ROY COOPER
ATTORNEY GENERAL

State of North Carolina

Department of Justice
PO Box 629
Raleigh, North Carolina
27602

March 7, 2012

Senator Harry Brown
Senator Thom Goolsby
Representative Leo Daughtry
Representative Shirley B. Randleman
Co-Chairs, Appropriations Subcommittees on Justice and Public Safety

Mark Trogdon
Acting Director, Fiscal Research Division

North Carolina General Assembly
Raleigh, North Carolina 27601-1096

RE: Criminal Information Database Study by the North Carolina Department of Justice

Dear Members:

In accordance with Section 16.6 of the Current Operations and Capital Improvements Appropriations Act of 2011, please find the attached study from the North Carolina Department of Justice on the CIIS Criminal Information Database.

Thank you for the opportunity to provide this information. We would be happy to respond to any questions you may have regarding this report.

Very truly yours,

Kristi Hyman
Chief of Staff

KH/ml

cc: Kristine Leggett
Fiscal Research Division

Criminal Information Database Study

Contents

1. Introduction

In Section 16.6 of the Current Operations and Capital Improvements Appropriations Act of 2011, the General Assembly of North Carolina included a provision for a Criminal Information Database Study by the NC Department of Justice (DOJ) that stated:

> *"The Department of Justice shall issue a request for information to determine the cost to have a private company maintain the software required for criminal information databases managed by the Criminal Information Division. The Department of Justice shall report the results of this request for information to the Chairs of the House and Senate Appropriations Subcommittees on Justice and Public Safety and to the Fiscal Research Division by March 1, 2012."*

The provision as worded brought up four issues within DOJ as to its scope and intent, each of which prevented DOJ from issuing a Request for Information (RFI) in the absence of clarification from the General Assembly. The first issue is with the term "criminal information database". The Criminal Information and Identification Section (CIIS) within the State Bureau of Investigation (SBI) has management control over numerous criminal information systems as well as information systems used by SBI and other law enforcement agencies to perform functions established by non-criminal statutes, such as civilian criminal history background checks. Additionally, the "database" software is just one of many components comprising each of these information systems. DOJ requests direction as to which specific CIIS systems should be included in the RFI and whether DOJ is to seek cost information for maintenance by a private company for just the database software components or the entire systems. The second issue is that "maintenance" is only one of many technical activities required for effective operation of CIIS's criminal information systems. DOJ requests direction as to whether the intent of the provision is to determine costs for software maintenance only by a private company of CIIS's criminal information systems or to determine costs for a private company to perform all technical activities required for successful operation of these systems or some subset of these technical activities. The third issue is that maintenance (and various other technical operational responsibilities) of many of CIIS's criminal information systems is already performed by private-sector companies under contract with DOJ. Moreover, some of these systems are proprietary systems that were provided by the vendor contracted to do the maintenance and cannot be maintained by any other company as a condition of that vendor's software license agreement with DOJ. DOJ requests direction as to whether the RFI should include maintenance of systems whose maintenance is already outsourced to a private sector company or just those systems that are maintained entirely by DOJ Information Technology Division (ITD). The fourth issue is with the term "a private company". DOJ requests clarification as to whether this means that the RFI must require responses for maintenance of all of CIIS's criminal information systems from each bidder or whether DOJ can accept proposals for maintenance of a subset of those systems that best match the company's capabilities and capacity. DOJ also requests clarification as to whether this term simply means a non-governmental business entity or more specifically a privately-held company whose shares are not publicly traded.

To assist the General Assembly in clarifying the intent of this provision, DOJ respectfully submits the following Criminal Information Database Study, which includes the following:

- an explanation of each type of technical activity (maintenance or otherwise) required for effective operation of an information system,
- a listing and description of each CIIS information system,
- the current approach (internal or outsourced) to maintenance and other technical operational activities for each CIIS information system and maintenance costs, and
- options and for transitioning each CIIS information system to be vendor-provided and vendor-maintained, including any financial, legal, technical, and operational concerns for each option.

2. Definition of Maintenance and Other Technical Operational Activities

After an information system is implemented to support one or more business functions, there are many technical activities that must be performed subsequent to that implementation in order to ensure that the system continues to work as needed for the business. These activities can be divided into five categories: software hosting, software operations, user support, software maintenance, and retirement / replacement.

Software hosting is the provision, maintenance, and operations of the computing and data storage equipment, data communications equipment and services, physical facilities, electrical power, and security and environmental controls required by the software comprising an information system.

