Executive Secretary
Karl R. Hade

Assistant Executive Secretary &
Legal Counsel
Edward M. Macon

Court Improvement Program
Sandra L. Karison, Director

Educational Services
Caroline E. Kirkpatrick, Director

Fiscal Services
Barry M. Wenzig, Director

Human Resources
Renée Fleming Mills, Director

Supreme Court of Virginia

Office of the Executive Secretary
100 North Ninth Street
Richmond, Virginia 23219-2334
(804) 786-6455

Judicial Information Technology
Michael J. Riggs, Sr., Director

Judicial Planning
Cyril W. Miller, Jr., Director

Judicial Services
Paul F. DeLosh, Director

Legal Research
Steven L. Dalle Mura, Director

Legislative & Public Relations
Alisa W. Padden, Director

Magistrate Services
Jonathan E. Green, Director

October 29, 2021

Ms. Kristen J. Howard, Executive Director
Virginia State Crime Commission
1111 East Broad Street
Suite B036
Richmond, Virginia 23219

Dear Ms. Howard:

Chapter 542, Enactment Clause 10, of the Virginia Acts of Assembly (2021 Special Session I) requires the Office of the Executive Secretary (OES) to provide a report to the Virginia State Crime Commission on the process of implementing automated systems to exchange information as required by Senate Bill 1339/House Bill 2113 by November 1, 2021 and by November 1 of each year thereafter until the automated systems have been fully implemented.

OES has begun work on implementation of the automated systems to exchange information as set forth in the legislation. The Circuit Case Management System (CCMS), General District Case Management System (GCMS) and Juvenile and Domestic Relations Case Management System (JCMS) will all need extensive programming to implement the provisions of SB1339/HB2113. The Circuit, General District, and Juvenile and Domestic Relations teams in the OES Department of Judicial Services have begun internal meetings to discuss requirements and have begun identifying additional OES systems impacted by the legislation. To date, the Records Management System and the Virginia Judicial Online Payment System have been identified as additional systems that will need programming changes to implement the provisions of the legislation.

OES has also begun discussions with the Clerk of the Fairfax Circuit Court to plan for implementation of this legislation. The Fairfax Circuit Court does not use the OES CCMS system and has requested an interface with OES systems that will enable the Fairfax Circuit Court to transmit data to the Department of State Police through OES systems.

The OES Department of Judicial Information Technology (DJIT) has been working on establishing the foundation of how a case will be sealed or expunged and archived from the case management systems. To meet the requirements of SB1339/HB2113, all archived cases must be moved out of their underlying case management systems, as there are too many systems and interfaces that would otherwise have to be modified to ensure that data is not inadvertently disclosed. To prevent those archived cases from being unintentionally disclosed, all case data will be moved to a separate "data vault" when archived.

Since the case data is physically removed from the case management systems during the archival process, the design calls for a multi-stage process that includes verifying the case data in the data vault before deleting it from the case management systems. After a case is written to the data vault, the comparator will directly compare that to the data in the underlying case management system data store before the data is deleted from the case management system. This ensures that we don't lose data unintentionally.

OES is in the early stages of recruiting for a number of positions related to this legislation. Initially we're seeking a project manager, one or two architect level technical resources, and at least one business analyst. As work continues on the business requirements, OES will begin recruiting additional analysts, developers, and quality assurance personnel.

The following is a description of the hardware and software related work that has been completed so far to facilitate the data vault. The first stage of implementation of the data vault will be the archiving of specific data elements of expunged unlawful detainer cases from the general district courts starting on January 1, 2022. This work will form the foundation for the expanded data vault needed to implement SB1339/HB2113:

- Secret management
    - Platform evaluated and purchased
    - Test, Production, and Production Disaster Recovery clusters created and configured (13 servers)
    - LDAP and MFA integrations
    - GUI access for secret management implemented
    - System admin access policies established and implemented
- Auditing established and implemented
    - Application authentication, ACLs, local agent, and templating POC complete, full implementation in progress.
- Hosting Infrastructure
    - 4 additional 2 socket, 16 cores each, 1.5 TB RAM) purchased and integrated into the cluster.
- Database expansion
    - 4 additional licenses purchased
    - Tested integration of additional nodes in test environment.
    - Added the additional nodes to the production cluster.
    - Greatly increased the resource allocation, vCPUs and RAM, to the cluster.
- J2EE Container
    - Evaluated multiple options, settled on our microservices J2EE container

    - Servers provisioned in development, integration, quality assurance, and user acceptance testing environments (16 servers)
- API Gateway Service
    - Provides a point of entry to the microservices infrastructure for all other applications (CCMS, GCMS and JCMS). Handles routing of all external requests to the correct nodes and ports withing the microservices environment
    - Evaluated multiple options and settled on our API gateway
    - Developed, tested, and deployed in development, integration, quality assurance, and user acceptance testing environments
- Service Discovery
    - Tracks what microservices are running on which servers/ports within the microservices environments
    - Integrates with the API gateway and all other microservices to facilitate inter-microservice communications
    - Evaluated multiple solutions and settled on a product
    - Developed, tested, and deployed in development, integration, quality assurance, and user acceptance testing environments
- Configuration Server
    - Manages external configurations for all microservices within the environment. Allows microservice deployments to remain stateless, and provides a central management point for configurations
    - Integrates with all other microservices to provide their configurations
    - Integrates with source control to facilitate the promotion of configurations through the hierarchy of environments in a controlled manner
    - Evaluated multiple solutions, and settled on our configurationserver
    - Developed, tested, and deployed in development, integration, quality assurance, and user acceptance testing environments
- OES Case Archival Service
    - Hosts services for archiving expunged or sealed cases from the case management systems
    - Additional services to be built here to support archival of complete cases
    - Developed, tested, and deployed in development, integration, and quality assurance testing environments
- Database "Data Vault" Data Store
    - Established location within database to store archived cases (expunged, sealed, etc.)
- General District Case Management System (GCMS)
    - Integrated with the OES Case Archival Service for expungements of unlawful detainers
    - Developed, tested, and deployed in development, integration, and quality assurance testing environments

If additional information is needed about this project, please do not hesitate to contact me at 786-6455.

With best wishes, I am

Very truly yours,

Karl R. Hade

KRH:jrs

cc: Division of Legislative Automated Systems