.

The FALCON system provides the ability to retain and search large groups of individuals (licensees, for example) against incoming arrests and notify the employer or regulating agency if that person is arrested.

FALCON also provides the ability for criminal justice agencies to create and maintain watch lists – a list of names that will generate a notification to the agency if any of those persons are arrested.

In addition, FALCON receives identification requests with two fingerprints from remote devices and interfaces with the Rapid ID system (described below) which searches and matches the fingerprints. FALCON, based on the information requested and the reason for fingerprinting, collects and bundles the requested information into a single response that is returned to the remote device. That information may include an identification based on a match in the Rapid ID System, Florida and National Wants and Warrants, Florida and National Criminal history, DNA availability status, and/or fingerprint matches to the FBI's Repository for Individuals of Special Concern (RISC). This service is used by corrections and probation facilities, medical examiners, and the court system to positively identify individuals (and to determine their DNA availability status) and is also used road-side by law enforcement officers.

Rapid ID

The Rapid Identification System is a separate fingerprint identification system using four fingerprint images from the BIS data on Florida's arrested subjects. The system – accessed through FALCON, allows the use of small remote devices that transmit one fingerprint image to confirm identity or two fingerprint images to search for an unknown person's identity.

Sex Offender / Predator and Career Offender

The Sex Offender/Predator system provides information and geomapping capabilities to law enforcement and the public on Florida's sexual predators and offenders. The Jessica Lunsford Act of 2005 required sex offenders and predators to reregister twice a year at designated county offices. Recently, this system has been revised to comply with the federal Adam Walsh Act and the Cybercrimes registration requiring offenders and predators to register their e-mail addresses and instant messenger screen names. To date, FDLE has identified 52,152 sexual offenders and predators to the public.

MEPIC - Missing and Endangered Persons Information Clearinghouse

FDLE maintains the Missing and Endangered Persons Information Clearinghouse (MEPIC), an application that provides information on missing and endangered adults and missing children to Florida law enforcement and coordinates with similar Federal missing person/children systems. The information is collected and disseminated to assist law enforcement agencies, public and private organizations and the citizens of Florida in locating missing children and endangered adults. This system coordinates with state and national Amber and Silver alert systems.

FLEX – Florida Law Enforcement eXchange

The FLEX project, begun shortly after September 11, 2001, established a strategy for greater information sharing among local and state agencies. The goal was to provide a way to link agencies to provide and analyze local agency information such as citations, field interviews, incident reports, pawn records, traffic accidents, warrants, permits, mugshots and arrests.

At the time, each Domestic Security Task Force region were developing their own regional systems and it was determined that the most efficient way to facilitate sharing was to link these existing systems. Three regions had their own regional information sharing systems – Region 1 (Pensacola) uses as system called SmartCOP, Region 3 (Jacksonville) uses LInX, and Region 5 (Orlando) uses Finder. FDLE, other state agencies, and the Domestic Security Task Force Regions 2 (Tallahassee), 6 (Ft. Myers), & 7 (Miami) pooled their resources to develop a single solution - R-LEX, the Regional Law Enforcement Exchange to share information between them and connect these agencies to Region 4 (Tampa Bay) information.

The final step – the development of FLEX – will connect all 7 regions and state law enforcement agencies to allow information sharing throughout Florida

FCAC Online Request Tracking System

This application allows law enforcement personnel to submit requests (via CJNet web form) for Financial Crime analysis from FDLE.

Insite (ACISS)

This application is used by the Office of Statewide Intelligence (OSI) and local intelligence units to track intelligence on Drug, Gang, and Terror related subjects.

LeadTracking (ACISS)

This program is a web application located on CJNet, and serves federal, state and local law enforcement agencies by providing a secure computer database of active criminal intelligence and active criminal investigative lead information.

MARS eXplorer - Mutual Aid Response System

MARS eXplorer provides a secured, comprehensive mutual aid inventory identifying specialized law enforcement expertise and equipment for use by Florida's county and municipal law enforcement agencies. This system provides critical information in times of a state emergency.

ATMS - Automated Training Management System

FDLE serves as the state's officer standards and training authority. The ATMS houses information related to Florida sworn criminal justice officer's training, employment history, and certification information. This system, used by FDLE, local criminal justice agencies and criminal justice training schools is the repository for information on all of Florida's certified criminal justice officers.

OCETS - Online Curriculum Electronic Tracking System

OCETS is used for all aspects of the Florida Officer Certification Exam process, including: registrations, rosters, grading, results notices, review and challenge sessions, and various reporting functions.

3B. LESSONS LEARNED

With the great variety of agency missions and services, the complexity of the processes involved in providing these services, and the criticality of the information held by these agencies, not all of the LE IT consolidation efforts in Florida have been entirely successful. These initiatives offer “lessons learned” that can be critical to the success of future consolidation efforts.

Dispatch Center Consolidation

In 2000, 11 state agencies embarked on a project to consider consolidation of state law enforcement dispatch services. The project would coincide with the build out of the new state law enforcement radio system which was the consolidation of all state agencies land mobile radio systems into a new shared radio system which cut down on maintenance and infrastructure cost, and allowed all officers to communicate with each other. The project involved closing 60 dispatch centers and moving to seven regional centers.

The consolidation of law enforcement dispatch services produced at 2.4 million dollars savings by cost avoidance related to data circuits, facilities, maintenance and FTE’s. The consolidation also provided, at no additional cost, 24x7 dispatch services to state agencies that could not afford it in the past..

Planning for the consolidation took approximately 2 years and implementation took 3 years. This project involved technical requirements, facility requirements, movement of personnel and more importantly, governance. Each agency involved had their own separate geographical working boundaries, their own method of operations either based on current agency policy, existing laws or administrative rule.

After successful implementation of dispatch center consolidation, the agencies maintained a governance structure to ensure that all agencies needs were being met, and DHSMV/FHP continued to manage all systems and infrastructure as well as personnel that were transferred from other agencies. FWC operates within each of the regional dispatch centers at this time, dispatching only for FWC officers but utilizing the shared radio system and FHP dispatch systems which also helped reduce cost.

There were many lessons learned during this consolidation due to the size and complexity of 11 state agencies. The main lesson dealt with up front planning and communications with personnel affected by the closure of centers. Other lessons learned involved extensive planning with IT professionals from the impacted agencies and vendor systems, phone companies and construction companies. We learned it is very important to retain personnel with institutional knowledge to help with a project of this scale.

Department of Environmental Protection, Division of Law Enforcement, Records Management and Rapid-ID Consolidation into DHSMV/FHP systems

In 2010, Department of Environmental Protection, Division of Law Enforcement (DEP-DLE) and the Department of Highway Safety and Motor Vehicles, Florida Highway Patrol (DHSMV FHP) entered in discussions related to DHSMV hosting RMS and Mobile Data Services for DLE officers. DEP-DLE had stood up their own systems a few years earlier and were having issues related to systems upkeep and mobile connectivity. DEP-DLE systems at the time were also configured to communicate with DHSMV/FHP systems for services related to Computer Aided Dispatch (CAD) via common services on the state network. DHSMV and DEP-DLE took several months to plan and then test a solution that would not only allow DHSMV to host all of DEP-DLE services, but also handle the transition with little or no down time for the DLE officers in the parks. DEP-DLE systems were initially moved over to the DHSMV data center intact and connected to HSMV back-end systems, while users were migrated to

connect to DHSMV/FHP mobility VPN services. Once completed and system functionality verified, DHSMV and DEP-DLE worked toward a single solution that allowed the decommissioning of 5 servers and the costs affiliated with maintenance. Planning to full implementation took over a year and resulted in minimal down time for any law enforcement officer. Once the RMS and mobile systems were migrated, DHSMV and DEP-DLE worked toward moving all of DEP-DLE law enforcement IT systems into DHSMV. The migration was completed in January 2011 and any hardware previously utilized by DEP-DLE was either decommissioned or repurposed.

