COMMONWEALTH of VIRGINIA

Office of the Governor

Data Sharing and Analytics Governance Structure for the Commonwealth of Virginia

Report Submitted to the General Assembly Pursuant to Chapter 679 of the 2018 Acts of the Assembly

Version 1.0

September 18, 2019

Data Sharing and Analytics Advisory Committee

Table of Contents

Executive Summary

According to the 2017 Executive Directive 7 Final Report, Leveraging the Use of Shared Data and Analytics (*Appendix 1*), only 22.2% of the Commonwealth's 1,686 enterprise data assets were shared outside of the source agency due to a "complex array of federal and state laws, regulations, program rules, and related policies." The report also mentions state agencies have developed a risk-averse culture opting to not share data by default. Further, agencies do not have the necessary "technical, financial, or personnel resources to sustain data sharing relationships" or initiate and manage data analytics projects.

The ED7 report also stated:

> *Several provisions in the Code of Virginia place general restrictions on agencies seeking to share data. State statutes also significantly limit the use of shared data in some contexts, such as provisions in the law that prevent agencies from using data on citizens except for the purpose for which the data was collected.*

Data governance and sharing will benefit the Commonwealth by improving operational efficiency, reducing cost, improving our data security posture by minimizing risk and reducing vulnerabilities, supporting outcome-based performance management, eliminating duplicative efforts, and facilitating the development of solutions to complex, multi-disciplinary problems. The ability for Executive Branch Agencies, Institutions of Higher Education, Commissions, Localities, and other Commonwealth-affiliated organizations to share data, information, knowledge, and intelligence raises the collective value of our data assets.

The recommended governance structure to support data sharing and analytics includes a Data Commission (*Appendix* 2) to set, plan, and prioritize data sharing performance goals for the Commonwealth, review agency accomplishments, and provide recommendations to the Governor and the General Assembly on any changes to laws or funding necessary to achieve desired objectives. The Data Commission should be established as an advisory commission in the executive branch of state government and consist of 25 members that include 8 legislative members, 7 non-legislative citizen members, and 10 state officials.

In addition, the Data Sharing and Analytics Advisory Committee recommends a governance structure for organizations conducting data operations (*Appendix* 3). These organizations, which are not limited to the executive branch of state government, are responsible for the collection, storage, management, protection, use and dissemination of data assets. The recommended governance structure facilitates communication and collaboration between executives, senior managers, and technical personnel. The data operations governance structure includes an Executive Data Board, Data Governance Council, Data Governance and Analytics Program Office, and Data Stewards Group.

The Executive Data Board sets strategic performance objectives, advocates for and allocates program and project resources, and coordinates, prioritizes, and oversees multi-agency data sharing and analytics projects. The Data Governance Council advises the Executive Data Board and the Commonwealth Data Commission on technology, policy, and governance strategies to meet Chapter 679 requirements. In addition the Data Governance Council governs the Commonwealth Data Trust promoting greater utility and accessibility of data assets. The Data Governance and Analytics Program Office manages the operation of the Commonwealth Data Trust, advises state agencies and political subdivisions regarding state best practices, standards, and policies, makes government data available, and ensures its security. Lastly, the Data Stewards Group facilitates secure and appropriate data sharing and use of data assets in support of data-driven policymaking, research, and analysis through the implementation of state standards, policies, and best practices.

Introduction

The General Assembly of Virginia in the 2018 Session enacted Chapter 679 of the Acts of the Assembly ("Chapter 679"), establishing the position of Chief Data Officer of the Commonwealth ("Chief Data Officer"), joining 16 other states that have created similar positions. Chapter 679 also created the Data Sharing and Analytics Advisory Committee ("Advisory Committee") to develop a permanent data sharing and analytics governance structure for the Commonwealth.

The Chief Data Officer, who serves under Virginia's Secretary of Administration, is charged with coordinating and overseeing the effective use and sharing of data among state, regional, and local public entities and public institutions of higher education and providing data governance recommendations to the Commonwealth CIO to maintain data integrity and security, support data analytics research, promote business intelligence for actionable decision-making, and facilitate access to open data where appropriate.

The recommendations in this report are intended to empower the Chief Data Officer to securely and effectively accomplish the following objectives:

- Promote and facilitate, subject to all applicable federal and state laws, rules, and regulations, the secure and appropriate sharing and use of data assets of the Commonwealth in support of data-driven policymaking, research, analysis, study, and economic development.
- Maximize the value and utility of Commonwealth data related investments and assets
- Promote increased data sharing between state agencies and localities providing tangible operational improvements assisting state agencies and localities in fulfilling their missions in a more coordinated, cost-efficient manner
- Leverage government data, using appropriate security and privacy standards, supporting evidenced-based policymaking addressing high priority public policy issues
- Provide for public access to certain data assets, where lawful and appropriate, enhancing research, innovation, and insight

Previous Activities

The report reflects previous activities relating to data sharing, governance, and analytics, under development within the state government since 2011. The following initiatives reflect a portion of the existing governance framework and the state government's accomplishments, to date. Artifacts from these milestones and deliverables have been identified in Appendix 1.

- State Council of Higher Education for Virginia Ad Hoc Committee on Data and Policy (Ongoing): SCHEV established this committee to examine its existing data assets to assess how SCHEV can improve how the data assets are used and applied to policy development and implementation. The committee developed a set of policy questions designed to ensure excellence in Virginia higher education, inform students about their educational pursuits, and measure the impact of

education on Virginia economic and civic prosperity. The 12 questions can be found at the following URL: http://www.schev.edu/docs/default-source/about-section/council-files/2018-council-meetings/september/handout-1-at-joint-meeting---datapolicygoalsbw.pdf

