Florida Cybersecurity Task Force
Meeting Scope: Data Management
Date & Time:
August 19, 2020
2:00 PM – 4:00 PM EST

I. Call to Order

II. Roll Call

III. Opening Business

IV. Approval of June 30, 2020 Meeting Minutes

V. Presentation: Florida Digital Service Data Initiatives
   Matt McCarville, DBA, Chief Data Officer, Florida Digital Service

VI. Presentation: CJIS
    Major Tim Roufa, Florida Highway Patrol

VII. Presentation: HIPPA and HHS Best Practices
     Jason Raymond, Vice President and Chief Information Security Officer, GuideWell

VIII. Group Discussion

IX. Public Comment

X. Executive Session

XI. Adjournment
I. Call to Order

Lieutenant Governor Jeanette Nuñez (Chair) calls the meeting to order and asks Cody Farrill to conduct a roll call.

II. Roll Call

Cody Farrill conducts a roll call and the Chair confirms that there is a quorum of the Task Force.

III. Opening Business

The Chair thanks everyone on the call for being able to join and asks for a motion to approve the minutes from the January 17th Task Force meeting. The motion is made by Inspector General Melinda Miguel and is seconded by Task Force member Byron Shinn. The motion is approved.

The Chair expresses gratitude to Division of Emergency Management Director Jared Moskowitz for his work the past few months and ties in the importance of technology during these times.

The Chair outlines the meeting agenda including a legislative session update and overview of the Task Force timeline moving forward by Cody Farrill, followed by group discussion, and public testimony. The Chair mentions that following public testimony, the Task Force will be convening for an executive session meeting.

IV. Presentation: Legislative Session Updates & Task Force Timeline

Cody Farrill thanks the Lieutenant Governor and provides a presentation including updates from the 2020 Florida Legislative Session. Cody goes on to outline four pieces of legislation that were passed during legislative session (HB 1391, HB 821, HB 5001, & HB 5003) that are either directly or indirectly related to the advancement of technology within state government. Before moving into a discussion on the Task Force Timeline, Cody asks participants if there are any questions. Seeing no questions...

Cody then provides an overview of the Task Force Timeline moving forward. Cody announces that three Department of Management Services’ staff have been identified to support the Task Force workgroups as subject matter experts. Meetings will continue through January with a final report expected in February. Workgroup meetings will occur in-between Task Force meetings. Cody then turns the meeting back to the Chair.
V. Group Discussion

The Chair opens the floor for discussion amongst members of the Task Force or to see if there are any questions about the Task Force Timeline. Seeing no questions, the Chair moves into Public Testimony.

VI. Public Testimony

The Chair opens the floor for any public comment for those on the phone. No members of the public speak, so the Chair requests a motion to move into executive session. Task Force member Byron Shinn makes the motion and is seconded.

VII. Adjournment

The Chair announces the Task Force will now convene for an executive session. The public conference line ends.
CHIEF DATA OFFICER

CYBERSECURITY TASK FORCE UPDATE
HHS Data Interoperability Workgroup

• On November 11, 2019, Governor Ron DeSantis directed the Agency for Healthcare Administration, the Department of Children and Families, the Department of Health, the Department of Education and the Department of Management Services to assemble a new interagency working group.

• When first established, workgroup members were asked to consider the following goals:
  • Ensuring that new IT systems can be integrated and compatible across multiple agencies and departments.
  • Identifying vendors to develop systems across multiple agencies and departments.
  • Developing modular systems that can be shared by agencies and departments.
  • Identifying cost-savings by avoiding duplicative and/ or redundant efforts being made to this end by agencies and departments.
  • Developing a proof of concept for interoperability that can be replicated across all agencies and determining other practices and systems that would achieve greater interagency collaboration and data gathering.
To accomplish these goals, the Division of State Technology has established four subgroups:

- **Roadmap & Strategy Subgroup**
  - The Roadmap and Strategy subgroup is responsible for outlining the overall roadmap and direction for achieving an interoperable environment.

- **Data Sharing Subgroup**
  - The Data Sharing Subgroup is responsible for identifying all existing data sharing agreements between interagency members, and subsequently developing a process, tool(s) and/or template to improve and standardize agreements for sharing data between agencies. This will reduce the time needed when completing data sharing for future needs.
HHS Data Interoperability Workgroup

• Data Quality Subgroup
  • The Data Quality Subgroup is responsible for identifying both current and future use cases that may require a data sharing agreement between agencies. Additionally, the Subgroup will also develop standards for data quality through common definitions and access and availability protocols.

