

Agency Operations Plan 2015-17

Agency:

0125 – ND Office of Attorney General

Line of Business:

The Office of Attorney General is the chief legal counsel and advisor to state government, providing legal representation to all facets of state government, including the Governor, all departments of state government, local government and all state agencies, boards and commissions.

The Attorney General is an elected official and has primary authority to act on behalf of the state of North Dakota in other areas, including criminal investigations; full arrest and law enforcement authority; sex offender risk assessment and registration; evidence examination and testimony; consumer protection and antitrust; administration, regulation and enforcement of charitable gaming and lottery activity; and fire inspections, investigations and mitigation of hazardous materials incidents. Attorney General staff members provide a significant amount of training to North Dakota citizens and others, including law enforcement and the fire services.

The Office of Attorney General has 7 sites in Bismarck and 13 sites across the state of North Dakota. The agency is the law enforcement agency of the state with approximately 220 full time employees. It consists of 13 divisions all with unique business needs, but often sharing data and responsibility across divisional boundaries.

- Administration
- Bureau of Criminal Investigation
- Civil Litigation (Legal)
- Consumer Protection and Antitrust
- Crime Laboratory
- Criminal and Regulatory (Legal)
- Finance and Administration
- Fire Marshal
- Gaming
- Information Technology
- Lottery
- Natural Resources and Indian Affairs (Legal)
- State and Local Government (Legal)

Contact:

Name:	Cher Thomas
Title:	Information Technology Director
Phone #:	701 328-5519
Email:	cthomas@nd.gov

Technology Strategy:

The Office of Attorney General is the law enforcement agency for the state and provides information and support for law enforcement in the local jurisdictions. Much of the information collected by the Bureau of Criminal Investigation is from local sources. This information is then made available to criminal justice entities across the state as well as across the nation through ND-CJIS or the teletype at State Radio.

The legal divisions handle many cases for other state agencies as well as representing the state in federal cases. Many of these cases are highly confidential and may contain information on individuals that work for government and require high security standards.

Some repositories are accessed by others for the purpose of acquiring background checks for applicants applying for employment. It is critical that the data be complete, accurate and timely to ensure the most up-to-date information is provided to employers concerning potential employees. In many cases the timeliness of the information means it is essential that data is provided electronically from the source of the information. Therefore, business processes are constantly being reviewed for improvement ideas, including technology advancements. Fingerprint devices are being investigated for many places where positive identification is required.

The AG staff continues to be a very mobile workforce, from agents investigating crimes to fire marshal deputies investigating fires; from legal cases being handled outside the state to legal cases across the state. Therefore, portable devices, such as tablets and smart phones must be provided for this workforce. At the same time a high level of security requirements must be met to ensure the safety of critical, sensitive information.

The IT staff maintains a public website for the office, as well as the ND Lottery website and the ND Sex Offender website. News releases and opinions issued by this office are published regularly. ND Lottery numbers are published through an automated process from MUSL, the Multi-state consortium that oversees policies and standards for lotteries across the nation. The sex offender website is updated real time as sex offenders are registered in the state repository.

Technology Infrastructure:

Services received from ITD

- Security – firewall installations and configuration changes at the request of AG network manager
- Security – VPN (Virtual Private Network) software management for accessing the network when away from the primary office location with encryption to protect the information traveling over lines used to across the internet
- Security – Wave Encryption for encrypting hard drives on laptops, to prevent access if stolen or lost
- Security – Multi-factor authentication – provides an additional mechanism, a randomly generated number through a token, along with the userid and password to verify a person has access to the network and data
- Mobile device management service – allows an agency to track its assets, such as smart phones and tablets and to be able to erase the device remotely if reported stolen or lost. Servers are located in ITD server room
- Hosting – AS400 for legal billing, legal docket and workload tracking, as well as Fire Marshal Billing
- Hosting – Sharepoint – tracking and collaboration for IT projects
- Active Directory network access accounts are setup by us, the servers are hosted at ITD
- Email accounts are hosted at ITD
- Wide area network with fiber lines to the majority of our remote locations across the state
-

IT Organization and Organizational Structure

The Information Technology (IT) division provides technical services and support for the agency's 13 locations across the state, as well as several locations in Bismarck. IT provides support for all employees' computers, including some highly specialized ones at the Crime Lab and BCI. The help desk provides valuable support to the entire agency by tracking and assigning calls. These calls result in IT staff providing network support, troubleshooting, software installation, equipment replacement, creation of new computer applications, and enhancement of existing applications.