- SCHEV also hosts the Virginia Longitudinal Data System (VLDS) featuring participation from multiple state agencies. Since 2012, the VLDS has had a strong trust-based governance model with oversight by a central coordinating body known as the Data Governance Council consistent with the framework presented in this report.
- Data Sharing among State HHR Agencies Report (2018): The Secretary of Health and Human Resources submitted a report to the Governor and the General Assembly providing a summary of agency activities and recommendations in response to House Bill 2457 passed during the 2017 session. The report states agencies reviewed data sharing policies, procedures, and existing agreements, developed or enhanced existing forms and templates for data sharing and non-disclosure agreements, and many are participating in the Virginia Longitudinal Data System (VLDS) as a means of sharing data with other agencies and academic researchers. The report recommends standardization and coordination of data sharing practices across agencies and "guidance to help agencies understand what types of data sharing are permissible (or not permissible), and a mechanism to make data sharing simple and secure."
- Executive Directive 7 (2017): The Secretary of Technology submitted to the Office of the Governor a comprehensive report on data sharing, analytics, and open data activities across the state government. The report identified constraints to data sharing, provided a cross-sectional view of data analytics capabilities, and offered recommendations on how to promote greater utility and accessibility of information assets collected and maintained by state agencies.
- Governor's Data Analytics Summit (2017): The Office of the Governor sponsored a two-day conference on data sharing, governance, and analytics. Participants included representatives from public and private sector organizations, nongovernmental organizations, and higher education. The first day of the conference was dedicated to all-day workshops focused on the legal, policy, governance, and technology foundations for data sharing in the Commonwealth. This led to the concept of the Commonwealth Data Trust and informed the legislation that was to become Chapter 679.
- Commonwealth's Open Data Portal (2017): The Secretary of Technology, Library of Virginia, and VITA established a public-facing open data portal, located at http://www.data.virginia.gov/. The open data portal supports the discovery, accessibility, and utilization of the state's open data assets.
- Statewide Address Database Feasibility Study (2017): The Secretary of Transportation was tasked to "convene a task force to study the feasibility of establishing a statewide one-stop online portal for address changes for the purposes of developing a statewide address database." The Secretary of Transportation submitted the report to the Governor and the General Assembly concluding that "a statewide, one-stop online change of address portal and statewide address database" should not be authorized due to the "tremendous Commonwealth

resources" required and "the laws, regulations, and business rules restricting the ways in which the portal and database can be used will limit its usefulness". The report also cites that the project is "technically feasible" and could provide (minimal) benefits to citizens and agencies. The report concludes with a recommendation to expand the scope of the project to include the delivery of other data integration services in addition to the address portal and database.

- Commonwealth HHR Data Governance (2016): The Secretary of Health and Human Resources (HHR) provided a report to the Governor and the House Appropriations and Senate Finance Committees describing a plan to improve the data governance structure in HHR agencies in order to streamline business processes, increase operational efficiency and effectiveness, and minimize duplication and overlap of current and future systems development. The report identified several actions and initiatives to address data governance, privacy, and security within the HHR Secretariat including HIPAA compliance across all HHR agencies, extend "proper purpose" to include HIPAA-defined uses, update the eMOU (enhanced Memorandum of Understanding) developed in 2012 to extend beyond HHR agencies creating a Commonwealth-wide data trust, establish enterprise level "Analytics as a Service", establish a cross-agency data governance structure, and establish a "Public-Private Data Collaborative" similar to the Commonwealth Data Commission described in the Advisory Committee's recommendations below.
- Governor's Data Internship Program (Ongoing): The Office of the Governor and the Secretary of Technology implemented the internship program in 2014 to pair interns from universities with state agencies using their data to perform advanced analytics on "real-world" problems. This program is now housed within VITA's Innovation Program (VIP) as the Commonwealth Data Internship Program and includes partnerships with DMV (https://datascience.virginia.edu/projects/can-you-predict-motor-vehicle-accidents) and DCLS (https://datascience.virginia.edu/projects/keeping-infants-healthy-across-commonwealth).
- Executive Directive 6 (2015): Governor McAuliffe issued Executive Directive 6 to expand cyber-related risk management activities and protections that safeguard the information entrusted to the Commonwealth's executive branch agencies. VITA and the Secretary of Technology conducted an inventory of all data systems providing a report with recommended strategies to strengthen and modernize agencies' cybersecurity posture.
- Data Stewards Groups (2014): VITA established three data steward groups – Executive, Functional (Business), and Technical Data Stewards – to support ongoing agency engagement and direction for implementation of the EIA Strategy and related data governance activities.
- Governor's Datathon (Ongoing): The Office of the Governor and the Secretary of Technology hosted the first annual "Datathon" challenge in 2014 to promote the use of open data and data analytics. Teams representing state agencies, local governments, universities, and private industry have competed to build applications and analytics toolsets aligned with the Governor's Policy Priorities. This year's datathon is in partnership with the Department of Education with a focus on 'Equity in Education'.

- Commonwealth Enterprise Information Architecture (EIA) Strategy (2013): The Secretary of Technology adopted an enterprise data strategy, developed with input from agency leaders, business managers and technical leads. Strategic goal areas: Data governance, data asset management, data standards, and data sharing.
- Data Exchange Standards for Interoperability: The Secretary of Technology and CIO of the Commonwealth, to date, have adopted more than 130 data exchange standards to promote interoperability for information exchange. Standards cover administrative data for core operations of state government, as required by the 2008 Appropriation Act; health information, on recommendation from the Commonwealth's Health IT Standards Advisory Committee (HITSAC) pursuant to § 2.2-2699.7; and the National Information Exchange Model (NIEM) for citizen-centric data, required under Item 427 of the 2012 Appropriation Act.
- Secretarial Committee on Data Sharing (2012): Committee formed in September 2011 by the Secretaries of Technology and Health and Human Resources to explore opportunities and constraints for an enterprise data-sharing agreement for state agencies. The committee published a report in 2012 with five recommendations including the establishment of a trust-agreement framework and governance model to support enterprise data sharing; formation of a governance committee to develop, implement, and maintain the trust-agreement framework; identification of applicable legal, regulatory, and policy constraints and requirements for informed consent and authorization; and development of standards, policies, guidelines, and procedures to govern the implementation of the trust-agreement framework. The enhanced Memorandum of Understanding (eMOU) is the product of the collaboration between the Secretaries of Health and Human Resources, Public Safety, Commerce and Trade, Technology, and Transportation with the goal of enhancing the security of data maintained and exchanged between participating organizations. The first version of this document was published July 2012 with over 15 revisions to date. The original document has been adopted and revised by multiple states including Indiana, Illinois, and Arizona.

Foundations for Evidence-based Policymaking Act (FEPA) of 2018

President Trump signed the Foundations for Evidenced-based Policymaking Act into law on January 14, 2019. The new law recognizes the role of the federal government in leveraging data as a strategic asset to inform decision-making and drive evidence-based policy. In addition to making government data open by default, the law contains provisions establishing the role of the Chief Data Officer, an enterprise data catalog, and a data governance council. The law contains four titles with Title II, the OPEN Government Data Act, mandating the organizational changes required to support data governance.

Title I – Federal Evidence-Building Activities

Title I establishes the foundation for outcome-based performance management by requiring agencies (specifically CFO-Act agencies) to develop agency evaluation plans defining key

questions, data requirements, stakeholder engagement (including public, agencies, State and local governments, and non-governmental researchers), and establishing the role of the evaluation officer. The evaluation officer is responsible for assessing the ongoing evaluation capabilities of the agency and establishing the agency's evaluation policy. This title also establishes the Advisory Committee on Data for Evidence Building charged with reviewing, analyzing, recommending actions and initiatives to promote the use of Federal data for evidence building. This title creates the framework for agencies to determine whether they are successful in meeting their desired outcomes.