Software operations are the routine technical activities performed to ensure correct functioning and continued availability of the system. Software operations may include activities such as performing backups and restores, monitoring software performance and error logs, performing data quality checks, correcting data problems, rerunning failed transactions, managing software license compliance, ensuring disaster recovery readiness of the software and its data, and routine system and database administration.

User support is focused on enabling people to begin using a system and continue to use the system effectively over time to perform their job function. User support activities may include setting up user accounts, installing and configuring software on the user's computer, providing user training and documentation, answering user questions regarding proper usage of the system, troubleshooting system problems with the user and providing workarounds where possible, and generating ad hoc reports on system data that is unavailable through the software capabilities provided to the user.

Software maintenance includes three types of maintenance: corrective, adaptive, and perfective. The purpose of corrective maintenance is to fix problems in the software that are discovered after implementation. Corrective maintenance generally involves identifying the source of the problem, making software coding and/or configuration changes to fix the problem, verifying that the fix works, and deploying the fix. The purpose of adaptive maintenance is to change the system so that it continues to be useful in a changing technical and business environment. Adaptive maintenance for technical reasons may include patches and upgrades to newer versions of operating systems and other software upon which the system relies or making changes to the software to accommodate users using new types of computing equipment with new types of software to access the system. Adaptive maintenance for business reasons may include making changes in the software to support modified business processes and organizational structures or to reflect changes in the laws governing the business functions that the software supports. The purpose of perfective maintenance is to improve the performance, maintainability, reliability, and/or usability of the system. Perfective maintenance typically involves identifying, prioritizing, and selecting improvements, making software coding and/or configuration changes to achieve the improvements, verifying that the changes work, and deploying the changes.

Retirement / replacement is an extension of software maintenance that marks its end. At some point in the life of an information system, corrective, adaptive, and perfective maintenance will likely cease to be a cost effective method of supporting the business functions that the software was originally designed to support, often because either the needs of the business have changed too dramatically or the technology has become obsolete and unsupportable with no path available to upgrade the technology. At this point, business needs are reevaluated, potential solutions are examined, and if warranted a new system is implemented to meet the needs of the business. The appropriateness of building the new system internally or purchasing it from an external vendor or some combination thereof as well as how the maintenance and other technical operational activities for the system will be performed is evaluated in terms of what is in the best interest of the business.

3. CIIS Criminal Information Systems

SBI's Criminal Information and Identification Section (CIIS) has management control over a wide array of criminal information systems as required to meet SBI's statutory responsibilities as defined in the following North Carolina General Statutes: 114-10, 114-19, Article 27A of Chapter 14, Article 54B of Chapter 14, Article 5 of Chapter 15A, 15A-502, and 15A-1382. CIIS also has management control of several information systems that DOJ does not consider to be criminal information systems, but may interface with criminal information systems for various reasons. An example of such a system would be the applicant processing system which interfaces with the fingerprint system for purposes of performing civilian criminal history background checks as called for in dozens of General Statutes. These non-criminal information systems within CIIS are not included in this study. The Attorney General has vested responsibility to provide all information technology services required to support DOJ's statutory responsibilities and associated business functions, including those responsibilities and functions that exist within SBI, with DOJ's Information Technology Division (ITD). To meet its responsibilities, ITD provides some information technology services directly using its staff, equipment, and facilities and contracts with private-sector companies and external public-sector agencies (i.e. State Information Technology Services) for the provision of other information technology services in a manner that best serves the interests of DOJ and law enforcement agencies statewide and is compliant with applicable state and federal law, rules, and regulations.

The criminal information systems within CIIS are as follows:

- Law Enforcement Message Switch (LEMS)
- Omnixx Force, Trainer, Charts, Alerts, and DMXLive
- Statewide Automatic Fingerprint Identification System (SAFIS)
- Computerized Criminal History (CCH)
- Sex Offender Registry (SOR)
- Sex Offender Registry Tracking System (SORTS)
- Sex Offender Registry Public Website
- Sex Offender Registry Mobile App
- Concealed Handgun Permits (CHP)
- EVOLVE
- Expungement
- Recovered Vehicles
- Crime Analysis Management System (CAMS)
- Crime Reporting
- Traffic Stops

In addition, NC-DEx, which is currently being implemented, will be managed by CIIS when it goes into production in July 2012.

The remainder of this section describes the purpose of each of these CIIS criminal information systems, the maintenance and technical operations approach and maintenance costs, and options for transitioning to private company maintenance, including financial, legal, technical, and operational concerns for each option.