This project, although well planned, had issues related to different security policies applied to DEP systems that were more lax. It resulted in some unnecessary down time while DEP had to deal with a virus that infected their entire LE network. Lesson learned by all was the importance of verifying security policies of any agency prior to moving systems in to DHSMV systems.

FDOT-Motor Carrier Compliance Office (MCCO)/ FHP Merger

The 2011 legislative session moved Motor Carrier Compliance Office from the Florida Department of Transportation (FDOT) to the Department of Highway Safety and Motor Vehicles/Florida Highway Patrol (DHSMV/FHP) effective July 1, 2011. DHSMV/FHP had previously developed high level plans when this move was proposed in prior legislative sessions but not to the level needed related to Information Technology Systems. In March of 2011, plans were being developed to move personnel into DHSMV from FDOT and teams were established based on the operational areas of each agency function (HR, IT, Fleet, Property, etc.). During the discovery phase of the project, each functional team had to determine what systems or functions were being impacted and how it was being mitigated. IT turned out to be the most complicated function to complete with a very short deadline.

Although personnel were transferred to DHSMV/FHP on July 1, 2011, none of the IT systems were able to be moved due to very complex dependencies on each agency's existing network systems, and the fact that no common connection existed on the network between the two agencies. Additionally, data center consolidation was underway with FDOT/MCCO which further complicated issues and increased costs.

Further complications from reduction in IT personnel as part of the consolidation of the two agencies also increased timelines due to inadequate resources available. To date, MCCO IT systems are still on the FDOT network and hope to be fully migrated to DHSMV/FHP systems by February 2012.

The lessons learned from this consolidation are many but most important is that consolidation which involves disparate IT systems takes time to plan and implement, and requires proper resources as well. The consolidation would have been less difficult to implement had detailed analysis time been available. The cooperative work between the two agencies and also FDLE has enabled systems to stay in place and to be maintained by FDOT while DHSMV works toward a full migration. The full migration of all MCCO IT systems and resources into DHSMV will take approximately one year.

Key Lessons Learned

Each of these projects has provided valuable insight that can be used to facilitate future efforts. These insights are summarized below:

1. Sufficient time for consolidation research and planning is critical to the success of the effort.
2. It is critical that the services, business processes, and requirements of all agencies must be studied and integrated prior to any attempt to consolidate any IT supporting those business processes.
3. The planning phase must include all affected parties to an appropriate degree.

4. Complications and complexities are multiplied once the systems are located in a Primary Data Center (PDC). The regulations, rules, and service agendas of all agencies and the PDC will require much more time to integrate than had been planned.
5. The current PDC funding methodology of Zero Balance provides no funding for additional hardware and software that may be necessary to the success of the project. The PDC must have flexible funds to provide service to the agencies and deal with equipment problems and DR considerations.
6. Agencies that have subsumed other agencies or bureaus (and currently still have a complex, two-tiered processes and systems) are now being consolidated into other agencies or the PDC's. This is adding layer upon layer of IT complexity and process that needs to be dealt with.
7. When consolidations are planned, careful consideration must be given to the full range of skill sets, duties and institutional knowledge required for system maintenance / 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.

4. DATA CENTER CONSOLIDATION

4A. LAW ENFORCEMENT DATA CENTER CONSOLIDATION WORKGROUP

Many of the team members had previously participated in the CIO Council AEIT Advisory Committee Law Enforcement Workgroup, which had identified data center requirements and recommendations specific to the needs of law enforcement. The work of the prior Workgroup was discussed extensively by the Team. The Team validated the findings of the Workgroup and raised concern that not enough has been done to address the recommendations documented in the Workgroup's deliverables.

Key Workgroup recommendations that the Team feels should be highlighted are:

- Data Center facilities MUST meet all requirements for CJIS security and for high availability, including sufficient failover and disaster recovery to geographically dispersed locations.
- Availability and security standards for consolidated LE systems should be even higher than those of non-consolidated LE systems. A consolidated data center, with the increased concentration of sensitive, confidential, and valuable systems and data, becomes an even more attractive target of security attacks, warranting even higher standards of security and redundancy.
- Data centers must implement a process for completing After Action Reports for all system failures or problems, detailing why the failure or problem occurred and what has been done to prevent reoccurrence.

The deliverables of the CIO Council AEIT Advisory Committee Law Enforcement Workgroup, including the "Law Enforcement Workgroup Charter and Overview", the "Law Enforcement Data Center Consolidation Requirements" and "Law Enforcement Data Center Consolidation Recommendations" may be found at http://cio.myflorida.com/committees_groups/AEIT.shtml. The recommendations and workgroup charter are also attached as Appendix A and B, respectively.

4B. GARTNER DATA CENTER CONSOLIDATION STUDY

In 2008, the state contracted with Gartner, Inc. (Gartner) to conduct a data center consolidation feasibility study. Gartner looked primarily at the facilities aspect of data center consolidation – examining the current state agency facilities and making recommendations for proceeding with the statewide consolidation. The study stated that “...successful data center consolidation projects are built around a decision to transform the organization – not just move the “machines” and people. The technical aspects of most consolidations are easier to manage than the cultural and operational dynamics of the organization.” [Final Report – State of Florida Data Center Consolidation Feasibility Study – 22 April 2008]

Gartner identified several Key factors that the State must keep in mind in moving forward with data center consolidation that closely mirror the general consolidation Critical Success Factors identified by the Team. Among Gartner’s key factors:

- Addressing and overcoming past consolidation experiences
- Applying the “lessons learned” regarding ineffective or nonexistent governance
- Avoiding cost reduction goals that are overly aggressive or unrealistic
- Ensuring the engagement, participation and ownership leadership across the State’s departments and agencies
- Allocating sufficient investment funding
- Establishing strong and confident project management oversight
- Developing the internal capacity and skills necessary for success
- Building a governance and management structure that creates a high level of trust in the data center host agency
- Making tough decisions regarding staffing levels
- Ensuring ownership and buy-in by State departments and agencies

As the project has moved forward in the 4 years since the study, technology has evolved, with resultant changes to many of the proposed consolidation solutions. The establishment of the Primary Data Centers (PDCs) as individual entities (each with their own policies, procedures and standards) and the initial movement of a variety of legacy agency systems into the PDCs results in many unknowns that must be addressed in the planning of any future consolidation efforts. The Team determined that it would be prudent for the State to conduct a comprehensive assessment of the PDC system with a focus not only on facilities, but also security, staffing, tools, processes, controls and transparency.

5. I.T. STAFFING AND RETENTION

The Team identified many challenges related to IT staffing that affect the State’s current IT environment and may have extensive affects on any future efforts at consolidation of IT.