Title II – OPEN Government Data Act

The Open, Public, Electronic, and Necessary Government Data Act establishes the Federal Data Catalog, the role of the Chief Data Officer (CDO), and the Chief Data Officer Council as well as declaring that federal data should be open by default while taking into account the need for protecting confidential or sensitive data. Thus, maintaining public trust in the federal government's ability to safeguard personal information. In addition, the title includes language requiring agencies to consider risks, restrictions, and security considerations to mitigate the 'mosaic' effect or the ability to identify an individual through the integration of multiple 'open' data assets.

This title also requires agencies to develop and maintain an Information Resources Management Strategic Plan describing how information technology helps the agency accomplish its mission, satisfies the open data requirement, facilitates collaboration with non-Government entities, and improves data quality. It also mentions designating a point of contact (data steward or custodian) within the agency to assist the public and respond to data quality issues as well as identify and implement methods to monitor data usage by users within and outside the agency.

This act also requires each agency develop and maintain a comprehensive data inventory accounting for all data assets created by, collected by, under the control or direction of, or maintained by the agency for inclusion in the Federal Data Catalogue pursuant to guidance by the director of the Office of Management and Budget (OMB). The Federal Data Catalogue is the single public interface established and maintained by the General Services Administration (GSA) as a point of entry dedicated to sharing agency data assets. In addition to the catalogue, the act includes developing and maintaining an online directory of tools, best practices, and schema standards to facilitate the adoption of open data practices across the Federal Government.

The OPEN Government Data Act requires each CFO-Act agency to designate a nonpolitical appointee employee as the Chief Data Officer responsible for lifecycle data management, establishing data standards, coordinating data use to meet mission goals, ensuring compliance with data management best practices, coordinating with the Chief Information Officer to ensure

the information technology infrastructure supports data assets accessibility, and supporting the Performance Improvement and Evaluation Officers of the agency.

Lastly, Title II establishes a Chief Data Officer Council within the Office of Management and Budget to establish Government-wide best practices, promote and encourage data sharing agreements, improve evidence-based policymaking, engage stakeholders, and evaluate new technology solutions for improving the collection and use of data. Council membership includes the CDOs from each of the 24 CFO-Act agencies, the Administrator of the Office of Electronic Government, and 2 ex-officio members representing Chief Information Officers and Evaluation Officers. The council is also responsible for submitting a biennial report of its activities to the OMB Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Government Reform of the House of Representatives.

Title III – Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

One of the driving forces behind this act is the need for continued public cooperation in statistical programs. The act cites the declining trust of the public in the government's ability to protect private and/or confidential information and how the decline adversely affects both the accuracy and completeness of statistical analyses. Therefore, the purpose of the act is to ensure private or confidential information supplied is used exclusively for statistical purposes, information will not be disclosed in identifiable form to anyone not authorized nor used for any non-statistical purpose.

The act also defines the requirements for disclosure of identifiable information including informed consent by the respondent, approval by the head of the agency, and not prohibited by any other law. Title III establishes the willful disclosure of identifiable information to a person or entity not entitled to receive it as a class E felony with imprisonment for not more than 5 years or fined up to $250,000 or both.

Recognizing the value of data sharing to improve agency efficiency, reduce reporting burdens on individuals and organizations, and provide enhanced citizen-centered services, the act directs the head of an agency to make any data asset maintained by the agency available, upon request, to any statistical agency or unit. CIPSEA requires the OMB Director to set sensitivity and accessibility standards that agencies can use to assess each data asset owned or accessed as well as the criteria for determining the sensitivity level and corresponding accessibility to promote consistency across the Federal Government. In addition, standard criteria shall be developed to determine whether a less sensitive and more accessible version can be produced and standards for removing or obscuring sensitive data to remove the identity of the data subject.

In order to further promote data sharing, the act requires the OMB Director establish an application process allowing agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals request access to data accessed or acquired by statistical agencies or units. This standard process shall include a common application form, access criteria specifications, timeframe requirements, appeals process definition, and transparency standards including the public reporting of all applications received, status of each application, the final determination, and any other information to ensure full transparency.

This new law details some of the primary components required to implement appropriate data governance and promote data sharing at the federal level. Although the size and scope of the Federal Government is considerably different from that of the Commonwealth, significant similarities exist to warrant further investigation to determine how the new law can positively influence the commonwealth's data governance structure.

Recommended Governance Structure for the Commonwealth of Virginia

The General Assembly of Virginia in the 2018 Session enacted Chapter 679 of the Acts of the Assembly ("Chapter 679") to mitigate some of the data sharing restrictions identified in the 2018 Report on Implementation of HB2457 – Data Sharing Among State Health and Human Resources Agencies (Chapter 467, 2017) by defining "proper purpose" as it relates to inter-agency data sharing.

> *"Proper purpose" includes the sharing or dissemination of data or information among and between agencies in order to*
>
> *(i) streamline administrative processes to improve the efficiency and efficacy of services, access to services, eligibility determinations for services, and service delivery;*
>
> *(ii) reduce paperwork and administrative burdens on applicants for and recipients of public services;*
>
> *(iii) improve the efficiency and efficacy of the management of public programs;*
>
> *(iv) prevent fraud and improve auditing capabilities;*
>
> *(v) conduct outcomes-related research;*
>
> *(vi) develop quantifiable data to aid in policy development and decision making to promote the most efficient and effective use of resources; and*
>
> *(vii) perform data analytics regarding any of the purposes set forth in this definition*

While this legislation expands the scope and paves the way for increased data sharing amongst Executive Branch Agencies, it does not address the fundamental need for enterprise-wide data governance across the Commonwealth. The lack of a comprehensive data inventory as well as data standards, data dictionaries, and regulation and compliance surrounding data quality makes understanding agency data very difficult both internally as well as externally between agencies. While organizations are focused on their mission mandates and operational goals, they may not be aware of the impact their data can have on the effectiveness of their sister agencies or organizations. As such,

agencies have little incentive to document or model their respective data beyond their current operational interests.

The Data Governance Framework resulting from the previously mentioned activities and deliverables (*see Previous Activities section*) not only helped to inform the agency engagement and analysis presented in this report, the framework recommended by the 2016 HHR report serves as a potential starting point for the state government to act on the recommendations.