The IT staff also maintains the website for the Office of Attorney General, the North Dakota Lottery, and the North Dakota Sex Offender web site which shares information with the National Dru Sjodin sex offender web site. In addition, we also facilitate the secure sharing of agency information residing in repositories located in our secure server room. The criminal justice information is shared with law enforcement across the state through State Radio and the North Dakota Criminal Justice Information Sharing (CJIS) initiative. We maintain connection with livescans across the state, routing information to various internal applications as well as the fingerprint database housed at the Bureau of Criminal Apprehension in Minnesota. South Dakota, North Dakota and Minnesota all house fingerprints in this repository.

Staff

The IT division currently has 14 full time positions and 1 temporary-part time person organized as follows:

IT Director

- 1 Temp Administrative Assistant
- 1 Architect/Quality Control
- 1 Database Analyst
- Application Development Manager

6 Programmer Analysts
IT Manager
1 Server Administrator
1 Desktop Support
1 Help Desk Support

In order to meet the demands of the agency for our services, we also utilize 6-10 consultants at any given time for application development and project managements. IT staff manage the projects and oversee the work of the consultants.

Services Provided by IT Staff

- Server administration of servers located in our secure server room, including file-and-print servers, database servers, web servers and application servers
- Web design and support for the AG public website, the Sex Offender website, the ND Lottery website, and the AG Intranet
- Enhancements to business applications as required through changes in business processes or policies, or legislative requirements as well as to add value and efficiency to existing business processes
- Support to local law enforcement and other criminal justice personnel who access the agency's various repositories directly or through the ND-CJIS portal or the State Radio (teletype) system.
- Hardware and software support for all divisions of the office to enable them to serve their customers including:
 - All desktops, laptops, tablets and other mobile devices for employees
 - Additional computers for crime lab employees in the lab, as well as computers connected to specialized instruments
 - BCI – specialized software and hardware used for various tasks such as polygraphs, crime scene drawings, suspect sketching, fingerprint analysis, and currency counting
 - Livescan fingerprint devices across the state
 - Support to the cybercrime unit of BCI as needed
- Hardware and software installs and upgrades
- Help desk calls with support, logging and reassigning as needed for agency employees, task force members and other criminal justice employees using agency applications
- Imaging of hard drives
- Maintaining technical inventory across all agency locations
- Setup/Configurations for new users
- Security training and use of computers for all new AG employees
- Purchasing of all technology for AG divisions
- IT Contracts
- Project Management of projects with state reporting as required
- Development of new applications
- Timely patch management of servers and desktops to help prevent vulnerabilities and data breaches
- Encryption of hard drives on laptops to protect information that may be temporarily stored on hard drives
- Manage multifactor authentication, where needed to ensure only authorized personnel have access to our sensitive data
- Backup and recovery services for AG data
- Troubleshoot and provide solutions to computer connectivity issues with assistance from ITD

when necessary

- Strategic planning for the office to address current as well as future technology needs for all the divisions
- Evaluation of ever-changing security requirements and planning to meet current market standards as well as stringent FBI policies

Remote Offices

The Office of Attorney General has 7 sites in Bismarck and 13 sites across the state of North Dakota. The IT division supports the IT needs of all the employees stationed at these locations. In some of the locations we also have task forces supported by our office. Usually one of our BCI agents is assigned to each of these task forces.

Stakeholders

The Public

Law Enforcement across the entire state of North Dakota, as well as nationally

State's Attorneys

Court Personnel

Department of Corrections

FBI

State agencies, boards and commissions

Local government

Security

The Office of Attorney General is the State Law Enforcement agency and has many responsibilities for the protection of the information we have stored in our databases. The office also provides legal services to other state and local agencies, many with strict non-disclosure requirements. Security is therefore a primary focus for many of our divisions.