Note that software hosting costs are not addressed because all software is hosted at the DOJ Data Center. The costs of running this data center are essentially fixed, so there are no cost savings to be realized by

hosting certain applications outside of the DOJ Data Center. In fact, doing so would be more expensive. Additionally, many of these systems require communications with the FBI network which is only accessible via the DOJ network, so again software hosting outside of the DOJ Data Center is not an option.

Internal DOJ ITD staff costs for software operations, user support, and software maintenance are expressed in full time equivalents (FTE's). A reasonable, fully loaded (including benefits and overhead) annual cost per ITD FTE would be $82,000. The maintenance fees paid for general server software, such as operating systems and relational database management software, that supports the CIIS systems is not included in this analysis because those fees would have to be paid regardless of whether the system was maintained by DOJ or a private company unless the system were to be replaced with different technologies.

Law Enforcement Message Switch (LEMS)

Purpose of System

LEMS is a message switch that transfers law enforcement information throughout the State of North Carolina and to national agencies, NCIC and NLETS. It is the heart of the State's criminal information network, which is relied upon by approximately 20,000 law enforcement officers in NC and indirectly by hundreds of thousands of law enforcement officers nationally to access NC criminal information, DMV information, and other information necessary for law enforcement to protect the public. LEMS connects either directly or indirectly with hundreds of databases in NC agencies, in federal agencies, and in other states and nations. Law enforcement officers access the information available in LEMS either through the Omnixx Force application (described separately) or through their agencies' own mobile or computer-aided dispatch systems through interfaces to LEMS coordinated with DOJ. The database within LEMS does not contain criminal information per se, but rather information necessary for the message switch to work and for users and other systems to connect to it.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. Given the mission-critical nature of this system, it is monitored continuously. LEMS software operations consume approximately 1 FTE of ITD staff.
- User support is performed by DOJ ITD staff on a 24 x 7 x 365 basis. LEMS user support consumes approximately 4 FTE of ITD staff. User training is provided by SBI staff, consuming approximately 3 FTE of SBI staff.
- Software maintenance of the Unisys LEMS/JX message switch software is performed by the vendor Unisys at a cost of approximately $85,000 per year. DOJ ITD staff performs maintenance of LEMS functions specific to its implementation within NC. Frequent changes to the transactions in LEMS are required to comply with changes in federal systems and to accommodate changes in NC laws. LEMS software maintenance consumes approximately 1 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

Software maintenance for LEMS is already performed by a private company – Unisys.

Omnixx Force, Trainer, Charts, Alerts, and DMXLive

Purpose of System

Omnixx Force is the primary system that law enforcement officers use to access the information available via LEMS. Omnixx Trainer is used by SBI to manage training classes and administer tests to certify users of Omnixx Force and LEMS. Omnixx Charts and Alerts and DMXLive are used by SBI to monitor usage of Omnixx and LEMS, to perform investigations on inappropriate use, and to perform other intelligence functions. The databases for Omnixx Force and Trainer and DMXLive do not contain criminal information per se, but rather information necessary for the software to work and information about users, such as login credentials, training, and Omnixx certifications. The Omnixx Charts and Alerts database contains copies of criminal information in the form of copies of all LEMS inquiries and responses from the prior 12 months.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. Given the mission-critical nature of this system, it is monitored continuously. Omnixx software operations consume approximately 1 FTE of ITD staff.
- User support is performed by DOJ ITD staff on a 24 x 7 x 365 basis. Omnixx user support consumes approximately 3 FTE of ITD staff. User training is provided by SBI staff, consuming approximately 3 FTE of SBI staff.
- Software maintenance of the Omnixx software is performed by the vendor Datamaxx at a cost of $179,100 per year. DOJ ITD staff performs maintenance of Omnixx functions specific to its implementation within NC. Frequent changes to the transactions in Omnixx are required to comply with changes in federal systems and to accommodate changes in NC laws. Omnixx software maintenance consumes approximately 1 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

Software maintenance for Omnixx is already performed by a private company – Datamaxx.