Commonwealth of Virginia Data Commission

The Advisory Committee recommends the creation of the Commonwealth Data Commission (*Appendix* 2) similar to the "Public-Private Data Collaborative" described in the 2016 HHR report on data governance. This should be an executive branch advisory commission with 25 members including 8 legislative, 7 citizen, and 10 state officials. The 8 legislative members should consist of four members from the House of Delegates appointed by the Speaker of the House, in accordance with the principles of proportional representation contained in the Rules of the House of Delegates, and 4 members of the Senate appointed by the Senate Committee on Rules. The Governor shall appoint one non-legislative citizen member from each of 7 geographic regions to represent the interests of the localities, academia, and technology council of their respective region. At least one member must represent the locality perspective, one from academia, and one from our technology partners. The commission shall also include the Chief Data Officer, the Attorney General or his designee, and a data governance representative from each of the following:

1. Administration, Finance, and Commonwealth Secretariats
2. Agriculture and Forestry and Natural Resources Secretariats
3. Commerce and Trade, Workforce, and Education Secretariats
4. Health and Human Resources and Veterans and Defense Affairs Secretariats
5. Public Safety and Homeland Security Secretariat
6. Transportation Secretariat
7. Legislative Branch
8. Judicial Branch

The commission shall review agency accomplishments; plan, prioritize, report, advise, and make recommendations to the Governor and the General Assembly on changes to the Budget and Code of Virginia to meet data governance, quality, sharing, analytics, and outcome-based performance goals and objectives; study the operations, management, jurisdiction, powers, and interrelationship of any such department, board, bureau, authority, or other agency that has any direct data operation including collection, storage, management, quality, transfer, analysis, and dissemination; review and comment on data-related budget items on annual state operating budget requests; define responsibilities among state agencies and other operational units for various data governance programs and to encourage data sharing among agencies, departments, bureaus, and other commonwealth organizations; monitor the data governance, sharing, and analytics development efforts of other states and nations; and develop

recommendations that will assist in making Virginia a national leader in evidenced-based policy and data-driven decision making. Staff assistance shall be provided to the Commission by the Data Governance and Analytics Program Office.

Data Operations

In addition to creating the Commonwealth of Virginia Data Commission to facilitate communication between data operators, legislators, and the public, the Advisory Committee also recommends the following governance structure to support organizations who conduct ongoing data operations. These organizations, which are not limited to the executive branch of state government, are responsible for the collection, storage, management, protection, use and dissemination of data assets. The recommended governance structure facilitates communication and collaboration between executives, senior managers, technical personnel, and data consumers. Governance should be driven by a Data Governance Council, with executive oversight, strategic goals, and performance objectives defined by an Executive Data Board. The Data Stewards Group informs the Data Governance Council of the technical needs and issues encountered as it implements the policies set forth by the Executive Data Board. The Data Governance and Analytics Program Office maximizes the value and utility of Commonwealth data-related investments by promoting data sharing between state agencies, localities, and other organizations providing tangible operational improvements assisting these organizations in fulfilling their respective missions in a coordinated, cost-effective manner.

This governance model (*Appendix* 3) will enable the Commonwealth to implement policies, standards, and best practices supporting the exchange and effective use of data by state agencies, localities, and other commonwealth organizations. The Data Governance Council defines, develops, and recommends policies, standards, and best practices to achieve performance targets set by the Executive Data Board and implemented by the Data Stewards Group. Appendix 4 represents the implementation of the recommended governance model currently supporting the DCJS Opioid Data Sharing and Analytics Platform Pilot.

Executive Data Board

The Advisory Committee recommends grouping the major organizational units by function and establishing an Executive Data Board to provide oversight of the Data Governance Council. The Executive Data Board proposes strategic goals and performance objectives to their respective state leaders for approval as well as advocate for and allocate program resources. The Executive Data Board shall chaired by the Chief Data Officer and consist of Commonwealth Executive Leadership, and other policy level stakeholders, as determined by the leadership of the Executive, Legislative, and Judicial branches of state government. The Executive Data Board will meet annually to review prior performance goals, identify new goals and objectives, set overall policy direction, and coordinate, prioritize, and oversee multi-agency data sharing and analytics programs with the purpose of improving citizen-centered services, monitoring agency performance, and removing obstacles to data sharing among commonwealth organizations. In

addition, the Executive Data Board shall appoint a representative to the Commonwealth Data Commission from each of the following:

1. Administration, Finance, and Commonwealth Secretariats
2. Natural Resources and Agriculture & Forestry Secretariats
3. Workforce, Education, and Commerce & Trade Secretariats
4. Health & Human Resources and Veterans & Defense Affairs Secretariats
5. Public Safety and Homeland Security Secretariat
6. Transportation Secretariat
7. Legislative Branch Operations
8. Judicial Branch Operations

Data Governance Council

The Advisory Committee recommends the creation of a Data Governance Council representing each of the organizational units mentioned above. The Data Governance Council is responsible for the governance of the Commonwealth Data Trust and administration of the permanent governance structure for the Commonwealth. The membership of the Data Governance Council shall be determined by the Executive Data Board. Agency participation on the council is voluntary if the agency is not a member of the data trust, but highly encouraged since the council acts as a bi-directional communication vehicle between operational units and the Commonwealth CDO. The council is expected to meet quarterly to execute the following functions:

- Advise the Executive Data Board and the Commonwealth Data Commission on technology, policy, and governance strategies to meet the Chapter 679 requirements.
- Govern the Commonwealth Data Trust
- Provide a governance, policy, and technology framework for information sharing, promoting greater utility and accessibility of data assets
- Recommend policies, standards, and guidelines for the formation, operations, and maintenance of the Data Governance Council
- Recommend policies, standards, and guidelines for defining, managing, approving, and distributing 'Open Data' maintained by state agencies
- Report progress, compliance, and performance to the Executive Data Board and the Commonwealth Data Commission
- Coordinate among agency projects and activities, to prevent duplication of functions, and to combine all agency data governance plans into a comprehensive interagency state plan

Commonwealth Data Trust

The Advisory Committee recommends founding the permanent governance structure for the Commonwealth on a trust framework-based governance model. Trust frameworks are multi-party agreements that establish a common set of rules and policies for an information sharing environment. They define the business, legal, and technical requirements for member parties to share data in a secure, compliant manner.

The Commonwealth Data Trust or "CDT" is a safe, secure, and legally compliant information sharing environment. The CDT is a multi-stakeholder data exchange and analytics platform to inform a holistic, cross-discipline response to the opioid crisis and other complex, multi-disciplinary concerns. The proposed CDT will ensure the privacy and security of sensitive personally identifiable information (PII, PHI, and SBU) through the development of a common de-identification algorithm deployed to all agencies that share data in the secure information sharing environment. This anonymization will allow the de-identified record-level data to be shared amongst member parties through a multi-tiered security model without violating federal or state laws, regulations, or policies.

The Commonwealth of Virginia has a precedent for being a member party to trust frameworks. Virginia's Department of Motor Vehicles operated a trust framework for the Cross Sector Digital Identity Initiative (CSDII), the state's pilot project under the National Strategy for Trusted Identities in Cyberspace. Also, the Virginia Department of Health participated in a trust framework operated by Connect Virginia, the statewide health information exchange. In addition, the proposed CDT builds on the governance models of the Virginia Longitudinal Data System (VLDS) and the Workforce Data Trust supporting the Common Access Portal. Core components of trust frameworks have been documented in Appendix 5.