The office is first protected by the firewall protections offered by ITD for all state government. Within that circle of protection around state government, another circle has been drawn around our servers and desktops at the Bureau of Criminal Investigation location to ensure it is a secure building according to FBI standards. This ensures that we are secure and protected from intrusion by possible rogue employees in other state government agencies.

Some key points concerning our office security are listed below.

- FBI Security Policy Manual states that we need to protect user computers that access criminal justice information. This is accomplished through a firewall located at BCI to protect user computers with access to Criminal History, Sex Offender, Concealed Weapon licenses, Automatic Fingerprint Identification System, and Teletype communication with State Radio. ITD manages the fire walls, but our agency defines the rules and policies for what information and devices is allowed to come through the fire wall.
- FBI Security polices do not consider anything inside the state network as being secure. Their definition of secure is the Office of Attorney General being protected from all outside entities including other state agencies.
- Management agreements must be signed with all agencies providing services to the Office of Attorney General including (Note: the agreements have not been developed yet, but the recent FBI

audit requires that we do this as soon as possible. They are being worked on):

- access to any equipment that is used to process or transmit criminal justice information including (but not limited to) switches, access devices (teletype units, desktops, tablets, smart phones, laptops etc.) circuits, hubs, routers, firewalls
 - access to any systems, applications, systems design, programming and operations procedures associated with the development, implementation and maintenance of any agency system including those who directly access NCIC programs through the teletype
 - guaranteed priority, integrity and availability of service needed by the criminal justice community
 - policy governing encryption and telecommunications networks needs of the agency
 - policies governing priorities of service
 - policies and standards for the selection, supervision, and termination of personnel who are allowed to touch any of the equipment used for transporting criminal justice information including level of fingerprint based background checks, credit checks, and BCI agent interviews
 - restriction of unauthorized personnel from access or use of equipment accessing related to criminal justice and the use of the state network
 - compliance with all rules and regulations of the Office of Attorney General Policies and CJIS Security Policy (FBI) in the operation of all information received
- Auditing is required to be available at the discretion of our office to determine who has touched our equipment or software and why
 - All IT personnel and IT consultants must undergo extended background checks according to FBI policy. These are repeated occasionally during employment to reveal any possible compromises.
 - Although the FBI dictates most security policies for BCI, there are other security policies required for the Crime Lab, Legal, and the Lottery divisions from other regulating authorities
 - Legal case files include information about state employees, state agencies, juveniles, and other extremely sensitive and confidential information.
 - Active directory services are approved by the FBI to be provided by the state as long as the agency uses an internal application to grant or deny access to the various applications. Anyone who touches the application code, or servers that house the code, must be authorized through the management agreement and approved by AG staff.
 - Any support of computers on the DNA network at the Crime Lab need to have additional background checks performed through CODIS (the national DNA repository) before anyone can access those desktop computers. Any support of instrument computers in the DNA lab requires a DNA sample be provided.
 - Firewall – FBI Security Policy states that the agency must protect both criminal justice information and end user computers that access that information. As a result we have some special needs at our remote offices. We prefer to have our IP range at the remote sites so we can set firewall rules accordingly. If necessary, we get and manage static IP addresses for any sites that do not have their own IP range. This includes the many fingerprint devices called livescans, located in various locations across the state, that transmit fingerprint images (identity data) to our office and on to the fingerprint database in Minnesota at the Bureau of Criminal Apprehension.
 - Multifactor authentication is required by the FBI security policy for all access to applications that contain criminal justice information. Our office has taken the position that since those applications reside on the same network as other office applications, when accessing any network resource from outside the state backbone, multifactor authentication will be required along with VPN access, which encrypts the data.
 - Patches are received electronically from ITD and pushed to our equipment, in order to keep current with fixes that could potentially affect the security of our information.

Hardware

Servers

The office manages a storage area network (SAN), web servers, application servers, file and print servers, and database servers all located in our agency data center, or a secondary backup location at the Crime Lab. We also support live-scan units for collecting fingerprints across the state. These units communicate with a vendor supplied server hosted in our data center. This server provided by the vendor also communicates with servers housed in Minnesota.

