ASSIGNED COUNSEL PLAN

CASE TRACKING & VOUCHER SYSTEM OVERVIEW

November 15, 2018

Version 3.0

1. Background

The Assigned Counsel Plan ("**ACP**") provides legal representation to indigent persons in New York City pursuant to Article 18-B of the County Law.[1] The Mayor's Office of Criminal Justice ("**MOCJ**") and the Department of Finance ("**DOF**") work collaboratively with ACP and the Appellate Division, First and Second Departments of the New York State Supreme Court, and the New York State Unified Court System ("**UCS**") to carry out this mission. These entities generally provide the following separate and distinct services:

- MOCJ: provides funding, stewardship, and operational support services;
- DOF: provides invoice ("**voucher**") processing and payment audit services; and
- First and Second Departments: oversee the certification and training of 18-B attorneys.

ACP is organized into two departments providing indigent defense services, aligning with Appellate Division, First and Second Departments. Each department in ACP is managed by an administrator ("**Administrator**") responsible for overseeing daily operations.

ACP manages approximately 130,000 cases annually, working with 3,300 private attorneys, experts, and ancillary providers ("**Consultants**"). Administration of ACP is achieved with a staff of 4. Separately, DOF and MOCJ services are supported by approximately 26 staff. ACP and DOF staff currently use two legacy systems, which allow ACP to schedule arraignment shifts for attorneys and manage vouchers. However, these systems do not equip ACP with the ability to effectively calendar case assignments or manage Consultant caseloads, professional activities, performance[2], or program expenditures. As such, ACP seeks to replace its existing systems with a Salesforce-based Case Tracking and Voucher System ("**CTVS**"), capable of managing the complete lifecycle of a case.

2. Case Tracking

The purpose of the CTVS is to link all relevant administrative aspects of a case, including components required to 1) schedule primary arraignment shifts; 2) assign cases; 3) calendar and track court appearances; 4) track consultant activities and time; 5) process voucher payments; 6) audit voucher submissions; 7) track case outcomes; and 8) track ACP expenditures. Establishing an effective CTVS will require integration with the Office of Court Administration's ("**OCA**") criminal data ("**Data**").

OCA Data, as referenced in **Appendix A**, is currently available to ACP and provides validation points to staff who are responsible for auditing, validating, and processing vouchers. Successful development

[1] *https://www.ils.ny.gov/files/County%20Law%2018b.pdf*

[2] *"Performance" relates to the assessment of ACP Consultants based on their ability to provide quality legal aid and other services, and achieve positive outcomes or dispositions.*

of the CTVS is dependent upon continued data integration across the CTVS platform, which will a) reduce data entry and associated errors; b) ensure continuity across systems; and c) inform case tracking workflows. *It should be noted that the CTVS is not intended to serve as a repository for case documents such as legal briefs.*

3. Permission

ACP, Appellate Division, ACP Consultants, DOF, and MOCJ ("**User Agencies**") who provide 1) administrative, audit, or technical support; 2) legal representation or expert/ancillary support services; and/or 3) compensation to those who provide legal or expert representation to indigent persons, shall be granted access to certain OCA Data based on pre-defined roles and associated permissions. A draft version of the permissions can be found in **Appendix A** and **Appendix B**. Separate permissions will apply to report level access. A preliminary list of report types and associated permissions can be found in **Appendix C**.

All permissions are pending validation, which will be confirmed by the selected vendor during the requirements gathering phase of the implementation process.

To further summarize these roles and permissions, i) ACP Administrators and Appellate Division users will be permitted to view all OCA Data, as required to manage daily operations; ii) ACP Consultants will only be permitted to view cases they are assigned and OCA Data elements that are critical to their role; iii) DOF users will only be permitted to view OCA Data elements associated with auditing and processing voucher payments; iv) MOCJ will only be permitted access to aggregate reports to support their role in funding and staffing ACP; and v) all users will be strictly prohibited from downloading or amassing bulk data.

Entities providing cloud services ("**3rd Party Service Providers**") will be controlled by a suite of trust services[3] that govern and restrict access to customer data, which allows for data encryption of fields, attachments, files, and other content. Separately, MOCJ submitted a detailed response to OCA's technical questions on October 3, 2018.