The Data Governance Council will develop a trust framework based on the following principles:

- Establish consistent requirements for member parties through a standardized data sharing agreement process.
- Provide a scalable alternative to multiple "point-to-point" agreements, which are not sustainable for widespread information exchange.
- Promote trust among member parties by recommending to the Commonwealth CIO common rules for data security, privacy, and confidentiality.
- Reduce technical costs by enabling member parties to onboard to a single information sharing environment using standard NIEM protocols.

Data Exchange Strategy

In 2013, the Commonwealth of Virginia adopted NIEM as the standard protocol for sharing person-centric data. The proposed data trust will feature a NIEM-conformant exchange to (1) promote interoperability among disparate data systems and (2) reduce the cost of sharing data through a single, standards-based environment. The data trust will integrate data from and support multiple vendor platforms, which will be integrated into a single environment.

Data Ownership and Stewardship

The Advisory Committee acknowledges that all Commonwealth data generated with taxpayer dollars belongs to the citizens of the Commonwealth. Executive Branch Agencies and Commonwealth organizations are trusted stewards of that data. Therefore, contracts between the Commonwealth of Virginia and other organizations or entities must ensure data ownership is explicitly documented and representatives of the Commonwealth must always have direct access to the data via Application Programming Interface (API) calls, standards-based web services, and/or direct database connections.

Data Security

Data security is a critical component of the data governance and sharing framework. In addition to the multi-tiered security model, a Sharing Security Matrix will be developed that defines the appropriate risk assessment process for a given sharing request. The risk criteria include, but are not limited to, the sensitivity of the requested data and the relationship between the proposed parties. For example, the risk assessment will be different for intra-agency data sharing, inter-agency data sharing, and sharing data with non-Executive Branch Agencies. As mentioned earlier, the data trust will only contain de-identified data adding another layer of security.

In addition, an Open Data Review Process will be developed to ensure data released for public consumption cannot be combined with other open data to identify persons or organizations. This process will be supported by the Data Stewards Group and the Cross-Agency Data Domain Coordinators with guidance from the Data Governance Council. The Data Governance Council should be responsible for approving all open data releases.

Data Stewards Group

The Data Governance Framework shall provide mechanisms for the prompt identification and resolution of data quality, integrity, and security issues through the establishment and promotion of the Commonwealth Data Stewards Group. The Data Stewards Group shall be composed of volunteers from across the state interested in maximizing the value of the Commonwealth's data assets by promoting and facilitating the secure and appropriate sharing

and use of data assets in support of data-driven policymaking, research, analysis, study, and economic development. The Data Stewards Group provides technical personnel a voice and an opportunity to be engaged in the data governance process. The Data Stewards Group should have multiple working groups to support the needs of the Data Governance Council. The Data Stewards Group should meet quarterly at a minimum with working groups meeting more frequently as needed.

Cross-Agency Data Domain Coordinators

An important function of the Data Stewards Group is the coordination of data assets belonging to the same domain across multiple agencies. The data domain coordinators are able to identify potential data integrity and interoperability issues and propose solutions to the Data Governance Council. Some example domains include, but are not limited to:

- Agriculture
- Economic Development
- Education
- Environmental Quality
- Finance
- Health
- Housing
- Law Enforcement
- Public Safety
- Social Services
- Transportation

Data domains cut across multiple agencies, cabinet offices, and commonwealth organizations requiring coordination and communication. In addition, some data elements are so ubiquitous they require enterprise-level management to maximize interoperability and re-use throughout the organization. The Cross-Agency Data Domain Coordinators is a specific, permanent working group of the Data Stewards Group.

Data Governance and Analytics Program Office

The Data Governance and Analytics Program Office reports to the Chief Data Officer within the Secretary of Administration and directly supports the Data Governance Council in the development of policies, standards, and best practices. This office will manage the Commonwealth Data Trust to facilitate data sharing across the Commonwealth and its partners and provide administrative support to the Commonwealth Data Commission, Executive Data Board, Data Governance Council, and Data Stewards Group (*Appendix 2 and 3*). In addition, the program office will provide guidance, support, oversight, and technical assistance to data trust member agencies and commonwealth organizations in the implementation of data governance,

sharing, security, and analytics projects. Additional responsibilities of the program office include, but is not limited to:

- Advise executive state agencies, commonwealth organizations, and political subdivisions regarding state best practices concerning the creation and maintenance of data
- Coordinate data analytics and transparency master planning for the executive branch agencies and provide leadership regarding state data analytics and transparency
- Collect, analyze, and exchange government information
- Advocate for data sharing providing expert guidance on federal and state data privacy laws
- Conduct operational and procedural audits of executive state agencies data governance and sharing implementations
- Identify data integration and business intelligence opportunities that will generate greater efficiencies in state agencies, departments, and institutions
- Leverage data from transactional systems for enterprise-level state business intelligence
- Compare capabilities and costs across state agencies
- Ensure data integration and sharing is performed in a manner that preserves data privacy, security, and confidentiality in transferring, storing, and accessing data, as appropriate

Proposed Program Office Staff

Based on an analysis of the composition of Indiana's Management Performance Hub (*Appendix 6*) and North Carolina's Government Data Analytics Center (*Appendix 7*), the Advisory Committee recommends the following positions be included in the Data Governance and Analytics Program Office. These positions cover the breadth and depth required to meet the current data governance, sharing, and analytic needs of the commonwealth.

- Chief Data Officer (political appointment)
- Deputy Chief Data Officer
- Program Coordinator
- Data Privacy Officer/General Counsel
- Data Security Analyst
- Data Scientist
- Data Analytics Project Manager*
- Data Analytics Specialist*
- Business Intelligence Specialist*
- Communications/Outreach/Engagement Manager
- Communications Analyst*
- Technical Project Manager*
- Data Architect*

- Data Engineer*

* Potentially more than 1 person

The Chief Data Officer is the only politically appointed position. The remaining positions should be non-political appointments to ensure continuity of operations between administrations. Additionally, the Advisory Committee recommends the compensation for the Chief Data Officer, Deputy Chief Data Officer, and Program Coordinator should be an appropriation from the General Funds while the remaining positions could be funded through VITA's charge-back structure based on agencies' consumption of data storage as defined by item 84.30 in HB1700 during the 2019 Session. However, there is concern among Advisory Committee members that drawing financial support for this office based on agencies' consumption of data may disincentivize agency participation or encourage agencies to 'game' the charge-back model by minimizing data storage and ultimately data sharing. The committee recommends further investigation of dedicated central funding mechanisms, equitable distribution models, and visible incentives to assure compliance, participation, and engagement.