Currently, an agency’s information technology services and resources primarily reside within the agency itself. IT support for a given law enforcement entity is often simply a component of the IT support provided to the entire agency. For agencies made up primarily of law enforcement units, a consolidation of law enforcement units would likely result in essentially all of the IT resources being consolidated as well. However, in many cases, the systems are shared between law enforcement and

non-law enforcement staff, and the IT resources to support those systems, including hardware, software and support staff, are also shared. Due to this complexity, there can be challenges in separating the IT support for a law enforcement unit from the IT support provided to the agency at large. For example, a law enforcement unit may use the same case management system as non-law-enforcement investigators and attorneys within the agency. System and database interfaces may exist between “law enforcement” systems and “non-law enforcement systems”. Separating the law enforcement unit(s) out from the remainder of the agency may result in higher costs as a result of duplicating hardware, software, and support staff, and may result in decreased efficiency in coordination, collaboration, and data sharing between law enforcement and non-law-enforcement units.

The platforms used and supported across different agencies vary widely, resulting in disparate applications, database platforms, and system platforms. Many of the law enforcement units use entirely different systems, many of which have been highly customized for the unit's statutory constraints, specific business needs, and current processes.

Many IT support personnel possess extensive business and institutional knowledge, related to the IT services in support of the specific agency mission. IT support levels vary widely given the differing missions among agencies. Some agencies operate on a mission critical 24/7 basis, whereas others may only routinely deploy law enforcement on an 8-5 weekday basis. All of these factors can make separation of the IT support function detrimental to the efficiency and effectiveness of the agency.

IT staffing issues are exacerbated by the difficulty that the state currently faces in attracting and retaining skilled technology professionals. Due to relatively low salaries (as compared to similar IT jobs in the private sector) coupled with the job uncertainty and perceived instability due to enterprise IT consolidation efforts, many agencies are already facing tremendous challenges in obtaining and retaining highly qualified IT staff. Many agencies have experienced a loss of staff to salaries 20-50% higher both inside and outside of state government, and are then unable to find qualified candidates willing to work for the salary available.

Every effort should be made to retain the knowledgeable and skilled IT resources that currently support the LE systems within the agencies, through consolidation and beyond. Consolidation decisions should not be made under the assumption that savings can be immediately achieved through the reduction of IT staff. Additionally, careful consideration must be given to the full range of skill sets, duties and institutional knowledge required for system maintenance / 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.

6. EFFICIENCY AND CONSOLIDATION OPPORTUNITIES

6A. LAW ENFORCEMENT APPLICATION SYSTEMS

The Team considered all aspects of IT consolidation, but focused primarily on the area of law enforcement applications. Due to the Enterprise IT Consolidation initiatives currently underway, the Team recognized that many areas of IT will eventually be consolidated as part of that initiative. The area not in scope for the Enterprise IT Consolidation is the area of applications. For this reason, the Team focused on law enforcement-specific applications, but recognizes that, with any consolidation or shifting of LE services or staff, hardware, software/licensing, and support staffing must be considered for all areas of IT such as application, database, desktop, file/print, security and mobile computing.

The Team compiled and reviewed a high level law enforcement application inventory submitted by the participating agencies. Applications were considered for their consolidation potential, with special

consideration being given to duplicative applications, where multiple agencies use distinct systems for similar purpose.

- A total of 66 of law enforcement applications were included in the Team's inventory, 29 of which are already consolidated or centralized. Of the remaining applications, 11 were considered possible candidates for consolidation, while 26 were determined to be poor candidates for consolidation, for one or more of the following reasons:
- The business need being met by the application does not exist in other agencies;
- The business rules governing how the application functions are significantly different between agencies;
- The application is shared by non-LE units in the agency (such as case management applications which are used throughout the case life cycle of complaint, investigation, enforcement, and litigation) causing additional costs and complexities in "splitting" the application.

Several categories of applications were widely used and seen as critical to the law enforcement mission. A cursory examination by the Team identified high level business requirements in these areas that are fairly consistent across agencies, and in some cases, a specific solution is already being used by numerous agencies. Because of the commonality in these areas, the Team believes these to be possible candidates for consideration. **However, it should be noted that every potential consolidation carries with it many issues that need to be considered that could result in additional costs or reduced benefits.** While each of these opportunities for consolidation seems deceptively simple, their complex issues require extensive and detailed investigation of the efficacy of consolidation and the identification of any benefits or cost savings.

Not all opportunities identified in this document may result in beneficial consolidations or efficiencies. Each area will require detailed business process analysis by the operational staff and extensive coordination between applicable agencies.

Extensive analysis and planning, ultimately including consideration of all system requirements and software licensing costs, is needed to determine full project costs, reduce risks, and improve chances for successful consolidation.

Training Management System

All Agencies track the training that their officers attend. Some of these training records are sent to FDLE to show compliance with mandatory retraining and some are kept at the Agency for internal record keeping procedures.

All Agencies could benefit by having a central application that could allow for them to track training and could allow for FDLE to automatically pull the records needed for mandatory retraining. Some agencies have taken steps to form a committee of training staff to begin the review of current business processes and requirements and create standardized processes and requirements that will facilitate the development of a consolidated IT solution.

Policy Management System

Systems used to manage policies throughout their entire life cycle are very important to law enforcement for purposes of accreditation, standards, and quality assurance. Policy Management systems aid in the development and maintenance of policies, as well as providing tracking of the acknowledgment and verification of policy review and acceptance by law enforcement staff. Accountability of effective development, awareness, and adherence to policy is a critical factor in the accreditation process. A centralized system for use by all law enforcement units would reduce duplicity and improve efficiency and accountability.

Evidence Management System

All Agencies have to track evidence seized by their officers. Most of the Agencies have multiple locations throughout the state to store evidence. All Agencies follow the same guidelines on how the evidence is handled, stored and processed. Each agency currently has an evidence tracking system developed or purchased to meet their tracking needs.

Agencies could benefit from a central evidence management system to track evidence. It could also allow the Agencies to “share” evidence facilities as they could all use the same software. For example, if a Trooper seizes evidence in an area where there is no FHP evidence facility but a DEP facility was nearby, the trooper could store the evidence there. It could save man hours and fuel costs of driving out of the way to drop off evidence.

Some Evidence Management Systems currently in use actually receive data automatically from the Records Management System. Any solution that does not maintain the same level of integration or automation could actually result in duplicate data entry and reduced efficiency for some users.

Records Management System

The larger Patrol Agencies (FHP, FWC) all currently use a Records Management System (RMS) from the same vendor. If the systems were consolidated it could reduce the cost associated the maintenance for the software and hardware. DHSMV currently hosts an RMS system used by FHP, DEP and SFM. Some Records Management Systems currently in use actually transfer property and evidence into those respective systems or modules. Any solution that does not maintain the same level of integration or automation could actually result in duplicate data entry and reduced efficiency for some users.

Property Management System

Most of the Agencies track issued property. The property is generally tracked by whom it is assigned to. The property is not just the items which are tracked by FLAIR but items of intrinsic value to law enforcement, such as firearms, computers, body armor, etc. Some Property Management Systems currently in use actually are integrated with the agency’s non-LE inventory, including an automated interface to the FLAIR Inventory Module. Any solution that does not maintain the same level of integration or automation could actually result in duplicate data entry and reduced efficiency for some users.

6B. CONSOLIDATION CRITICAL SUCCESS FACTORS

It is important to note that every potential consolidation carries with it many issues that need to be considered that could result in additional risk, time or costs, or possibly in reduced benefits. Extensive analysis and planning is needed to determine full project costs, to reduce risks, and to improve chances for successful consolidation.

Currently, each agency has its own services and processes (that may be similar, but are different in many critical ways) that drive the needs of Agency IT. The services and business processes of all agencies should be analyzed and preferably integrated to the extent possible, prior to any attempt to consolidate the IT supporting those business processes.

