ITEM 7.4.0 | TRANSPORT

All data transport should be secured and encrypted in compliance with ECF 4.0.1, Section 5, Service Interaction Profiles, as augmented below. See Appendix B – [FIPS-180-2] and Appendix C).

- Data Exchange Protocol: Enhanced transport requirements shall be Secure HTTP (HTTPS) that consists of the standard HyperText Transfer Protocol (HTTP) layered on top of a secure Transport Level Security (TLS) session. To maximize security, any public-facing interface should be registered with a Certificate Authority ("CA); either a commercial service or maintained via the State Courts System. For the best security, 2048-bit (or more) key lengths should be used. For closed data center environments where communications occur between trusted servers, TCP may also be used (See Appendix A).

- Web Services: To ease implementation, the use of the Web Services Description Language ("WSDL") is strongly recommended, as it helps automate the creation of compliant interfaces for clients by providing a machine-readable description of the web service.

Data transport includes the transfer of data to the state and other repositories. For example, Section 2, E-Filing Standards, identifies the capability to transfer case and court activity data, both as single records and in bulk, to state-level data repositories as an essential capability of court data management systems. Transfers may be made for a wide variety of purposes including routine activity reporting, program and performance monitoring, resource allocation, court operations management, and data warehousing. The transfers may use a wide variety of data exchange scenarios, e.g., a data transfer initiated by a local data provider to a receiving state repository in response to changes within the underlying data being reported (event-push), or a transfer where the request originates from the repository to the local data management system (timed-pull). Consequently, the general web services capability established at either end of the data transfer should be capable of handling both types of transactions. The specific strategy, event-push or timed-pull, should be identified by the entity originating the transaction as part of the data request package definition.

It is recommended that data transfer occur using the lowest level, stable technology suitable for the task, in conformance to this standards document. However, it may be necessary to define

alternate data transfer mechanisms, such as FTP or FTPS, in order to maintain compatibility with legacy reporting systems or when reporting is sufficiently short-term or is of such a nature as to not justify the cost to develop a web services solution. The suitability of alternative transfer mechanisms should be determined by the entity originating the reporting requirement and approved by this standard's governing body.

While this data transfer standard is comprehensive, not all elements defined for a data request package may apply to a given exchange scenario. Since the data request may involve a large number of agencies, the entity originating the request should define a data transfer package description document detailing the format and content of the data being transferred and identifying the appropriate auditing and tracking elements as provided in this standard. This information may be included as part of the integration kit discussed below. If necessary, to ensure data transfer integrity, the service enabling the specific data transfer should provide for immediate, synchronous response to, for example, allow a service to initiate a transfer and the receiving service to signal success or failure of a transfer. (See Appendix C).