Appendix 1. Artifacts from Previous Data Sharing and Analytics Activities

VLDS: VLDS Book of Data Governance Version 2.1 February 16, 2017

http://vlds.virginia.gov/media/1087/vlds_book_of_dg.pdf

VITA Executive Directive 6: Cyber-related Risk Management Activities and Protections

https://www.vita.virginia.gov/about/news-events/news-archive/2015-news--events/governor-mcauliffe-signs-executive-directive-6.html

VITA Executive Directive 7 Final Report: Leveraging the Use of Shared Data and Analytics

https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/pdf/ExecutiveDirective7.pdf

Secretary of Health and Human Resources and Secretary of Technology: Secretarial Committee on Data Sharing. Committee Report and Recommendations, Version 2.2. March 2012

https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/pdf/SCDS_DURSA_Report.pdf

Commonwealth Enterprise Information Architecture (EIA) Strategy:

https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/pdf/Commonwealth_EIA_Strategy_FINAL.pdf

ITRM Data Exchange Standards:

https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/commonwealth-data-standardization-plan/pdf/Item_427-FinalPlanSoTechTransmittal_07012013.pdf

NIEM Adoption Strategy:

https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/commonwealth-data-standardization-plan/pdf/Appendix_2-NIEMCorePersonStandardNarrative.pdf

Adopted Health IT Standards:

https://www.vita.virginia.gov/media/vitavirginiagov/about/pdf/itac-and-hitsac-archives/COVHealthITStandardsAdoptedHITSACAug2016.pdf

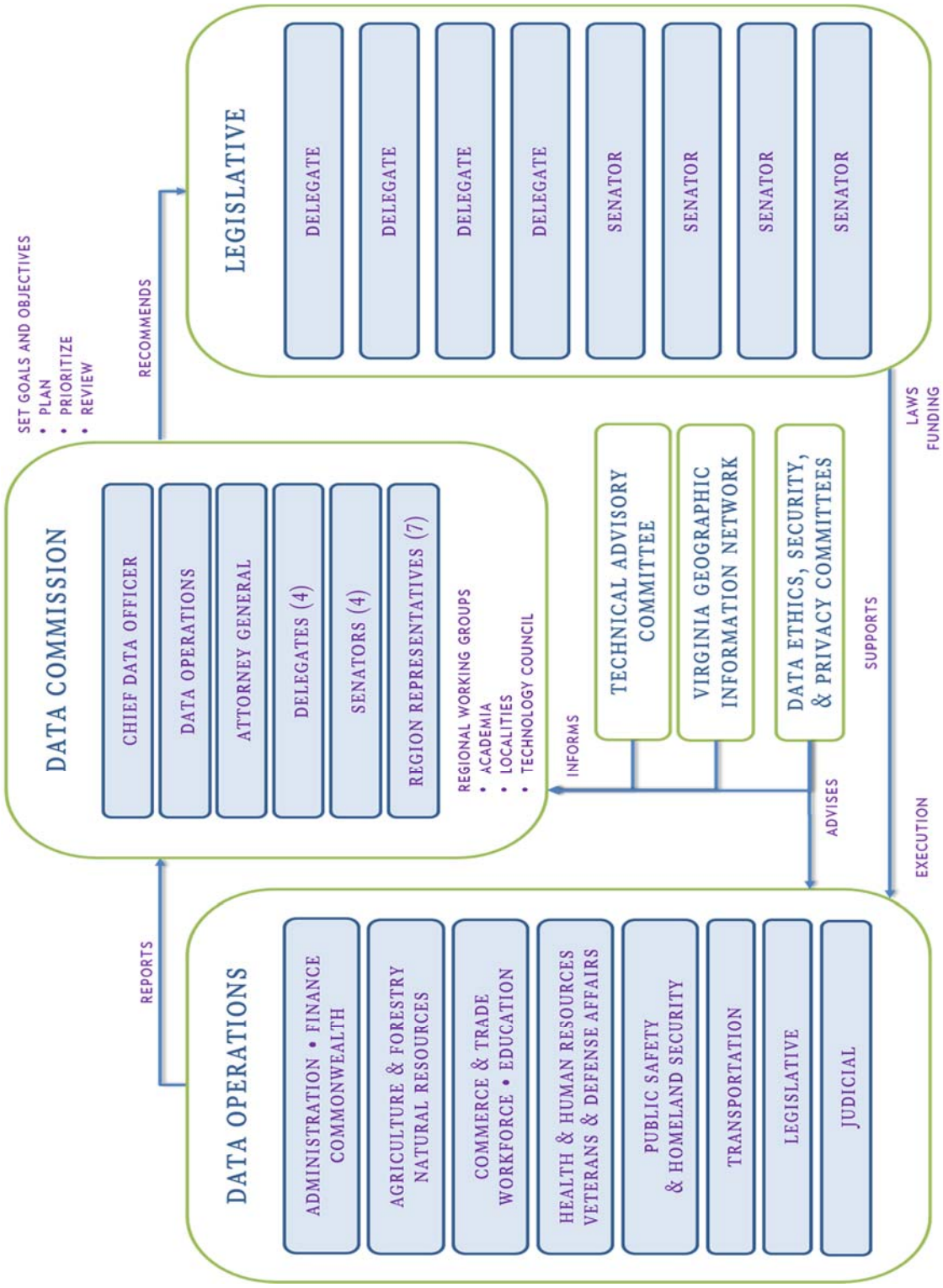
Governor's Data Internship Program (GDIP):

http://www.govtech.com/data/Virginia-Launches-Open-Data-Open-Jobs-Initiative.html