Critical success factors include, but are not limited to:

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. This business process analysis will identify specific areas that are appropriate candidates for IT consolidation or efficiencies and provide standard requirements for this service. This information can then be provided to the IT units for systems planning to meet the requirements and process identified. In addition to detailed business requirements and

process analysis, it is important to address specifics such as: software licensing, hardware capacity and refresh schedules, system and database interfaces, data migration and/or access to legacy data, mobile technologies, and consolidated dispatch.

2. **Planning** - Sufficient time for consolidation research and planning is critical to the success of the effort. It is critical that the services and business processes of all agencies must be studied and integrated prior to any attempt to consolidate any IT supporting those business processes. The planning phase must include all affected parties to an appropriate degree.
3. **Project Management** – Unmanaged IT projects have a much higher rate of failure. Use of standard project management practices is recommended, including: designation of an experienced project lead, establishment of a detailed project plan with a clear scope and reasonable timeline, commitment of sufficient resources, effective project governance including risk identification and mitigation, and ongoing communication and coordination.
4. **Comprehensive IT Assessment** – When any consolidation is being considered, a comprehensive IT assessment should include applications, infrastructure, desktops, data, support and staffing. IT staff from all of these areas, as well as knowledgeable business/LE staff, should be included to determine all of the tasks, costs and risks associated with the consolidation in question.
5. **IT Staffing** – Every effort should be made to retain the knowledgeable and skilled staff that currently manage and support the LE systems within the agencies, through consolidation and beyond. Consolidation decisions should not be made under the assumption that savings can be immediately achieved through the reduction of IT. When consolidations are planned, careful consideration must be given to the full range of skill sets, duties and institutional knowledge required for system maintenance / 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.
6. **Primary Data Center Coordination** - Complications and complexities are multiplied once systems are centrally located in a Primary Data Center (PDC). The regulations, rules, and service agendas of all agencies and the PDC will require much more time to integrate than had been planned. In addition, the current establishment of the PDC's as individual entities (each with their own policies, procedures and standards) and the initial movement of legacy agency systems into the Centers, provide many unknowns that must be addressed in the planning of any future consolidation efforts.
7. **Primary Data Center Budgeting** – current PDC funding methodology of Zero Balance provides no funding for additional hardware, software, or other expenses that may be necessary to the success of the project. The PDC must have flexible funds to provide service to the agencies and deal with equipment problems and disaster recovery considerations.

7. RECOMMENDATIONS

The Information Technology Team recommends the following:

1. Consider the following application systems for possible centralization or consolidation, which are used similarly by most law enforcement units: **Training Management, Policy Management, Evidence Management, Records Management, and Property Management Systems.** However, comprehensive analysis of agency-specific business requirements, processes, and interfaces is warranted prior to any final decision.

2. Any potential consolidation of law enforcement should include comprehensive and effective planning, business analysis, coordination and communication, addressing all areas of information technology and utilizing accepted practices in project management. LE consolidation may impact and be impacted by the AEIT Data Center Consolidation and other Enterprise Consolidation efforts currently underway, and such potential impacts should be considered during analysis and planning of any proposed LE consolidation.
3. Interagency workgroups made up of both business (LE) and IT personnel should be established for detailed study and business process analysis of any recommended area of consolidation or major efficiency initiative. It is critical that the services and business processes of all agencies must be analyzed from an operational perspective prior to any attempt to consolidate any IT supporting those business processes.
4. The importance of retaining skilled and knowledgeable IT staff should not be underestimated. The State should make every attempt to retain IT staff throughout the consolidation process, during which time agency-specific technical and institutional knowledge is especially critical. No reduction in IT staff should be attempted until well past the successful completion of consolidation, and even then reduction should only be through normal attrition.
5. The Agency for Enterprise Information Technology should be given the necessary resources and authority to take action to implement and comply with requirements and recommendations from the Law Enforcement Data Center Requirements Workgroup. Specifically, Data Center facilities MUST comply with federal CJIS Security Policy and MUST meet all requirements for high availability, including sufficient failover and disaster recovery to geographically dispersed locations.
6. The state should undertake a comprehensive assessment of the Primary Data Center system with specific focus on facilities, security, staffing, tools, processes, controls and transparency.
7. Any future recommendations to address the consolidation of IT functionality across state criminal justice and law enforcement agencies should comply with standards as adopted by the CJJIS Council in accordance with its duties stated in Florida Statute 943.08 and be reviewed by the Council as necessary. (See Appendix C for additional information on the CJJIS Council)

APPENDIX A – LE DATA CENTER CONSOLIDATION RECOMMENDATIONS

(Produced by CIO Council AEIT Advisory Committee Law Enforcement Workgroup, October 12, 2010)

Chief Information Officers Council – AEIT Advisory Committee
Law Enforcement Data Center Requirements Workgroup
Law Enforcement/Criminal Justice
Data Center Consolidation Recommendations

1. The State's Primary Data Centers (PDC or Data Center) shall comply with all current and future versions of the FBI Criminal Justice Information Services (CJIS) Security Policy.
2. Primary Data Centers should designate all Data Center positions as positions of special trust. Positions of special trust can be declared by the agency head. Positions of special trust require a level 2 fingerprint check. The purpose for this designation is to enable the PDC to perform a criminal history check where necessary, but does not replace the check to be performed by the lead Criminal Justice Agency in the Data Center.
3. Primary Data Centers should request retention of fingerprints for arrest notification on all applicants to FDLE.
4. Each PDC should develop and adhere to policies and procedures that comply with Florida's Criminal Justice User Agreement, Section 3, Paragraph 1, for responding to notification of an arrest due to retention of fingerprints or reporting of that arrest via some other mechanism.
5. The AEIT should amend F.S. 110.1127 (a) to allow for the inclusion of contractors as position of special trust which would provide non-criminal justice agencies with the ability to conduct security background checks, including fingerprinting on contractors. Currently non-criminal justice agencies are restricted to conducting background checks on employees only however most agencies including primary data centers employ contract staff to perform information technology work that is either similar or identical to work performed by full-time equivalent (FTE) staff or contract staff may be hired to work on specific projects where they have access to the same systems or data as FTE's. The FBI considers criminal history background checks conducted by a CJ agency for site security to be a criminal justice purpose. (28 CFR 20.33 and s.943.053 (a)).
6. Law Enforcement/Criminal Justice Agencies have varying background processes that are required for staff, prior to initial employment, above and beyond the level two fingerprint-based criminal history record check required by the FBI's CJIS Security Policy. The Law Enforcement workgroup considered the background processes of agency workgroup members, with FDLE's background process being the most stringent. The workgroup recommends that Primary Data Centers that process or store Law Enforcement/Criminal Justice (CJ) data or systems should adopt a standard background process that includes the components listed below. These background processes would include support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas unless these individuals are escorted by authorized personnel at all times. Non-PDC Agency staff having unescorted physical access to the Data Center would go through the same background process as Data Center staff. Recommended components are divided into two categories, those background processes that the Primary Data Center has access

to the information in order to complete and those background process that a Law Enforcement or Criminal Justice Agency should complete due to access to the information. The workgroup considered it important to point out that these additional screening methods are recommended, but subject to definition of policies and guidelines that would reduce potential inconsistency in application and interpretation of results across data centers. In addition, advanced notification to existing employees of these new processes to ensure fairness would be extremely important. One final note regarding background processes, the workgroup considered but rejected credit checks as part of the background process due to the potential impact on existing employees. This does however remain a requirement of FDLE.