Communications with FBI and law enforcement across the nation are handled through a server hosted and supported by the AG office. This server is in constant communications with the switch at State Radio to provide real-time criminal justice information to all requests. We provide sex offender information, warrants, protection order information, concealed license information for every drivers license check requested. Requests for information can come through investigations being conducted across the entire nation.

Some Crime Lab devices have their own computer system to collect data for that particular instrument. These devices then transfer data collected to the Crime Lab Management application for further reporting or analysis.

Additional information concerning the servers housed in our data center below:

- 8 physical servers belonging to the AG office, 4 are used to host the virtual servers
- AFIS servers provided and supported by the vendor for communication with Minnesota and the fingerprint database housed there
- 26 virtual servers located at the BCI location and 5 virtual servers located at the Crime Lab location
- Replacement cycle for physical servers is 6 years.
- Operating system is currently some with Windows 2008 R2 and some Windows 2012 R2. All new servers will have Windows 2012 R2. All servers operate on a currently supported operating system and are upgraded as time permits to the latest version.
- The servers sit behind a firewall. Patches are applied on a monthly basis. Downtime is scheduled so that we can perform a restart of a server if necessary.
- The management of our servers is mostly accomplished through the virtualization management interface. We have a server monitoring application that monitors items such as disk usage, service status, server availability, web site availability, etc. and notifies us when a failure status is detected.

Desktops (229)

- Computers used for Lab Instrument
- Some lab employees have two computers, one in the lab and one at their desk
- Most Lottery employees have two computers, one on the state network and one on the secure Lottery Gaming Network
- Computers dedicated to performing computer forensics
- Computers dedicated to operation of Currency Scanners

- Conference room computers used for presentations
- Computers dedicated to performing Cell phone analysis
- Computers dedicated to operation of building security systems
- Computers used for specialized fingerprint analysis
- IT power users with specialty software for development of applications, database design, etc.
- Desktops are on a 4-year replacement cycle. There are a few exceptions: computers used by crime lab instruments where the latest operating system may not be supported; desktops used by temporary personnel since use is limited; desktops used to access the Lottery network with limited functionality; and other specialty computers.
- Currently use Altiris for basic Windows imaging and to deploy software to computers across the office. Use RAdmin and Dameware for remote support. Use Network Inventory Advisor for software inventory
- Operating system on all desktops currently is Windows 7.
- Patches are received by Microsoft at ITD monthly. ITD validates and then publishes usually within a week, and we receive automatically from ITD and apply.

Laptops (155)

- Employee laptops are used for desktop purposes in the office and remotely when traveling.
- Several used as laptops to be checked-out for the occasional need for a laptop. Some designated as being used for emergency situations such as the flooding response in Minot.
- Several used by our Cyber Crime section to conduct training.
- Multiple in use by each Cyber Crime Agent to perform computer analysis when on site when necessary.
- Laptops dedicated to crime scene diagraming software.
- Laptops dedicated to crime scene vans.
- Laptops used for SORAC committee for assessment ranking of sex offenders
- Laptops are on a 4-year replacement cycle, except for the ones used for checkout, which typically are used in a limited fashion to access the web and read emails.
- Currently use Altiris for basic Windows imaging and to deploy software to computers across the office. Use RAdmin and Dameware for remote support. Use Network Inventory Advisor for software inventory.
- Operating system on most laptops currently is Windows 7. There are a few installations of Windows 8.
- Patches are received by Microsoft at ITD monthly. ITD validates and then publishes usually within a week, and we receive automatically from ITD and apply.
- Security - All laptops assigned to an individual employee have self-encrypting hard drives installed. The drives are enabled using WAVE which is hosted by ITD. The use of self-encrypting hard drives prevents unauthorized access to the drive should it be lost or stolen.

Tablets

- Own and manage 7 iPad Tablets
- Manage 9 Tablets owned by task forces which BCI oversees
- We anticipate the future direction will be to deploy tablet/laptop hybrids because of the high security requirements needed and the ability to manage these devices with our current device

management software provided by ITD

Mobile Devices

We have 89 smartphones managed by our office. These include office owned smartphones, employee owned smartphones, and Task Force owned smartphones. The smartphones owned by the office and Task Forces are all iPhones.