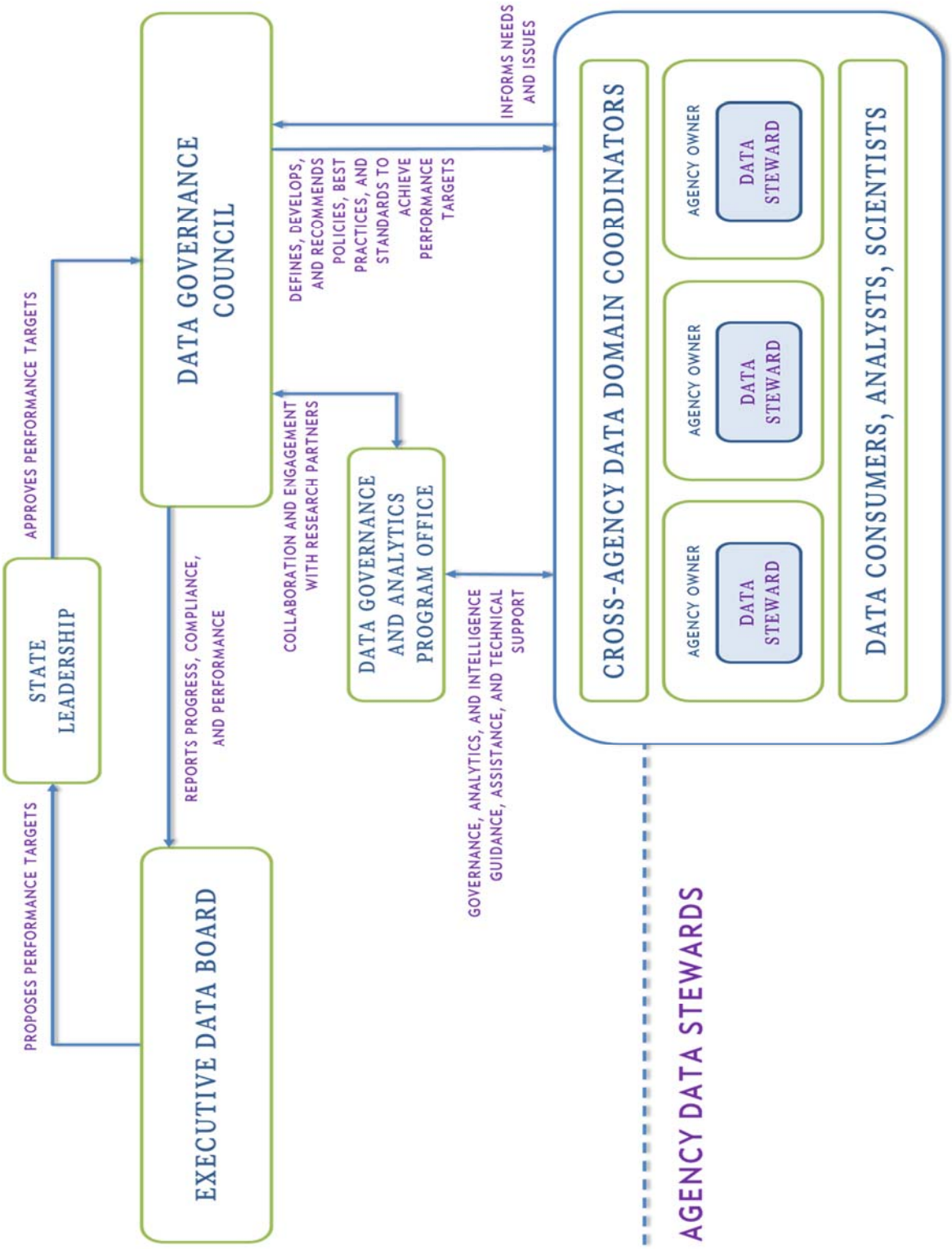
Commonwealth Data Internship Program (CDIP):

vip.virginia.gov/services/cdip

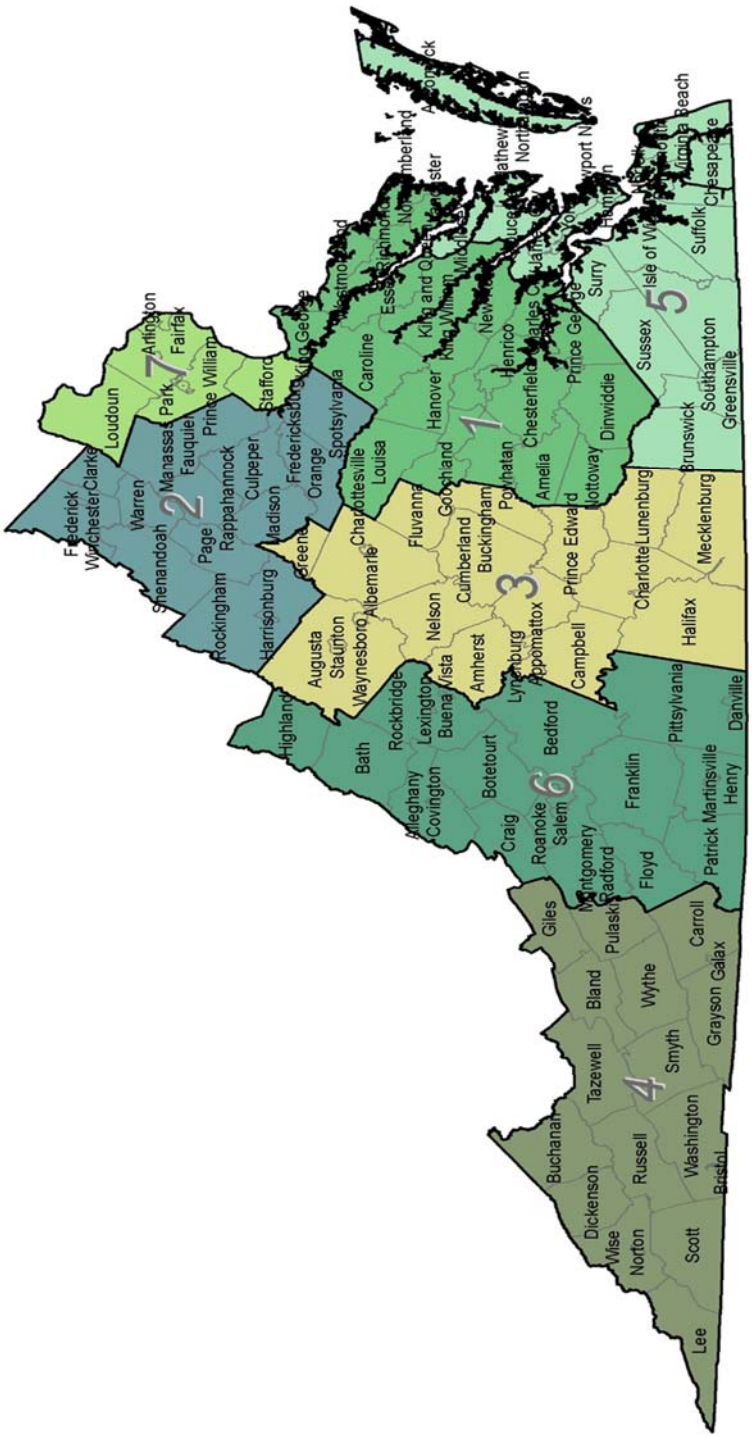
Appendix 2. Commonwealth of Virginia Data Commission



Appendix 3. Governance Model for Data Operations



Appendix 4. Data Commission Regions



Appendix 5. Core Components of Trust Frameworks

Business Components

- Limitations on Use of Data: Collection, maintenance, and use of a sensitive information solely for the purpose for which it was collected.
- Governing Body & Change Processes: Governance model for the trust framework built on a transparent, clearly defined structure and change-management process.
- Operating Policies & Procedures: Policies and procedures for the operations, maintenance, and business continuity of the trust framework's operational authority.
- Security, Privacy & Confidentiality (Business): Compliant business processes and documentation for notifying a member party of the security, privacy, and confidentiality provisions in the trust framework and for gaining consent from the member party for using information.
- Suspension & Termination (Voluntary & Involuntary): Provisions for suspending or terminating a member party due to failure to meet the obligations in the agreement, or the member party's self-suspension or termination of participation in the identity trust framework.
- Data Elements & Data Classification: Attribute-level documentation, classification, and labeling of the sensitive information shared among member parties of the trust framework to support compliant handling of the data through the entire data lifecycle.
- Expectations of Performance: Provisions in the trust framework that set the performance and service criteria for all member parties including requirements for breach response and resolution, system(s) interruption or failure, and other risk situations.
- Use Cases (Exchange & Member Types): Documented examples for roles and responsibilities of member parties of the trust framework.