PDC Conducted Background Processes:

- a. Drug Screen
- b. Employment Verification for past 5 years
- c. Education Verification
- d. Military/Selective Service records verification
- e. Birth and Citizenship Verification (Birth Certificate &/or Immigration & customs Enforcement documentation)
- f. Three Personal References
- g. Internet Search (i.e. Facebook, Google, MySpace) – this should be based on further definition of policies and guidelines
- h. Driver License

Law Enforcement or Criminal Justice Agency Conducted Background Processes:

- a. Local Law Enforcement Record Check
 - b. State Attorney's Office Inquiry
 - c. Local and State Civil and Criminal Court Inquiries
 - d. Federal Civil and Criminal Court Inquiries (PACER System)
 - e. Check Commercially Available Databases
 - f. Other Criminal Justice Indices as Available
 - g. Limited checks on spouses and/or roommates should be performed
7. The Primary Data Centers should develop a policy regarding staff reporting of arrests and/or their involvement in investigations within a designated period of time (recommendation is within two business days). This should include any investigation of suspected illegal involvement (to include but not be limited to possession, use, sale and delivery) with controlled substances or other drugs.
 8. When multiple Criminal Justice agencies are housed in the same Primary Data Center, the CJ agencies will select a primary CJ agency to provide oversight regarding adherence to FBI CJIS Security Policies and to be responsible for conducting Criminal History Checks. This includes conducting level 2 background check (fingerprint based – as defined in F.S. 435.04) conducted by the primary CJ agency and review process in accordance with the FDLE CJ User Agreement. Based on the review, the primary CJ agency will make a determination of eligibility.
 9. The CJ Agency selected within a Data Center to provide oversight and conduct fingerprint checks will be provided an Originating Agency Identifier (ORI) by FDLE specifically for the purpose of performing checks for the PDC.

10. As an option, the Primary Data Centers may acquire their own ORI as a non-criminal justice agency and conduct their own State and National Fingerprint Check under F.S. 110. This would allow the PDC to obtain their own criminal history results on applicants who may have been denied access by FDLE, and/or to receive arrest notifications on any other retained applicants the PDC chooses to conduct a fingerprint check for. This information could be used by the PDC if the Criminal Justice Agency that has Management Control denies access to current or prospective employees; the Data Center would then have information to understand the circumstances and to determine if the PDC's Inspector General needs to begin an internal investigation on any current employees.
11. The Primary Data Center should develop policies and procedures for handling the results of fingerprint based criminal history checks conducted by the designated primary CJ Agency in the Data Center. These policies and procedures should include notification to the staff and contractors who have physical or logical access, and other State agency personnel with unescorted physical access to the Data Center of the background requirements, what may constitute denial of access, how notification will be handled with the staff, how termination of access to the data center (logically and physically) will be handled, whether staff will be placed on administrative leave, etc. Policies and procedures will be consistent with the CJIS Security Policies. If the Primary Data Center chooses to conduct their own fingerprint checks, the policy should also include how the receipt of arrest notifications for retained applicants will be handled and the process for conducting any internal investigations that may occur as a result.
12. Primary Data Centers should develop and implement a written policy for the discipline including dismissal and/or criminal prosecution of employees who violate the CJIS Security policy or other security requirements.
13. Primary Data Centers should develop a policy regarding Professional Standards of Employee Conduct that addresses such items as avoiding the appearance of impropriety, drug free workplace, acts of misconduct and work standard violations, ethics, release of confidential information, dual employment and drug testing.
14. Primary Data Centers should communicate with the PDC Board, employees, and contractors regarding changes in policy due to the CJIS Security Requirements and what the implications are as well as provide them with new policies and procedures that need to be followed. PDCs should also develop a list of staff and contractors that will need access and prepare well in advance of moving day for the CJ Agency to begin the process of fingerprint checks as this can be time consuming. PDC staff will need to be notified of the specific documents they will need to bring with them at the time they are to be fingerprinted and should be made aware well in advance of the process and potential outcomes.
15. Primary Data Centers that house or are planning to house FBI/CJIS data should develop a written plan for how they will meet the requirements of the CJIS Security Policy. The plan must then be reviewed with and approved by the CJIS Systems Officer (CSO). This should be done well in advance of the move date for any Criminal Justice Agency into the Primary Data Center.
16. The Primary Data Center should request a pre-assessment to be conducted by FDLE in order to ensure compliance and resolve any outstanding issues prior to the move of any CJ Agency.
17. Prior to the move of any CJ Agency into a Primary Data Center, the Primary Data Center must develop a written plan for how they will meet any requirements specific to that CJ Agency that are above and beyond the requirements of the CJIS Security Policy, including but not limited to availability requirements.
18. The CJ Agency shall execute a Management Control Agreement with the State Primary Data Center expected to house their CJIS system/data. This agreement includes the terms and

conditions of the FDLE CJIS User Agreement that is executed with each CJ Agency. It also includes the requirements of the Federal Regulations 28 CFR (part 20), 23.20 and 20.21.

19. In conjunction with the Criminal Justice Agencies, FDLE will develop a standard template for the *Management Control Agreement* that is required by the FBI to be executed between each CJ Agency and the Primary Data Center housing FBI CJIS data.
20. Primary Data Centers shall have documented procedures in place to monitor all CJIS security policies with appropriate points of contact as coordinated with the FDLE/CJIS Information Security Officer (ISO).
21. Primary Data Centers shall prioritize the recovery of Criminal Justice systems and data over all others in the Data Center. (reference CJIS Security Policy version 5.0 3.2.2 (3) (a) and (b))
22. Primary Data Centers shall prioritize public safety network traffic giving priority within Public Safety to Criminal Justice systems and data. (reference CJIS Security Policy version 5.0 3.2.2 (3) (a) and (b))
23. Any agreement between a primary data center and a private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI (acting for the U.S. Attorney General), as referenced in Title 28 CFR 20.33 (a) (7). Private contractors who perform the administration of criminal justice shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.
24. In conjunction with F.S. 943.0311, all Primary Data Centers should be designated as Critical Infrastructure and FDLE should be requested to perform vulnerability assessments. Results of the assessments should be shared with the Criminal Justice Agencies that are planned to be housed in the specific Primary Data Center. Plans should be developed to mitigate identified vulnerabilities prior to the occupancy of the Primary Data Center by any CJ Agency.
25. Primary Data Centers should have established policies and procedures for continuity of operations and emergency succession procedures for all critical data center positions.
26. Primary Data Centers should have established policies and procedures regarding an Inspector General's role in the coordination of and responsibility for activities that promote accountability, integrity and efficiency of the data center as delineated in Section 20.055, F.S.
27. Primary Data Centers should develop policies and procedures for preparing After-Action Reports (AAR) for all significant system outages or degradation of service. An AAR is an assessment conducted after a major event or outage that allows staff to discover what happened and why it happened, and to learn from that experience. It also provides the customer with a description of the outage, scope of the outage, the root cause of the outage, and preventive actions or proactive steps to be performed to prevent future outages.
28. There should be consistency with regards to disqualifiers for Data Center access under Florida law. One or more State Agencies (e.g. DJJ, DCF, etc.) have statutory employment disqualifiers that are different. If more than one Criminal Justice Agency is housed within a PDC, the primary CJA performing the fingerprint-based criminal history check is only adjudicating against the CJIS Security Policy and their agency's disqualifiers therefore, it is possible that the PDC board as the hiring authority may make an employment decision without the benefit of knowing the requirements of each agency. This is further complicated by the fact that the hiring authority is not provided the specifics of the background record check. The recommendation is that statute should be reviewed and all agency disqualifiers identified, then a single standard should be developed based on these disqualifiers for adjudication purposes (beyond the CJIS Security requirements) for the data centers to ensure consistency in the screening standard across all data centers.