• Technology Subgroup
  • The Technology Subgroup is responsible for identifying and standardizing the technology needed to ensure systems can be interoperable. The subgroup will also create an inventory of technology that is currently being used by state agencies for the purpose of data collection, exchange, and visualization. Additionally, the Subgroup will identify possible technologies that may assist in interoperability efforts.
Recent Updates in Data

• HHS Data Interoperability Groups
  • Enterprise Memorandum and Agreement Collection (MAC)
  • Technical Group-HHS Constituent ‘Universal Eligibility’ routing page:
    • SNAP/TANF
    • Reemployment Assistance

• Release several CIO surveys:
  • Survey Sent to CIOs on April 27th to Capture a Baseline-now includes 23 agencies
    • Implemented a Dashboard for Survey Results
  • Data Governance Survey
  • Data Maturity Survey is in development that includes questions on:
    • SSO, AD, IAM, MFA, as well as HIPAA, PCI-DSS, and CJIS
Recent Updates in Data

- Enterprise Data Catalog (EDC)
  - In Proof of Concept (POC) with multiple vendors.
  - In line to hit 10/1/2021 EDC implementation

- Brought in other scalable IT solutions/platforms for agency adoption:
  - Analytics Processing Automation
  - Robotic Processing Automation
  - Self-Service Artificial Intelligence (AI)

- HB 1391 requires the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services to adopt standards that allow for open data interoperability.
Questions?
OVERVIEW
At the direction of Governor Ron DeSantis, the Florida Department of Management Services continues to work with Health and Human Services agencies to explore opportunities to increase interoperability between agencies and explore synergies for multi-agency IT systems redesign.

To accomplish this directive, the Division of State Technology has established four subgroups:
- Roadmap and Strategy
- Data Sharing
- Data Quality
- Technology

An overview of each workgroup is provided below. When combined, these efforts are expected to produce more streamlined cost-effective operations such as standard processes for data sharing agreements, technical models for data sharing, and processes for governing the quality of the collected and shared data.

ROADMAP & STRATEGY SUBGROUP
The Roadmap and Strategy subgroup is responsible for outlining the overall roadmap and direction for achieving an interoperable environment. A list of the team members and projected timeline is included below:

Team
- Julie Madden, CIO, Department of Children and Families (Lead)
- Scott Ward, CIO, Agency for Healthcare Administration (Lead)
- Joe Wright, Department of Children and Families
- Bob Ward, CIO, Department of Management Services
- Mike Magnuson, FX Project Director, Agency for Healthcare Administration
- Shandra McGlohon, CIO, Department of Elder Affairs
- Tom Herring, Department of Health
- Dennis Hollingsworth, Department of Juvenile Justice

Timeline
1. By June 30, 2020, each participating agency shall:
   a. Produce an inventory of existing data sharing agreements
   b. Provide an inventory of business intelligence/visualization tools, including count of licenses.
2. By January 2021, each participating agency shall:
   a. Complete a draft of a Master Data Sharing Agreement
   b. Complete draft of a Universal Consent Form
   c. Begin working with General Counsels to gain approval for Master Data Sharing Agreement and a Universal Consent Form
   d. Be ready to present draft master data sharing agreement and universal consent form to stakeholders in the Legislature and Governor’s office.
3. By April 2021, each participating agency shall:
   a. Produce a proof of concept, to include interactively displaying data sourced in real-time from multiple agencies to show a “360 degree” view of a customer of services provided by the agencies.
4. By April 2022, each participating agency shall:
   a. Identify tools that can be negotiated for as the enterprise standard and develop procurement vehicles allowing for most cost-effective contracts available to all agencies.
DATA SHARING SUBGROUP
The Data Sharing Subgroup is responsible for identifying all existing data sharing agreements between interagency members, and subsequently developing a process, tool(s) and/or template to improve and standardize agreements for sharing data between agencies. This will reduce the time needed when completing data sharing for future needs.

The subgroup is currently working to scale a process and online resource initially developed by the Department of Children and Families into an enterprise solution. By piloting with HHS agencies, the solution is expected to be expanded to all state agencies to assist in the development and management of data sharing agreements.

Team
- Drew Richardson, Interim Deputy State CIO, Department of Management Services (Lead)
- Shandra McGlohon, Department of Elder Affairs
- Shaun French, Agency for Healthcare Administration
- Emily Roach, Department of Education
- Chris Veal, Department of Health
- Jackie Suttle, Department of Juvenile Justice
- Brooke Powell, Department of Children and Families

DATA QUALITY SUBGROUP
The Data Quality Subgroup is responsible for identifying both current and future use cases that may require a data sharing agreement between agencies. Additionally, the Subgroup will also develop standards for data quality through common definitions and access and availability protocols.