Printers (56)

- 2 ID printers for Concealed Weapon Permits.
- 45 Networked Laser Printers
- 2 Networked Plotter Printers
- 2 Networked AFIS Fingerprinting Printers.
- 5 Networked Lottery Printers on the Secure Lottery Network.

Multifunction Copier/Printer/Scanners (25)

Other Equipment

- Projectors
- Video Conferencing Systems
- Scanners

Business Continuity/Disaster Recovery

We replicate our databases several times a day or once a day depending on the criticality rating of the data. We backup critical data and configuration settings to tape on a daily basis. Full backups are performed on Friday. Differential backups are performed Monday through Thursday. We have the latest full backup and the latest differential backups stored off site every day.

List of Critical Business Applications

36 non-desktop applications are hosted by the AG office

9 total hosted outside of our agency - 1 in Minnesota state government, 1 Federal software for Fire Marshal Incident Reporting, 4 ITD AS400, 1 for vendor to manage SCRAM bracelets for 24/7 Sobriety program, and 2 for the Lottery, a general management system and an internal control system.

15 of our current business applications are either currently available for direct access by people outside our agency or will be by the end of this biennium.

We have 39 data exchanges, mostly real time, between our applications and other agencies or customers, which includes ND-CJIS, State Radio, FBI, ND Supreme Court, Department of Corrections, and National Sex Offender Website. We have two that currently generate electronic emails as a service when certain events happen, and one that generates text messages.

The last application that was running on the mainframe at ITD has been eliminated. By the end of the biennium, or shortly thereafter, all applications currently running on the AS400 computer at ITD will

have been replaced with web apps running in a network environment.

BUREAU OF CRIMINAL INVESTIGATION Division

Available within the office

- AFIS Interfaces**
- Case Management**
- Fingerprint Identification Transaction Service (FITS)**

Available to other criminal justice entities as well as our office

- Criminal History Repository**
- Concealed Weapon Licenses**
- Protection Order Repository**
- Sex Offender Registry**
- Sex Offender Blue Books for Ranking**
- Sex Offender Website**
- Incident Based Reporting (IBR) system (Crime Statistics)**
- IBR Web for publishing statistics (COTS) – currently being implemented**
- Warrants**
- CJIS Hub Interfaces**
- 24/7 Sobriety**
- Denied Person Repository**
- State Radio Teletype Switch Interface**
- SCRAM (Hosted outside agency) Cloud product that tracks those assigned SCRAM bracelets for alcohol/drug related offenses**

CONSUMER PROTECTION Division

- Complaint Tracking**
- Mail Tracking**
- Public Business Search for Complaints**

CRIME LAB

- Online Training System**
- Laboratory Management System (COTS)**
- CJIS Hub Interfaces**

GAMING Division

- Charitable Gaming Licenses and Tax Returns**

FINANCIAL ADMINISTRATION Division

FIRE MARSHAL Division

- FM Time Keeping and Billing**
- FM Fire Safer Cigarette System**

LEGAL Divisions

- Alcohol/Tobacco/Misc Licenses**
- Legal Time Keeping and Billing**

Docket/Workload Tracking
Legal Case Management System (RFP about ready to be released)
Mail Tracking

LOTTERY Division

Lottery Licensing and Management System

AGENCY WIDE

Time Keeping – Billquick (COTS)
Deposits
Legislative Bill Tracking

IT

Application Security System
Programming Workflow (Sharepoint)

For additional information see attached spreadsheet

Current Projects:

IBR Submission Project was completed the end of July. Replaces an old DOS based application for collecting crime statistics for small agencies that do not have a records management system, as well as task forces working with our office.

Online concealed weapon license projects – we have completed two of the 3 projects for the enhancement of our concealed weapon licensing system. The first project created an online form to enter data for an application to carry a concealed weapon and submit it to a holding database. The second project allowed the review of the application and receiving the application into the repository for processing. The third project, which is just starting, will allow for attachments to be submitted with the license application, such as pictures and other documentation. The system will also accept online payment and a complete rewrite of the deposit portion of concealed weapon licensing processing.