APPENDIX B – LE DATA CENTER REQUIREMENTS WORKGROUP CHARTER

State of Florida Chief Information Officers Council

Agency for Enterprise Information Technology Advisory Committee

The Law Enforcement Data Center Requirements Workgroup

Charter & Overview Document

October 12, 2010

The following is a record of the changes that have occurred on this document from the time of its origination.

#	Change Description	Author	Date
1	Original draft	Nelson Munn	12/23/09
2	Added legal input from Lou Carroll	Nelson Munn	12/28/09
3	Group Additions/Changes	Workgroup	2/19/10
4	Pulled law/requirements section out to spreadsheet	Nelson Munn	3/3/10
5	Update by FDLE to Risks, Constraints and Other Considerations Sections	Penny Kincannon	3/14/10
6	Added acronyms, assumptions, constraints, and other considerations to word document	Penny Kincannon	5/13/10
7	FDLE completed writing of CJIS & FDLE requirements (spreadsheet) and provided to Nelson	FDLE	5/13/10
8	Added AEIT and FHP Requirements to spreadsheet	Amy Caldeira Steve Williams	6/10/10
9	Update to specific definitions and inserting a definition of terms	Tom Trunda	7/7/10
10	Revisions in LE Workgroup meeting to definition of terms, assumptions, risks, and constraints	Workgroup	8/13/10
11	Updated document change activity, workgroup membership, and outstanding issues sections	Penny Kincannon	8/15/10
12	In Workgroup meeting on 8/26/10 the team made additional modifications and additions to Section 9 Assumptions, Section 11 Constraints and Section 12 Other Considerations and updated Outstanding Issues.	Workgroup	8/26/10
13	Added new tasks to Outstanding Issues and accepted all track changes; removed Calea requirements (duplicates of CJIS).	Penny Kincannon	8/29/10
14	Moved the functional requirements to a word document/table due to the excel row limitation, combined requirements that had been split, combined "applies to" columns from one for each agency down to two; added an additional recommendation regarding after action report; updated several recommendations; updated AEIT requirements changes; added/clarified requirements regarding VLANS/firewalls/logical segmentation of CJ data from non-CJ data or encrypt data.	Penny Kincannon, Joey Hornsby	10/1/10
15	Added recommendation on notification of arrests, revised working on 11.7, discussed DOC recommendation with Doug, spelled out ORI, added recommendation on disqualifiers, summarized workgroup's recommendation on background process, added reference to recommendations in primary document and information on how requirements were derived; added cover page.	Penny Kincannon, Joey Hornsby, Larry Coffee, Workgroup Members contribution	10/11/10

The State of Florida’s CIO Council as part of their established Agency for Enterprise Information Technology (AEIT) Advisory Committee formed the Law Enforcement Data Center Requirements Workgroup in October of 2009 to address the unique business needs and concerns specific to the operation of law enforcement and criminal justice information systems and associated infrastructure in a shared computing facility. The Council invited all agencies with a law enforcement component to participate as well as the Agency for Enterprise Information Technology and the State’s Primary Data Centers. The workgroup came together to document Federal, State, and Agency law enforcement related laws, policies, and practices and the associated requirements for the State data center system. The workgroup also documented specific process and workflow related issues that need to be considered by data center managers as they offer services to law enforcement users. As discussions evolved and the first Criminal Justice Agency moved into a primary data center the LE Workgroup was asked to prepare a list of recommendations in addition to the documented requirements.

The work of the LE Workgroup has resulting in three documents which consist of the following:

- 1) *LE Workgroup Charter & Overview.doc* – this document references general information about the purpose behind the project, participants, definitions, and most importantly identifies assumptions, risks, constraints, and other considerations regarding Law Enforcement/ Criminal Justice Agency consolidation into a shared computing facility.
- 2) *LE Data Center Consolidation Requirements.doc* – this document provided as a separate attachment in MSWORD table format is a list of requirements provided by the participating LE agencies. See Section 7.0 for more details on the requirements document.
- 3) *LE-CJ Data Center Consolidation Recommendations.doc* – this document provided as a separated MSWORD document contains specific recommendations based on issues raised during the LE Workgroup meetings. The recommendations are not meant to be prescriptive in most cases but as a jump start for further discussion as there are some complicated issues. Others are simply to follow up on lessons learned after the first CJ Agency move into a PDC.

These LE Workgroup deliverable documents will be drafted and finalized by members of the workgroup and offered to the AEIT Advisory Committee as a final report. The AEIT Advisory Committee will then have the opportunity to provide it to the CIO Council for use in advising the AEIT regarding the state-wide data center system.

Name	Agency	Email Address
Abe Kani	Dept of Financial Services	abe.kani@myfloridacfo.com
Alan Neubauer	Supreme Court	neubauer@flcourts.org
Amy Caldeira	Agency for Enterprise Info. Tech	amy.caldeira@aeit.myflorida.com
Ben Hinkle	Dept of Transportation	Ben.hinkle@dot.state.fl.us
Benita Williams	Dept of Juvenile Justice	Benita.Williams@djj.state.fl.us
Brett Norton	Fish & Wildlife Conservation Commission	brett.norton@myfwc.com
Bruce McCormick	Dept of Legal Affairs	bruce.mccormick@myfloridalegal.com
Charles Murphy	Dept of Law Enforcement	CharlesMurphy@fdle.state.fl.us
Chris Sella	Fish & Wildlife Conservation Commission	chris.sella@myfwc.com

Law Enforcement Consolidation Task Force / Information Technology Team

Name	Agency	Email Address
Clyde Gaskins	Dept of Financial Services	Clyde.Gaskins@myfloridacfo.com
Craig Vollertsen	Fish & Wildlife Conservation Commission	Craig.Vollertsen@myfwc.com
Crill Merryday	Dept of Highway Safety & Motor Vehicles	CrillMerryday@flhsmv.gov
Dan Starling	Dept of Transportation	Dan.starling@dot.state.fl.us
Dave Kallenborn	Dept of Juvenile Justice	dave.kallenborn@djj.state.fl.us
Deborah Stevens	Dept of Legal Affairs	deborah.stevens@myfloridalegal.com
Denver Gordon	Dept of Law Enforcement	DenverGordon@fdle.state.fl.us
Diana Patterson	Dept of Highway Safety & Motor Vehicles	dianapatterson@flhsmv.gov
Doug Smith	Dept of Corrections	Smith.Doug@mail.dc.state.fl.us
Emery Gainey	Dept of Legal Affairs	Emery.Gainey@myfloridalegal.com
Gene Hatcher	Dept of Corrections	hatcher.gene@mail.dc.state.fl.us
Ignacio Sanchez	State Attorneys office	isanche@jud5.flcourts.org
Jeff Griffin	Dept of Agriculture	griffij@doacs.state.fl.us
Joey Hornsby	Dept of Law Enforcement	JoeyHornsby@fdle.state.fl.us
John Wade	Southwood Shared Resource Center	john.wade@ssrc.myflorida.com
John Willmott	Dept of Environmental Protection	john.willmott@dep.state.fl.us
Kevin Patten	Fish & Wildlife Conservation Commission	Kevin.Patten@myfwc.com
Kincannon, Penny	Dept of Law Enforcement	PennyKincannon@fdle.state.fl.us
Larry Coffee	Dept of Law Enforcement	LarryCoffee@fdle.state.fl.us
Lou Carroll	Dept of Corrections	carroll.lou@mail.dc.state.fl.us
Matt Stolk	Northwest Regional Data Center	matt_stolk@nwrdc.fsu.edu
Mike Russo	Agency for Enterprise Info. Tech	mike.russo@aeit.myflorida.com
Mitch Golloher	Dept of Environmental Protection	mitch.golloher@dep.state.fl.us
Nancy Kenyon	Northwood Shared Resource Center	Nancy_Kenyon@nsrc.myflorida.com
Nelson Hill	Dept of Transportation	nelson.hill@dot.state.fl.us
Pati Lytle	Dept of Agriculture	lytlep@doacs.state.fl.us
Roger Norris	Dept of Transportation	roger.norris@dot.state.fl.us
Steve Lyncker	Dept of Financial Services	Steve.Lyncker@myfloridacfo.com