Statewide Automatic Fingerprint Identification System (SAFIS)

Purpose of System

SAFIS is a highly specialized system used by SBI and law enforcement agencies throughout NC to perform hundreds of thousands of fingerprint and palm print identifications per year for purposes of arrest processing, sex offender registration, DNA collection, prisoner movement and release, solving crimes by identifying latent fingerprints left at crime scenes, and performing criminal history background checks for employment and concealed handgun permits. SAFIS integrates with two other CIIS criminal information systems: Computerized Criminal History (CCH) and Sex Offender Registry (SOR). SAFIS is the conduit for criminal history information to CCH because NC official criminal histories must be tied to a fingerprint identification of the subject to whom the criminal history belongs. Beyond CCH and SOR, SAFIS integrates with other criminal information systems at FBI, NC State Crime Laboratory, NC Department of Corrections, and Mecklenburg County. SAFIS also integrates with NCATS, a non-criminal system used by CIIS for processing criminal history background checks.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. All SAFIS hardware is provided by the SAFIS vendor, MorphoTrak. All hosting maintenance and operations tasks pertaining to the SAFIS hardware are performed by MorphoTrak. DOJ ITD staff only performs hosting maintenance and operations tasks pertaining to the provision of space, power, and data communications to SAFIS at the DOJ Data Center.
- Software operations are the responsibility of MorphoTrak, but SBI CIIS staff performs some basic operations, such as rotating backup tapes and running system scripts as directed by MorphoTrak.
- User support and training is provided at a basic level by SBI CIIS staff (less than one FTE) while more advanced user support and training is provided by MorphoTrak.
- Software maintenance is performed entirely by MorphoTrak. The cost of MorphoTrak providing all of the above SAFIS operations, maintenance, and support is $413,733 per year. Additionally MorphoTrak charges Department of Corrections and Mecklenburg County $23,071 and $44,686 respectively for annual maintenance and support of their remote SAFIS sites. MorphoTrak also charges maintenance and support directly to NC law enforcement agencies that purchase and operate latent fingerprint workstations and live-scan fingerprint capture devices connected to SAFIS.

Options for Transitioning to Private Company Maintenance

Software maintenance (and operations and support) for SAFIS is already performed by a private company – MorphoTrak.

Computerized Criminal History (CCH)

Purpose of System

CCH stores all NC criminal histories, including court disposition information, initiated from a fingerprinted arrest. It also stores information on correctional admissions and releases linked to fingerprint identification. From FBI's perspective, CCH is considered the sole official criminal history repository for NC. CCH does not have its own user interface. Instead CCH information is accessed by law enforcement agencies within NC via CIIS' Omnixx and LEMS systems. Law enforcement agencies outside of NC can access the CCH database through LEMS' connection to NLETS. CCH interfaces with SAFIS, LEMS, NC Administrative Office of the Courts systems, FBI systems, and the CODIS DNA Specimen Manager within the State Crime Laboratory.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. CCH software operations consume approximately 1 FTE of ITD staff.
- User support is not directly applicable to CCH because its user support is embedded in LEMS and Omnixx user support. A negligible amount of ITD staff time is also spent fulfilling research requests for CCH data.
- Software maintenance is performed by DOJ ITD. CCH software maintenance consumes approximately 0.5 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

CCH is software that was developed by ITD staff and contractors working under the direction of ITD. One option for having this software maintained by a private company would be to have that company perform software maintenance tasks on the software in its current state. It is unlikely that a company would be interested in maintaining highly complex software that it did not develop. Were a company to consider such an arrangement, it would require ITD to create extensive technical documentation and perform knowledge transfer that would result in greater than cost than ITD continuing to maintain the software internally. A better option for transitioning to private company maintenance would be to replace the CCH software with vendor-provided software and then have that vendor perform the maintenance. Given the inextricable linkage between SAFIS and CCH, replacement of CCH could be bid out as an integral part of the next SAFIS replacement, which is anticipated to be in 2017 depending on the availability of legislative appropriation to fund this replacement.

Sex Offender Registry (SOR)

Purpose of System

SOR stores all information on registered sex offenders as required by NC General Statutes (Chapter 14, Article 27A). SOR is also used to manage compliance with ongoing registration requirements, such as address verification. SOR does not have its own user interface. Instead SOR information is accessed by law enforcement agencies within NC via CIIS' Omnixx and LEMS systems. SOR data can also be accessed via Office of State Controller's CJLEADS system, which receives daily updates from SOR. SOR interfaces with LEMS, SAFIS, and FBI's national sex offender registry.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. SOR software operations consume approximately 0.5 FTE of ITD staff.
- User support and training is primarily provided by SBI CIIS. DOJ ITD assists in user support for issues that cannot be resolved by CIIS staff, which consumes approximately 0.1 FTE of ITD staff.
- Software maintenance is performed by DOJ ITD. Frequent changes to SOR software are required to support North Carolina's continually changing sex offender registration laws. SOR software maintenance consumes approximately 1.5 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