4. Obligation

Each User Agency shall 1) require its staff, agents, subcontractors, and consultants to protect and prevent improper access to OCA Data; 2) ensure that access to OCA Data by staff, agents, subcontractors, and consultants is restricted based on their role, which will be limited on a need-to-know basis in connection with the permitted use; 4) ensure that user authentication mechanisms will be protected and will only be used by the individual to whom they are granted; and 5) familiarize its staff, agents, subcontractors, and consultants with the limitations on access to and use and dissemination of OCA Data.

User Agencies may not copy, backup, or otherwise archive OCA Data for any purpose other than the permitted use. OCA Data **may not be** a) accessed in a mobile or portable device unless the same is password protected and encrypted to prevent improper access; and/or b) stored or transmitted via a thumb drive, flash drive, mobile device, or similar device. Upon launching the application, users will be

[3] *https://resources.docs.salesforce.com/214/latest/en-us/sfdc/pdf/salesforce_platform_encryption_implementation_guide.pdf*

presented with a clickwrap[4] agreement, reinforcing the data restrictions and obligations as outlined in this memo. Declining the policy will prevent the user from accessing the application.

The system will i) reside in a secure, FedRAMP approved GovCloud platform; ii) integrate with NYC.ID with 2-factor authentication; and iii) enable encryption in-transit and at rest. File transfer mechanisms will maintain up-to-date encryption technology to prevent inadvertent disclosure to unauthorized individuals.

OCA will provide sufficient notice to MOCJ prior to implementing changes to data structures or associated interfaces.

5. Data

OCA Data requested for integration with the CTVS is referenced in **Appendix A**, **Appendix B**, and the **UCS Bulk Data Application** (submitted to OCA on August 3, 2018). This Data will allow ACP Administrators to assign cases to ACP Consultants certified on Criminal, Criminal Appellate, Integrated Domestic Violence, Parole, and Criminal Supreme Court panels. All OCA Data referenced in **Appendix A** supports existing ACP systems. Additional OCA Data elements requested are referenced separately in **Appendix B** and are available on the DataShare platform.

To limit the transmission of data, the vendor will be provisioned with access to a subset of the data tables and elements available through DataShare. For example, a restricted database view may be created representing only the data elements described in **Appendix A** and **Appendix B**. This data will be accessed by the vendor during the course of the implementation process through a secure connection. Upon delivery of the CTVS, the vendor will return encryption keys to MOCJ.[5]

6. Retention

ACP systems contain datasets from a variety of sources. Automated retention rules for OCA Data sources will ensure that 1) protected and confidential data elements are masked immediately upon notification when a case has been sealed; 2) data destruction policies are enforced when a case has exceeded the Appellate Division's seven (7) year post-closing-payment[6] retention requirement, barring any active exception codes[7] on the case; and 3) static aggregate reports based on sealed or destroyed OCA Data will remain available in the CTVS for program oversight and management purposes. Additional automated retention policies will govern non-OCA Data generated internally by CTVS users. MOCJ will work closely with OCA to implement any technical data sync protocols that may be required.

7. Family Court Act, Section 262

Family court 18-B programs are managed by another entity with its own set of administrators. The Attorneys for Children ("**AFC**") program administers these 18-B cases in family court. AFC is aligned with each Appellate Division Department. . The New York State Comptroller processes vouchers for 18-B providers who handle family court cases where a child is defended. DOF processes vouchers for other family court cases where an adult is defended by an 18-B provider.

---

[4] A clickwrap or clickthrough agreement is a digital prompt that offers individuals the opportunity to accept or decline a digitally mediated policy.

[5] For additional information related to cloud security, please see the responses submitted to OCA, by MOCJ and Salesforce on October 3, 2018, in response to the UCS Security Checklist.

[6] "Post-closing-payment" is defined as the final payment issued to the Consultant upon case disposition.

[7] Exception codes refer to post-disposition cases that have been restored to the calendar.

OCA Data specific to the Administrative Order, referenced in **Attachment A**, grants ACP access to certain proceedings for the purpose of monitoring and processing vouchers for attorneys representing adults in Family Court pursuant to Section 262 of the Family Court Act.

The CTVS will provide DOF with a mechanism for processing these voucher types, but it will not include case assignment or case management functionality. The Use and Dissemination Agreement associated with this data can be found in **Exhibit A**. Draft permissions for this data are referenced in **Appendix D**.

As referenced above, all permissions are pending validation, which will be confirmed by the selected vendor during the requirements gathering phase of the implementation process.