Law Enforcement Consolidation Task Force / Information Technology Team

Name	Agency	Email Address
Steve Williams	Dept of Highway Safety & Motor Vehicles	stevewilliams@flhsmv.gov
Tammy Crummel	Dept of Corrections	crumel.tammy@mail.dc.state.fl.us
Tim Brown	Northwest Regional Data Center	Tim_Brown@nwrdc.fsu.edu
Tom Trunda	Dept of Transportation	tom.trunda@dot.state.fl.us
Willis Rabon	Dept of Financial Services	willis.rabon@myflorida.com

CALEA	Commission on Accreditation for Law Enforcement Agencies
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CHIS	Criminal History Information System
CJA	Criminal Justice Agency
CJIS APB	CJIS Advisory Policy Board
CJIS	Criminal Justice Information Services
CJNET	Criminal Justice Network
CJUA	Criminal Justice User Agreement
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officers
FBI	Federal Bureau of Investigations
FCIC	Florida Crime Information Center
ISM	Information Security Manager
ISO	Information Security Officer
LASO	Local Agency Security Officers
NCIC	National Crime Information Center

DEFINITION OF TERMS. Terms referenced in this document and the “*LE Data Center Consolidation Requirements*” word document shall have the meaning defined by National Institute of Standards and Technology Interagency Reports (NISTIRs), Federal Information Processing Standards (FIPS) and Special Publications (SP). Unless otherwise stated, all terms used in NIST publications are also consistent with the definitions contained in

the Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary and State of Florida Information Technology Resource Security Policies and Standards.

- 6.1. CJIS Security Policy related entries are based on version 4.5 as updated January 2010. Laws and Policies are captured in the requirements section of the attached "*LE Data Center Consolidation Requirements*" word document.
- 7.1. See attached "*LE Data Center Consolidation Requirements*". The vast majority of the requirements identified came directly from the FBI Criminal Justice Information Security Policy version 4.5. Requirements based on the CJIS Security Policy are focused on those that would be necessary for a governmental agency to follow and were not inclusive of those required if the data center were being managed by a non-governmental agency or private contractor. In addition, this list of requirements should not be considered a replacement for reading, understanding and following the totality of the CJIS Security Policy but is meant to highlight the most important requirements as they apply to data center consolidation and to provide some clarification regarding how some apply in a shared environment.
- 7.2. The Federal or State law or Agency Policy and Procedure has been cited for each requirement and requirements have been categorized according to the following areas although it should be noted that more than one category could apply:
 - Governance
 - Policy & Procedure
 - Personnel
 - Security
 - Operations
 - Availability
- 7.3. Each requirement is checked as applying either specifically only to FDLE or to Criminal Justice Agencies & Data Centers hosting FBI CJIS Data. There are two reasons for this: 1) FDLE serves as the State's CJIS Systems Agency and employs the CJIS Systems Officer for the State and as such has some very unique responsibilities. So these responsibilities are noted with a check as being unique to FDLE and 2) the background processes that FDLE employs are much more restrictive than other LE agencies and are therefore checked as unique to FDLE. Although the requirements document makes an attempt to stay away from unique agency service level agreement type requirements, those that have the potential to impact other agencies have been included.
- 8.1. In accordance with 28 CFR Part 23 Guideline (Criminal Intelligence Systems Policies) – subsection 23.3 Applicability, (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies. The State's Primary Data Centers would be considered such a project.
- 8.2. In accordance with 28 CFR Part 23 Guideline (Criminal Intelligence Systems Policies) – a project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information and the date of each dissemination outside the project shall be kept.
- 8.3. When multiple criminal justice agencies data and systems are housed in a primary data center the CJ agencies will select a primary CJ agency to assure data center adherence to FBI CJIS Security Policies. This includes conducting level 2 background check (fingerprint based – as defined in F.S. 435.04) conducted by the primary CJ agency and review process in accordance with the FDLE CJ User

Agreement. Based on the review, the primary CJ agency will make a determination of eligibility. FDLE is the designated CSA (CJIS Systems Agency) for Florida which is defined by 28 CFR 20.3(c) as "is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division." Facilities supporting FDLE are suggested to select FDLE as the primary CJ agency

- 8.4. The primary data center should work with the initial CJ Agency moving into the data center or the selected primary CJ agency to complete level 2 background checks on existing staff with logical or physical access to data and systems prior to any CJ agency moving into the data center. In addition, a process should be established for completing level 2 background checks on all potential staff prior to employment with the primary data center.
- 8.5. The provisions of the CJIS Security Policy "Security Addendum" apply to all Privatized (non governmental) State Primary Data Center personnel, systems, networks and support facilities supporting and/or acting on behalf of the CJ agency.
- 8.6. The term "FCIC" includes FBI Criminal Justice Information Systems Data as well as State of Florida Criminal Information.
- 8.7. Primary data centers must give priority to criminal justice network traffic over that of all others and must prioritize the recovery of Criminal Justice systems and data over all others in the Data Center.
- 8.8. The State's Primary Data Centers shall assign a Security Officer accountable for the management of the security program and to ensure compliance with the FBI CJIS Security Policy and the Management Control Agreement. This will be the same person designated as the Information Security Manager in F.S. 282.318.
- 8.9. The Primary CJ Agency shall work in conjunction with the Primary Data Center's Information Security Officer/Manager and the CJIS Systems Agency (FDLE) to ensure the Primary Data Center's compliance with the FBI CJIS Security Policy.
- 8.10. It is the responsibility of the individual CJ Agency to ensure compliance of the CJ applications with the FBI CJIS Security Policy with the Data Center providing a supporting role in this process where necessary.
- 8.11. The Primary Data Centers will develop and implement standard operating procedures based on best practices for Data Centers.
- 9.1 Bandwidth Requirements necessary between current data center facilities and the State's Primary Data Centers. Agencies that offer 10/100/1000 connectivity per desktop to their users today that are collocated with the servers that house their applications and data enjoy gigabits of aggregated throughput to these systems. Impact to bandwidth has the potential to impact officer safety and public safety when Criminal Justice and Law Enforcement applications and data are affected. In a consolidated data center environment the users will have to share a much smaller link to all of these systems and user productivity as well as user satisfaction with Information systems may suffer.
- 9.2 Some agencies make use of backup data shares for local data files and email archives to ensure users never lose critical mail or documents. Reduced bandwidth may impact user desktop backup functionality as well as the automatic/remote installation of application software including office suite products and antivirus software onto user desktops remotely from servers.
- 9.3 Lack of redundancy or disaster recovery planning on the part of the primary data centers for systems moving to the data centers. Failover to recovery sites is still the responsibility of the LE/CJ Agency although responsibility/administration for the agency systems may have been transferred to the primary data center. The agency is still responsible for replication and maintenance of the DR site.
- 9.4 LE/CJ agencies are extremely concerned with discussion regarding the use of one primary data center as the disaster recovery site for another primary data center as this does not meet the best practice of being

geographically dispersed. It would however be a good idea from a backup perspective or to meet the requirement of specific public safety systems that may require high availability.