SOR is software that was developed by ITD staff. Because this software is tightly linked with CIIS's SORTS and SOR Public Website, maintenance of these three systems must be considered as a whole. One option for having this software maintained by a private company would be to have that company perform software maintenance tasks on the software in its current state. It is unlikely that a company would be interested in maintaining highly complex software that it did not develop. Were a company to consider such an arrangement, it would require ITD to create extensive technical documentation and perform knowledge transfer that would likely result in greater than cost than ITD continuing to maintain the software internally. A better option for transitioning to private company maintenance would be to replace the SOR software with vendor-provided software and then have that vendor perform the maintenance. If North Carolina were to adopt all provisions of the federal Sex Offender Registration and Notification Act, that would be an appropriate time to consider soliciting proposals to replace SOR with a vendor-provided solution. Even then, DOJ would have considerable concern about outsourcing maintenance of a system that requires such frequent, large maintenance changes with aggressive, fixed deadlines resulting from changes in law. No private company would be willing to take on a fixed-price maintenance contract to perform tasks that are unknown until laws are passed, which means new contracts to change SOR to comply with new laws would need to be created every time a new law impacting SOR is passed. While ITD is able to accommodate these changes in the tight legislatively-dictated timeframes, an external vendor would not have enough time to do this after waiting for completion of the procurement process.

Sex Offender Registry Tracking System (SORTS)

Purpose of System

SORTS is a web-based system using the same database as SOR that provides a more flexible user interface than that provided by Omnixx to allow CIIS and Sheriff's Offices to perform tasks that are better supported by such a user interface, such as uploading and editing sex offender photos, editing address mapping data, and providing a view for managing all sex offenders in the jurisdiction. Over time, the data entry functions in SOR are expected to be migrated to SORTS in order to support more efficient processing of sex offenders by CIIS and Sheriff's Offices.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. SORTS software operations consume approximately 0.1 FTE of ITD staff.
- User support and training is primarily provided by SBI CIIS. DOJ ITD assists in user support for issues that cannot be resolved by CIIS staff, which consumes approximately 0.05 FTE of ITD staff.
- Software maintenance is performed by DOJ ITD. SORTS software maintenance consumes approximately 0.25 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

SORTS is software that was developed by ITD staff as an extension to SOR. The same options for transition to private company maintenance described for SOR apply to SORTS.

Sex Offender Registry Public Website

Purpose of System

The SOR Public Website allows citizens to view public information (as opposed to law-enforcement-only information) on sex offenders registered in North Carolina. Citizens can subscribe to receive email notifications on the movement of specific offenders or offenders within 1-,3-, or 5-mile radius of a specified address. This system uses the same database as SOR, but is limited to public information. Public SOR data is also published to the North Carolina Statewide Automated Victim Assistance and Notification system (SAVAN), which is operated by Appriss via a contract with Department of Public Safety, on an hourly basis to support phone-based notifications to victims on sex offender movement.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. SOR Public Website software operations consume approximately 0.1 FTE of ITD staff.
- User support is primarily provided by SBI CIIS. DOJ ITD assists in user support for issues that cannot be resolved by CIIS staff, which are negligible.
- Software maintenance is performed by DOJ ITD. SOR Public Website software maintenance consumes approximately 0.25 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

The SOR Public Website is software that was developed by ITD staff as an extension to SOR. The same options for transition to private company maintenance described for SOR apply to the SOR Public Website.

Sex Offender Registry Mobile App

Purpose of System

The SOR Mobile App allows citizens to view public information (as opposed to law-enforcement-only information) on sex offenders registered in North Carolina using an iPhone app downloadable from Apple's iStore. Citizens can subscribe to receive email notifications on the movement of specific offenders or offenders within 1-,3-, or 5-mile radius of a specified address. This system uses the same database as SOR, but is limited to public information.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract for those portions of the software with which app communicates. Hosting of the iPhone app for download purposes only is at the Apple iStore. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. SOR Mobile App software operations consume negligible DOJ ITD staff time because these tasks already covered by operation of the SOR Public Website.
- User support is primarily provided by DOJ ITD. The need for such support has been negligible to date.
- Software maintenance is performed by DOJ ITD. SOR Mobile App software maintenance consumes approximately 0.1 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

The SOR Mobile App is software that was developed by ITD staff as an extension to SOR. The same options for transition to private company maintenance described for SOR apply to the SOR Mobile App.