Legal Case Management – Requirements are finalized and RFP is close to being released for a case management system for our attorneys with an optional timekeeping and billing module.

Fire Marshal Billing – We are in the process of rewriting our Fire Marshal Billing system. The planning and high level analysis phases are almost complete. The current system resides on the AS400 at ITD. The new system will be a web app over a SQL database using Microsoft C#.NET.

Portable Fingerprint Devices – We are close to issuing an RFP for the purchase of 25 portable fingerprint devices for sex offender registration across the state. These devices will access Federal databases, such as RISC, as well as state databases like sex offender registry, warrants, criminal history, etc. A state contract will be issued so that local agencies can purchase devices from the contract.

CHIA – MAP – This project will create a workflow for background checks for applicants applying for positions in criminal justice organizations. This workflow will interact with livescans and AFIS (the automatic fingerprint database) housed in Minnesota. The project is in the high level analysis phase.

Denied Person Repository – There are three projects slated to complete this effort. The first project created an online form for entry of information, as well as an interface between us and the courts to receive the information electronically. This is in production. The second project creates an electronic transfer of the information from the repository to the FBI. This project is almost completed and is waiting on testing through the switch at state radio. The third project will enhance the system to send a message back to the courts, that a particular record has been received by us. The third project is in the high level analysis phase.

Warrants – the application has been rewritten utilizing current technology. This project improves the search capabilities of warrants through ND-CJIS and improves the performance of the system. It is in the final stage of testing and will be in production by the end of August 2014.

Security – Livescans running Windows XP were replaced. All livescans across the state replaced by this office have installed firewalls managed by the office. The IT division worked with ITD to implement an encryption policy for laptop hard drives. We also worked with ITD and State Radio to implement a multifactor authentication solution required by the FBI for any application that contains criminal justice information.

Planned Activities:

Application Development

Programmer analysts are difficult to find in the ND market. In order to keep up with the demand for development services from the divisions of the office we will continue to augment staff with contractors to provide programming and analysis services for business applications essential to the many business functions of the various divisions of the office. This includes maintenance support and enhancements for existing applications and the development of new applications.

We will continue to develop applications accessible via the web for the office's customers, thus eliminating manual entry by office staff and delays caused by mail delivery. This method also enables validation at the time of entry reducing errors coming in the office. We will continue to maintain and enhance our current business applications to meet the needs of our agency personnel as well as the criminal justice agencies that depend on the timeliness and accuracy of our data, both nationally and state-wide.

We will continue to evaluate ever changing business processes, and offer recommendations where technology can improve these processes. There were many legislative changes in the last session due to the oil boom in the western part of the state. These legislative changes required a lot of changes to our existing applications. We will continue to be proactive in evaluating legislative changes and their impact on the business processes that drive our computer applications.

Security

We will continue to make security a priority. The state performs a security audit biennially required by statute. We will move towards conducting internal audits on the off years to ensure we are meeting strict FBI standards as well as standards set by our agency that may be more stringent than FBI standards. We will re-evaluate our security policies based on industry standards and current threats on a regular basis and make adjustments as required.

Software and Hardware

The office will continue:

- To evaluate tablets, smart phones, portable fingerprint devices, and other mobile devices that will enhance and improve business processes for the agency.
- To support the livescans across the entire state used for capturing fingerprints and find ways to improve the process. The connecting of data to a set of fingerprints for many events is critical. The timeliness of receiving that information is critical as well.
- To evaluate business processes and automation since it is extremely important that we have complete criminal histories on file as soon as possible to provide employers with valid information when evaluating prospective employees.
- To evaluate and move toward a rapback system that will allow employers to enroll employees in the program. If an arrest of an enrolled person should happen, a notification would be sent back to the enrolling agency to decide what to do.
- To evaluate and acquire specialized software and hardware for various needs within the agency

Training

Technology evolves very rapidly and it is a challenge to keep up with the changes. It requires constant education of staff and critical evaluation of IT processes is essential. We will continue to train IT personnel:

- In business analysis techniques to understand how to document and re-engineer business processes
- How to best determine technical solutions for business requirements
- Latest programming techniques
- Latest versions of software and operating systems
- Security
- Database design
- Application Architecture
- Server Administration

Other Services

The IT division will continue to work with ITD to provide connectivity and security to our remote sites across the state. We will continue to improve our auditing capabilities to know who has access to our hardware and software and when someone accesses these resources.