- 10.1 Financial impact of Bandwidth Requirements with users housed at one location and servers at another, especially for those applications that are client-server based or applications that are graphically or image intensive.
- 10.2 Vendor managed systems that are housed at the CJ agency and have contract support staff collocated with the equipment per the contract (i.e. MorphoTrak fingerprint systems and Regional Law Enforcement Exchange System (R-LEX), DOC Canteen system) and/or that are managed remotely by the vendor (SmartCop).
- 10.3 The State's Primary Data Centers must execute a Management Control Agreement with each CJ Agency supported. This agreement includes the terms and conditions of the FDLE CJIS User Agreement that is executed with each CJA. It also includes the requirements of the Federal Regulations 28 CFR (part 20), 23.20 and 20.21.
- 10.4 The CJ Agency maintains the authority to approve or deny staff having logical or physical access to systems used to transmit, store or process FBI/CJIS data. This includes the background process needing to be completed by a CJ Agency, as opposed to by a Data Center directly or other managing non-CJ Agency. It also includes review and decision making authority regarding background results and post background subsequent arrest notification.
- 10.5 Responsibility for the management of security control shall remain with the criminal justice agency. Security control includes the authority to set and enforce policy governing the operation of computers, circuits and telecommunications terminals used to process, store or transmit CJIS data and to guarantee the priority service needed by the criminal justice community.
- 10.6 As coordinated through the State of Florida's CSA, each primary data center as per their management control agreement with the CJ Agency shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of DOJ Order 2640.2E.
- 10.7 The data center must incorporate the CJIS Security Addendum into any contract with a private contractor for any services that would involve access to systems used to process or store FBI CJIS data. This would include contracts to support data center hardware, operating systems, monitoring software, other utility type software that may have access to these systems, etc. The security addendum requires the contractors to follow specific security policies and ensures they meet the same training and certification criteria required by governmental agencies performing a similar function. These requirements have the potential to add additional cost and constraints to the services provided by the vendor.
- 10.8 All private contractors who have been permitted to access the CJIS record information systems shall abide by all aspects of the CJIS Security Addendum. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.
- 10.9 Physical security perimeters for the PDC as defined by the CJIS Security Policy shall be defined by the CJIS Systems Officer (FDLE).
- 10.10 FDLE and FBI CJIS data can only be accessed and disseminated for an authorized purpose. This includes maintenance of an IT System. CJIS systems data is sensitive information and security shall be afforded to prevent any unauthorized access, use or dissemination of the information. Improper access, use and/or dissemination of CHRI and hot file information is serious and may result in the imposition of administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.
- 10.11 The State's Primary Data Centers shall educate employees who work on any components utilizing CJIS data through the CJIS Online Security Training program conducted by FDLE as per the requirements in the CJIS Security Policy & FDLE Policy and Procedures.

- 10.12 The State's Primary Data Centers must comply with all current and future versions of the FBI CJIS Security Policy. New changes in the CJIS Security Policy (Version 5.0) are estimated to be in effect by January 2011.

- 11.1 Consolidating all Florida Public Safety Entities in one or two facilities introduces risk and creates an attractive target from a homeland security perspective. In addition, this creates a higher risk of failure for criminal justice and law enforcement systems.

- 11.2 The State's Primary Data Centers are expected to provide data center physical interior/exterior facility security; redundant environmental (power/HVAC) capacities and communications equipment backup with physical security to mitigate any impact to Law Enforcement operational capabilities and Officer Safety concerns. Access to the CJIS systems must be secure and maintained at the highest level of operational availability to meet Law Enforcement support requirements.

APPENDIX C – CRIMINAL & JUVENILE JUSTICE INFORMATION SYSTEMS COUNCIL

Duties of the Criminal and Juvenile Justice Information Systems (CJJIS) Council are statutorily defined in F.S. 943.08.

943.08 Duties; Criminal and Juvenile Justice Information Systems Council.—

- (1) The council shall facilitate the identification, standardization, sharing, and coordination of criminal and juvenile justice data and other public safety system data among federal, state, and local agencies.
- (2) The council shall adopt uniform information exchange standards, methodologies, and best practices, applying national standards and models when appropriate, in order to guide local and state criminal justice agencies when procuring, implementing, or modifying information systems.
- (3) The council shall provide statewide oversight and support the development of plans and policies relating to public safety information systems in order to facilitate the effective identification, standardization, access, sharing, integrating, and coordinating of criminal and juvenile justice data among federal, state, and local agencies. The council shall make recommendations addressing each of the following:
 - (a) Privacy of data.
 - (b) Security of systems.
 - (c) Functional and information sharing standards.
 - (d) Accuracy, timeliness, and completeness of data.
 - (e) Access to data and systems.
 - (f) Transmission of data and information.
 - (g) Dissemination of information.
 - (h) Training.
 - (i) Other areas that effect the sharing of criminal and juvenile justice information and other public safety system information.
- (4) The council shall provide oversight to the operation of the Criminal Justice Network (CJNet) for which the department shall serve as custodial manager pursuant to s. 943.0544. Criminal justice agencies participating in the Criminal Justice Network shall adhere to CJNet standards and policies.

APPENDIX D – GLOSSARY OF ACRONYMS & ABBREVIATIONS

AAR	After Action Report
AEIT	Agency for Enterprise Information Technology
AGO	Attorney General's Office
ATMS	Automated Training Management System
BIS	Biometric Identification System
CCH	Computerized Criminal History

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CJ	Criminal Justice
CJA	Criminal Justice Agency
CJIS	Criminal Justice Information Systems
CPCU	Child Predator Cybercrime Unit
CSA	CJIS Systems Agency
CSO	CJIS Systems Officer
DBPR	Department of Business and Professional Regulation
DCF	Department of Children & Families
DEP	Department of Environmental Protection
DFS	Department of Financial Services
DJJ	Department of Juvenile Justice
DOACS	Department of
DOC	Department of Corrections
FBI	Federal Bureau of Investigation
FCIC	Florida Crime Information Center
FDLE	Florida Department of Law Enforcement
FHP	Florida Highway Patrol
FLEX	Florida Law Enforcement eXchange
FMP	Florida Marine Patrol
FTE	Full Time Equivalent
FWC	Florida Wildlife Commission
GIS	Geographic Information System
HSMV	Highway Safety & Motor Vehicles
IRM	Information Resource Management
IT	Information Technology
LECTF	Law Enforcement Consolidation Task Force
LE	Law Enforcement
MEPIC	Missing & Endangered Persons Information Center
NCIC	National Crime Information Center
ORI	Originating Agency Identifier
OCETS	Online Curriculum Electronic Tracking System
PDC	Primary Data Center
RMS	Record Management System
R-LEX	Regional Law Enforcement eXchange
SFM	State Fire Marshall
VPN	Virtual Private Network