Concealed Handgun Permits (CHP)

Purpose of System

CHP stores information on all concealed handgun permits applied for and issued in North Carolina. While CHP does not store what is typically considered to be criminal information, it exists because of a provision in criminal law (Chapter 14, Article 54B of NC General Statutes) and as such is being included in this study. CHP does not have its own user interface. Instead CHP information is accessed by law enforcement agencies within NC via CIIS' Omnixx and LEMS systems. CHP interfaces with CIIS' NCATS for purposes of providing data to invoice Sheriffs for SBI's portion of the CHP application processing fees.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. CHP software operations consume approximately 0.2 FTE of ITD staff.
- User support is not directly applicable to CHP because its user support is embedded in LEMS and Omnixx user support.
- Software maintenance is performed by DOJ ITD. CHP software maintenance consumes approximately 0.5 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

CHP is software that was developed by ITD staff. One option for having this software maintained by a private company would be to have that company perform software maintenance tasks on the software in its current state. It is unlikely that a company would be interested in maintaining software that it did not develop. Were a company to consider such an arrangement, it would require ITD to create extensive technical documentation and perform knowledge transfer that would result in greater than cost than ITD continuing to maintain the software internally. Another option for transitioning to private company maintenance would be to replace the CHP software with vendor-provided software and then have that vendor perform the maintenance. That is also not a desirable option because DOJ envisions all CHP data entry functions being absorbed into NCATS in the future. NCATS, which is an extremely low-maintenance system, is where CIIS already performs most of its work required for processing of CHP applications. This consolidation would streamline CHP application processing for both CIIS and Sheriff's Offices.

EVOLVE

Purpose of System

EVOLVE allows NC law enforcement agencies to review and validate their FBI "hot file" entries on a monthly basis as required by FBI policies. While these validations can also be done via LEMS/Omnixx on a single record at a time basis, EVOLVE allows this validation to be done in bulk, which is a big timesaver for law enforcement. EVOLVE is a proprietary system provided by Peak Performance Solutions using its CJIS Validations software.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are the responsibility of Peak Performance Solutions.
- User support and training is provided at a basic level by SBI CIIS staff (less than one FTE) while more advanced user support is provided by Peak Performance Solutions.
- Software maintenance is performed entirely by Peak Performance Solutions. The cost of Peak Performance Solutions providing all of the above EVOLVE operations, maintenance, and support is $22,500 per year.

Options for Transitioning to Private Company Maintenance

Software maintenance (and operations and support) for EVOLVE is already performed by a private company – Peak Performance Solutions.

Expungement

Purpose of System

The Expungement system tracks CIIS's processing of court orders to expunge criminal records. This is a minor system with just a few users in CIIS.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. Expungement software operations consume a negligible amount of ITD staff time.
- User support is performed by DOJ ITD staff and consumes approximately 0.05 FTE of ITD staff.
- Software maintenance is performed by DOJ ITD. Expungement software maintenance consumes approximately 0.05 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

Expungement is software that was developed by ITD staff. One option for having this software maintained by a private company would be to have that company perform software maintenance tasks on the software in its current state. It is unlikely that a company would be interested in maintaining software that it did not develop, especially this software, which is using an old technology that very few people know. The amount of maintenance to be done for this system is also so small that no vendor would likely consider the business to be worth pursuing. Another option for transitioning to private company maintenance would be to replace the Expungement software with vendor-provided software and then have that vendor perform the maintenance. Given that this is such a small application to replace, going through a procurement process would almost certainly be more expensive than replacing the software with an internal solution. DOJ plans to replace Expungement with the software used in NCATS, which is extremely low-maintenance.

Recovered Vehicles

Should we include this given that it is not truly storing criminal information?

Purpose of System

The Recovered Vehicles system tracks recovered vehicles that are in the possession of law enforcement, but have not been reported stolen, and the owner is unknown or cannot be contacted. Recovered Vehicles does not have its own user interface. Instead recovered vehicles information is accessed by law enforcement agencies within NC via CIIS' Omnixx and LEMS systems.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. Recovered Vehicles software operations consume a negligible amount of ITD staff time.
- User support is not directly applicable to Recovered Vehicles because its user support is embedded in LEMS and Omnixx user support.
- Software maintenance is performed by DOJ ITD. Recovered Vehicles software maintenance consumes approximately 0.05 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

Recovered Vehicles is software that was developed by ITD staff. One option for having this software maintained by a private company would be to have that company perform software maintenance tasks on the software in its current state. It is unlikely that a company would be interested in maintaining software that it did not develop. The amount of maintenance to be done for this system is also so small that no vendor would likely consider the business to be worth pursuing. Another option for transitioning to private company maintenance would be to replace the Recovered Vehicle software with vendor-provided software and then have that vendor perform the maintenance. Given that this is such a small application to replace, going through a procurement process would almost certainly be more expensive than replacing the software with an internal solution. The technology for Recovered Vehicles has also been refreshed recently, so there is no driving need to replace the system.