Legal Components

- Definition/Identification of Applicable Law: Provisions requiring member parties of the trust framework to comply with all governing laws, statutes, rules, and regulations of the jurisdiction in which each member operates.
- Legal Agreements for Exchange Structure: Statement of requirements for the architecture, performance, and service specifications, and member obligations for the operation and maintenance of the exchange of sensitive information within the trust framework.
- Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing member party obligations for the collection, labeling, operational use, and maintenance of sensitive information and for gaining consent from the member party for using information.
- Assignment of Liability & Risk for Member parties: Articles that define how liability and risk within the trust framework will be distributed among member parties.
- Representations & Warranties: Statements of factual principles in the trust framework upon which member parties may rely.

- Authorizations for Data Requests by Member parties: Articles defining role-based rules, requirements, and processes for member parties of the trust framework to access sensitive information.
- Open Disclosure & Anti-Circumvention: Provisions requiring transparency in the rules, policies, and practices for operations and governance of the trust framework, and prohibiting the circumvention of technical protections within the information sharing environment for the handling of sensitive information.
- Confidential Sensitive information: Statements documenting the business, legal and technical requirements for the classification, labeling and handling of confidential sensitive information.
- Audit, Accountability & Compliance: Terms of conditions highlighting best practices, findings, and corrective action plan to address deficiencies.

Technical Components

- Performance & Service Specifications: Architecture and infrastructure specifications, protocols, and requirements for all member parties covering full end-to-end integration for the information sharing environment supported by the trust framework, including technical, solutions, and information architecture.
- Security, Privacy & Confidentiality: Architecture and infrastructure specifications, protocols, and requirements within the information sharing environment supported by the trust framework designed for the collection, labeling, operational use, and maintenance of sensitive information and for gaining consent from the person for using information.
- Breach Notification: Processes, protocols, and requirements compliant with applicable law for notifying the appropriate authorities in the event of a breach of sensitive information, and related risk situations, within the trust framework.
- System Access: Standards-based, open architecture processes, protocols, and requirements for member authentication into the information sharing environment supported by the trust framework.
- Provisions for Future Use of Data: Terms and conditions defining limitations on, and permitted purposes for, the use of sensitive information after the information has been used for the designated purpose.
- Duty of Response by Member parties: Terms and conditions requiring trust framework member party systems to respond to and process messaging requests – inbound and outbound – within the information sharing environment, normally establishing the time in which the member system must respond and process the request.
- Onboarding, Testing & Certification Requirements: Documented processes, protocols, specifications, and requirements for onboarding, testing, and certifying prospective member party systems in the information sharing environment.
- Handling of Test Data v. Production Data: Terms and conditions compliant with applicable law preventing the use of production data in a test environment.

- Compliance with Governing Standards: Terms and conditions identifying and stating requirements for member party compliance with governing external standards for the trust framework.

Appendix 6. Indiana Management Performance Hub

The Director of Indiana's Management Performance Hub is considered the Chief Data Officer for the state and reports to the Director of the Office of Management and Budget. The organization consists of 26 staff members supporting Communications, Data Engineering, Infrastructure, Project Management, Engagement and Analytics, Data Science, Business Intelligence, and Data Privacy.

- Advise executive state agencies and political subdivisions regarding state best practices concerning the creation and maintenance of data
- Coordinate data analytics and transparency master planning for the executive state agencies and provide leadership regarding state data analytics and transparency
- Collect, analyze, and exchange government information
- Ensure the security of government information
- Conduct operational and procedural audits of executive branch agencies

Budget

General Funds Appropriation: $8.3M

Direct Agency Support (Agency funds provided to support agency-specific projects): $0

Agency Charge-back (cost recovery): $0

Grants: ~$2M (includes federal matching funds)

Organizational Structure (numbers in parentheses are multiple positions)

- Chief Data Officer
    - Executive Assistant
    - Communications Director
        - Digital Communications
    - Chief of Staff
        - Assistant Chief of Staff
        - Technology Director
            - Data Architect (2)
            - Technical Project Manager
                - Data Engineer (3)
                - Data Management
            - Database Administrator and Architect
            - Application Database Administrator
            - Application Administrator (2)
            - Linux/Hadoop Administrator (2)
        - Engagement and Analytics Director

- Program Manager (2)
- Technical Project Manager
- Engagement and Analytics (4)
    - Tableau Developer (3)

- Data Scientist (2)

- Chief Privacy Officer
    - Information Security Analyst

Appendix 7. NC Government Data Analytics Center

The Director of the Government Data Analytics Center is recognized as the Chief Data Officer for the state of North Carolina and reports to the Chief Information Officer. The center has approximately 30 positions and utilizes public-private partnerships as part of a statewide data integration and data sharing initiative. The center is responsible for the following:

- Identify data integration and business intelligence opportunities that will generate greater efficiencies in state agencies, departments, and institutions
- Leverage data from transactional systems for enterprise-level state business intelligence
- Compare capabilities and costs across state agencies
- Ensure data integration and sharing is performed in a manner that preserves data privacy and security in transferring, storing, and accessing data

Budget

General Funds Appropriation: ~$30M

Direct Agency Support (Agency funds provided to support agency-specific projects): ~$10M

Agency Charge-back (cost recovery): ~0.6M

Grants: ~$30M

Organizational Structure (numbers in parentheses are multiple positions)

- Chief Data Officer
    - Executive Assistant (2)
    - IT Director – CGIA
        - IT Project Manager
        - IT Business Relationship Specialist
        - Database Analyst
        - Application Systems Analyst
    - IT Director – Enterprise Data Management
        - Data Architect (2)
    - IT Director – Health Information Exchange
        - IT Project Manager (2)
        - Application Systems Manager
        - Applications Systems Specialist (5)
        - Information and Communications Specialist
        - Business Officer
        - Business Relationship Specialist (2)
    - IT Director – Data Solutions

        - Applications Systems Manager (3)
        - Applications Systems Analyst (2)
        - Applications Systems Specialist
        - IT Architect
    - IT Business Systems Manager – Data Production
        - User Support Technician (5)
        - User Support Specialist
        - Business Systems Analyst (2)
    - Information and Communications Specialist
        - Technical Writer (2)
        - Education and Training (3)