Team
- Sriram “Sir” Kommu, CIO, Agency for Persons with Disabilities (Lead)
- Shandra McGlohon, CIO, Department of Elder Affairs
- Erica Wilson, Agency for Healthcare Administration
- Emily Roach, Department of Education
- Allison Culpeper, Department of Health
- Jackie Suttle, Department of Juvenile Justice
- Brooke Powell, Department of Children and Families

TECHNOLOGY SUBGROUP
This Technology Subgroup is responsible for identifying and standardizing the technology needed to ensure systems can be interoperable. The subgroup will also create an inventory of technology that is currently being used by state agencies for the purpose of data collection, exchange, and visualization. Additionally, the Subgroup will identify possible technologies that may assist in interoperability efforts.

Team
- Paul Chafin, Interim CIO, Department of Health (Lead)
- Shandra McGlohon, Department of Elder Affairs
- Michael Tatum, Agency for Healthcare Administration
- Bryan Hudnall, Department of Education
- Sean Miller, Department of Health
- Geoff Fulcher, Department of Juvenile Justice
- Cole Sousa, Department of Children and Families
November 11, 2019

Secretary Mary Mayhew, Agency for Health Care Administration
Secretary Chad Poppell, Department of Children and Families
Surgeon General Scott Rivkees, Department of Health
Commissioner Richard Corcoran, Department of Education
Secretary Jonathan Satter, Department of Management Services

Dear Agency Heads:

Innovative technologies in the health and human services sector are continuing to emerge. New information systems and strategic data governance are transforming how healthcare services are delivered both in the private sector, and in government. Integrating our information technology (IT) systems across our state’s health and human services agencies will be an important step towards improving the way we operate and serve the public.

As we begin to develop blueprints for future systems, your agencies have a unique opportunity to work together and reimagine interagency cooperation in the administration health and human services. The design of future IT systems must emphasize collaboration to ultimately improve efficiency and deliver positive outcomes for Floridians across a multitude of services.

To this end, I am directing the Agency for Healthcare Administration, the Department of Children and Families, the Department of Health, the Department of Education and the Department of Management Services to assemble a new interagency working group to explore opportunities for collaboration for a multi-agency IT systems redesign.

When established, working group members shall consider the following goals:

- Ensuring that new IT systems can be integrated and compatible across multiple agencies and departments.
- Identifying vendors to develop systems across multiple agencies and departments.
- Developing modular systems that can be shared by agencies and departments.
• Identifying cost-savings by avoiding duplicative and/or redundant efforts being made to this end by agencies and departments.
• Developing a proof of concept for interoperability that can be replicated across all agencies and determining other practices and systems that would achieve greater interagency collaboration and data gathering.

This working group will help guide project development, and will be a critical driver of success in interagency IT integration. By identifying efficiencies and synergies, we can create a system that enables improved communication and coordination. Thank you for your diligence in working toward this goal.

Sincerely,

[Signature]

Ron DeSantis
Governor
CJIS Partnerships

Data Center Security Considerations
Major Tim Roufa, Florida Highway Patrol
## Terms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CJIS</td>
<td>Criminal Justice Information Systems</td>
</tr>
<tr>
<td>CJA</td>
<td>Criminal Justice Agency – (court, governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice)</td>
</tr>
<tr>
<td>NCJA</td>
<td>Agencies and non-governmental entities or subunits thereof that provide services primarily for purposes other than the administration of criminal justice. For CJIS purposes must operate under supervision of a CJA.</td>
</tr>
<tr>
<td>PII</td>
<td>Personally identifiable information (name, date of birth, social security information or biometric records alone or when combined with other personal or identifying information which is linked or linkable to a specific individual)</td>
</tr>
<tr>
<td>FCIC</td>
<td>Florida Crime Information Center</td>
</tr>
<tr>
<td>FALCON</td>
<td>Florida’s Integrated Criminal History System – mechanism for retaining fingerprints under agency ORIs and creating watchlists for rap backs</td>
</tr>
<tr>
<td>Rap Back</td>
<td>Notification when an individual whose prints are retained has been arrested</td>
</tr>
<tr>
<td>ORI</td>
<td>Originating Agency Identifier – used to track requests and transmission of CJI through CJI Systems</td>
</tr>
<tr>
<td>CJI</td>
<td>Criminal Justice Information, often referred to as CJIS data</td>
</tr>
<tr>
<td>MCA</td>
<td>Management Control Agreement enabling CJA to supervise NCJA</td>
</tr>
</tbody>
</table>
Computing systems that access FBI CJIS services and/or store or process data derived from those services

- Florida agencies access CJIS services through FDLE’s CJNet
- CJIS Systems include data derived from the National Law Enforcement Telecommunications System (NLETS)

In Florida, CJI means the information or data obtained from any FDLE CJIS system

- Florida Crime Information Center (FCIC)
- Biometric Identification System
- Falcon
- Computerized Criminal History

Source of the information determines whether CJIS Security Policy applies

- Data contained within CJI may be available from other sources, in which case it would not be CJI
- PII is not automatically CJI
- Driver data is not CJI unless it is obtained through FCIC/NELTS
- Florida has determined police videos do not constitute CJI
CJIS Certification vs Compliance