Crime Analysis Management System (CAMS)

Purpose of System

CIIS administers the crime reporting standards for North Carolina and provides technical support to the approximately 420 law enforcement agencies that participate in the North Carolina Uniform Crime Reporting Program (UCR Reports). The data is compiled into the Crime in North Carolina report along with various UCR reports, posted on the SBI website and disseminated to the FBI as part of a national UCR system.

In addition, CIIS is often called upon to provide statewide crime data to various constituents, including the public, media, law enforcement and other state agencies and legislative bodies. In response to its various constituencies, the SBI administers a voluntary program whereby LLEAs provide crime data from their respective jurisdictions to the SBI. Although voluntary, reporting agencies represent 97.5% of the population coverage of North Carolina.

CAMS provides a flexible and consistent approach to collecting and reporting crime data. The primary focus of CAMS is to provide consistency in reporting by enforcing national data standards for crime reporting. The SBI leverages the power and flexibility of SAS analytical tools for reporting and analysis. The CAMS solution provides enhanced analytical capabilities, brings North Carolina in line with national crime data reporting standards, reduces time required to generate reports, and automates data collection.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. CAMS software operations consume approximately 0.25 FTE of ITD staff.
- User support and training is provided by DOJ ITD staff and SBI CIIS and consumes approximately 0.25 FTE and 0.75 FTE of staff time from these groups respectively.
- Software maintenance of the analysis and reporting software is performed by SAS as a cost of $33,568 per year. Maintenance of the NC reports and data is performed by DOJ ITD and SBI CIIS and consumes approximately 0.25 FTE and 0.25 FTE of staff time from these groups respectively.

Options for Transitioning to Private Company Maintenance

The CAMS software was developed by ITD and SBI staff, as well as contractors working under the direction of ITD using SAS analytical software as a foundation. SAS already maintains this analysis software. Transitioning maintenance of other parts of CAMS to a private company at this time would be inadvisable due the strong dependency between CAMS and the NC-DEx system, which is currently under development. Transitioning maintenance of CAMS to a private company could be considered after NC-DEx is fully implemented.

Crime Reporting

Purpose of System

The Crime Reporting system is the prior system that CIIS used to collect crime information for UCR reports and other analytics, but has far fewer capabilities than SBI requires, which is why the CAMS and NC-DEx systems are being implemented. While CAMS has already replaced the reporting and analysis functions in the legacy Crime Reporting system, Crime Reporting is still used by law enforcement agencies to submit their UCR data to CIIS. This function will eventually be taken over by the NC-DEx system, which is currently in development.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff and consume approximately 0.25 FTE of staff time.
- User support and training is provided by SBI CIIS and consumes approximately 0.75 FTE of staff time.
- Software maintenance is performed by DOJ ITD and consumes approximately 0.25 FTE of staff time.

Options for Transitioning to Private Company Maintenance

This system is at the end of its life and is being replaced by CAMS and NC-DEx, so transitioning maintenance to a private company is inadvisable.

Traffic Stops

Purpose of System

The Traffic Stops system allows law enforcement agencies to enter traffic stop information via a website or through an FTP file transfer. This information includes date/time and location of stop, agency/officer making the stop, reason for stop, characteristics of person stopped and any others persons searched, and outcomes of stop. Traffic Stops also provides a website for the SBI to view all traffic stop statistics and for the public to view traffic stop statistics that are deemed public information.

Maintenance and Technical Operations Approach and Costs

- Software hosting is at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks are performed by DOJ ITD staff.
- Software operations are performed by DOJ ITD staff. Traffic Stops software operations consume approximately 0.05 FTE of ITD staff.
- User support and training is primarily provided by SBI CIIS. DOJ ITD assists in user support for issues that cannot be resolved by CIIS staff, which consumes approximately 0.05 FTE of ITD staff.
- Software maintenance is performed by DOJ ITD. Traffic Stops software maintenance consumes approximately 0.1 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

Traffic Stops is software that was developed by ITD staff. One option for having this software maintained by a private company would be to have that company perform software maintenance tasks on the software in its current state. It is unlikely that a company would be interested in maintaining software that it did not develop. The amount of maintenance to be done for this system is also so small that no vendor would likely consider the business to be worth pursuing. Another option for transitioning to private company maintenance would be to replace the Traffic Stops software with vendor-provided software and then have that vendor perform the maintenance. Given that this is such a small application to replace, going through a procurement process would almost certainly be more expensive than replacing the software with an internal solution. The technology for Traffic Stops has also been refreshed recently, so there is no driving need to replace the system.