We will continue to monitor and improve security practices across the agency. We will continue to monitor the FBI security policy to make sure we are in compliance.

We will continue to evaluate ways to put management tools in the hands of our managers and supervisors, such as dashboards, to enable them to make more timely and effective decisions.

We will continue to offer services currently provided by this office in an effective and efficient manner: the help desk; training for new employees; security; evaluation and procurement of hardware, software and computer services; contract negotiations; 24/7 support for law enforcement accessing the information

stored in our repositories.

We will continue to participate in the North Dakota Criminal Justice Information Sharing (ND-CJIS) program by providing information from our repositories that is beneficial to the criminal justice community. We will continue to meet quarterly to discuss ways to improve and share information.

We will continue to participate in the enterprise architecture process and provide input into the state technology decisions.

We will help facilitate additional offices for BCI across the state as needed or move offices within cities as needed.

Planned Projects

The Office of Attorney General has many opportunities to apply for federal grants. When received, these can quickly change priorities for internal projects. The Attorney General is an elected official with his own priority items for the office that can affect Information Technology project schedules. Most of the computer application work undertaken by our office is internally built with the help of contractors. These work efforts are most of the time broken into multiple small projects in order to show some benefit as quickly as possible, as well as to ensure success.

CHIA (Criminal History Improvement Analysis)

We received funding in a previous biennium to do planning for improving the efficiencies of the criminal history repository and the reporting of information electronically. We also received funding last biennium to move that planning forward. The money received has been used on several projects and the work effort will continue to be broken down into small projects.

Several projects have either been completed or started:

- Common Statute Table (in coordination with the Courts and ND-CJIS)
- Upgrade of livescans to handle new technology
- Portable fingerprint devices
- Criminal History Repository rewrite
- MAP – Workflow through Livescans for criminal justice agency job applicant background checks
- Upgrades of development software to be compatible with the new processes
- Firewalls added for security purposes surrounding livescans

Future projects identified:

- Electronic filing (in coordination with ND-CJIS and the Courts)
- Other employment background checks workflow and online payment through a new application
- Rework of arrest and booking information workflow with livescans to include photos
- Photo repository
- Other biometrics
- Rapback
- Third party submission of fingerprints for employment purposes as well as concealed weapon licenses

Intel Application (for investigation personnel)

The intelligence community of law enforcement, which includes task force personnel, is in need of a new Intel Case Management system. The rules for sharing Intel information are extremely strict and governed by federal regulations. We need to provide them with a tool to help track criminal activity and suspected criminal activity in a way that allows them to analyze and make quality decisions in a timely manner.

BCI Enhancements

IT personnel spend 75-80% of their time supporting BCI and the Crime Lab. There are several small projects that need consulting help to get done. These projects will enhance current applications used by BCI for their daily activity.

- Forward sex offender supplemental information to the FBI
- Improve biometric use for sex offender registration identification
- Provide information to the sex offender federal office including documents for transfer to other states
- Receive information from the sex offender federal office including documents for transfers from another state
- Improvements to evidence tracking and evidence interaction with the crime lab
- Improvements for case reporting
- Enhancements to the 24/7 Sobriety program
- Enhancements to the DNA reporting process

We do not expect to have any large projects over the \$500,000 level. Planning has not been completed to the level of producing architecture or planning documentation required by ITD for efforts over \$100,000. These will be provided at the time the project enters the planning stage.

Technologies being considered or investigated:

Continue to evaluate and improve our service availability through mobile technology, such as smart phones, tablets, etc.

Evaluate current desktop management suite alongside other products to determine best approach for this office.

Evaluate other biometric methods of identification for criminal justice purposes.