NC-DEx

Purpose of System

NC-DEx will enable the accurate and timely sharing of law enforcement data across jurisdictional boundaries and offer investigative tools to assist in providing investigatory leads and linking crime characteristics.

NC-DEx provides seamless data transfer from local law enforcement agencies to the state incident data repository in near real-time. Data is added to the repository through an automated connect with an agency's records management system or through a direct-entry website.

Data received by NC-DEx will be forwarded to the FBI's national data-sharing system, N-DEx. The linking of these two data-sharing systems creates a comprehensive system with valuable law enforcement services and capabilities allowing users to detect relationships between people, places, and things.

NC-DEx along with the CAMS system will also replace the state's current crime reporting system, creating a seamless, more efficient data submission process. Uniform Crime Reporting (UCR) data will be extracted from submitted data, cleansed, and reported for each agency. This will greatly reduce or eliminate effort required for UCR submission.

In order to minimize the financial impact on the law enforcement community, NC-DEx uses nationally-developed standards and leverages existing records management systems.

Maintenance and Technical Operations Approach and Costs

- Software hosting will be at the DOJ data center and at its disaster recovery site at MCNC under contract. Hosting maintenance and operations tasks will be performed by DOJ ITD staff.
- Software operations will be performed by DOJ ITD staff. NC-DEx software operations are expected to consume approximately 0.5 FTE of ITD staff.
- User support and training will be provided by DOJ ITD and SBI CIIS and is expected to consume 0.25 FTE and 1.25 FTE of staff time from those groups respectively.
- Software maintenance will be performed by DOJ ITD. NC-DEx software maintenance is expected to consume about 0.5 FTE of ITD staff.

Options for Transitioning to Private Company Maintenance

The NC-DEx solution is being developed using "open-source" software that was developed for the National Institute of Justice. Other states have taken the same code and customized it for their use. North Carolina outsourced the customization. When customization is complete the source code will become the property of NC DOJ with the understanding that NC DOJ will share the code with other states if requested. The advantage is that the cost of developing future modules can be shared among the states using the base code. Outsourcing maintenance and support for NC-DEx is an option provided that appropriated funds are available.

4. Conclusions

Of the five largest and most important criminal information systems in SBI CIIS (which are LEMS, Omnixx, SAFIS, CCH, and SOR), only the CCH and SOR software is not already maintained by a private-sector company. Engaging a vendor to maintain CCH and SOR in their current states is not a viable option because this is expected to cost more than the current maintenance performed by DOJ ITD and does not provide sufficient flexibility to respond to legislative changes that impact these systems. CCH and SOR also require significant ITD involvement in software operations. Separating software maintenance from software operations can be difficult because both tasks require the same administrative rights to the software, so both maintenance and operations should be considered for transition to a vendor. When the time comes to replace CCH and SOR based on the emergence of a business driver to justify the replacement, DOJ plans to investigate the feasibility of having a vendor replace the software and take responsibility for ongoing maintenance and operations. The same consideration would be given to the lesser criminal information systems in CIIS when those systems are due for replacement.

Should the General Assembly direct DOJ to proceed with obtaining vendor bids for maintaining (or replacing and maintaining) all or part of the CIIS criminal information systems explained in this study, DOJ would require an appropriation for contracting with a vendor to develop requirements and write the procurement documents because DOJ lacks the internal staff capacity to take on such a task, which is outside of the existing information systems lifecycle schedule planned for these systems. The amount of appropriation required would depend on the quantity and complexity of the systems whose maintenance is to be addressed.

For reference, in 2005 DOJ secured the services of an information technology firm with expertise in law enforcement security systems whose sole job was to develop technical Request for Proposal (RFP) and procurement specifications to replace our outdated SAFIS fingerprint system. Total costs incurred for the technical expert were $166,160 which proved essential to ensuring the procurement and final totals for the new SAFIS system came in under our budgeted level of $6.5 million. Actual SAFIS system replacement expenditures were $5.1 million because of the detailed technical specifications were completed in a thorough comprehensive and professional manner for this complex subsystem that is yet one part of the Criminal Information Division technology portfolio.