**No Such Thing as CJIS Certified Data Center**

- There is no blanket certification for CJIS solutions
- Certification refers to individual's ability to access, not provider’s approval to provide services
- Individual CJAs must determine CJIS compliance in consultation with FDLE
- CJIS-compliant solutions must still be reviewed prior to implementation to ensure agency compliance since network infrastructure and interfaces may be different from agency to agency

Lead CJIS Agency Concept Mitigates Redundancies

- Allows a CJA to take on role of ensuring compliance
- Reduces workload for providers and criminal justice partners
FHP Lead CJIS Agency Overview

- State Computer-Aided Dispatch and Mobile Forms Contract
- State Law Enforcement Dispatch Operations
- State Law Enforcement Radio System Security Management
- State Data Center Lead CJA
- DSM Winter Haven Lead CJA
- NWRDC Lead CJA
FHP Lead CJA Responsibilities

- Interagency Agreements and Management Control Agreements
- Physical Security Confirmation
- Personnel Screening
- Arrange CJIS CJIS security Awareness Training for NCJA Partners
- Consultations with Data Center partners
- FDLE and FBI Compliance Audits
## CJIS Compliance Requirements

### Physically Secured Location

- Perimeter prominently marked
- Facility maintains a list of authorized personnel for access
- Physical access points controlled by facility
- All personnel verified prior to gaining entry
- Transmission lines protected to prevent unauthorized access
- Screens with access to CJI/CJI systems positioned to prevent viewing
- Physical access monitored to detect and respond to physical security incidents
- Visitors authenticated before access is provided
- All visitors are always escorted
- Entity authorizes and controls hardware containing CJI from leaving the secured area

### Escorted access

Escorted access means escort is present for duration of access (hip to hip)

### For open floor facilities

For open floor facilities, individual CJIS systems must be locked in a cage or cabinet

- Keys must be unique to cage
- Only CJIS certified individuals may have access to keys

---

A physically secure location is a facility - or an area, room, or group of rooms within a facility - with both the physical and personnel security controls sufficient to protect CJI and associated information systems.
CJIS Access Requirements

Access only granted to people:

- Employed by or contracting with a criminal justice agency; or
- Employed by or contracting with a non-criminal justice agency which is supervised by a criminal justice agency (such as a shared resource center under a management control agreement).

Escorted vs Unescorted

- Screening and access requirements apply to individuals who will have unescorted access
- Personnel who have not met screening requirements may have access to secure areas if escorted at all times.
- Personnel who have not met requirements may NOT have physical (i.e. printouts) or logical access to CJI

National Fingerprint-Based Background Check

- Background check MUST be fingerprint based
- Eliminates potential for false names
- Name-based searches may miss past aliases
- Fingerprint checks allow CJA to retain prints in FALCON and receive rap backs
- CJIS level fingerprint screening reserved for CJAs and entities supporting CJAs through MCA s

CJIS Security Awareness Training

- Training varies by access level (i.e. IT staff, users, maintenance and cleaning staff, etc.)
- Training provided online and required periodically
- FBI Security Addendum required to be signed by each individual employed by nongovernmental NCJA who will have access
Personnel Screening

Prints sent to FDLE and FBI

Fingerprints taken at electronic terminal or submitted via hard card

Prints Compared to state and national criminal history databases

Criminal history reviewed by CJA for approval or denial

Results available to CJA online via FALCON

CJA receives notification if employee or contractor is arrested

CJIS Screening Includes Juvenile and Expunged Records
CJIS Access Denial Reasons

**ACCESS DENIED**

- **Felony conviction, regardless of time passed since conviction**
- **Pending felony charge which has not yet been disposed of in court**
- **Pending misdemeanor charge which has not yet been disposed of in court**
- **Misdemeanor conviction or adjudication withheld and has not completed court sanctions**
- **Active warrant or fugitive from justice**
- **Multiple arrests, regardless of court disposition or sentencing provisions, when records indicate access would not be in the public interest**
Some Technical Considerations for CJIS Solutions

Even when working with a lead CJA, technical solutions will need to be vetted and verified on an individual user basis.

**Encryption in transit**
- Required if CJI transmitted outside boundary of the physically secure location
- Must be FIPS 140-2 certified, minimum 128 bit strength

**Encryption at rest**
- Required when CJI is stored outside boundary of physically secured location
- Must be FIPS 197 certified, minimum 256 bit strength

**Cloud solutions**
- Storage of CJI only be permitted in environments which reside within the physical boundaries of the U.S., U.S. territories, Indian Tribes, and Canada
- Metadata derived from unencrypted CJI shall be protected in the same manner as CJI
- Cloud assessment available at FBI CJIS Security Policy Resource Center

**Partitioning**
- User functions must be separate from information system management functions
- Can be accomplished using different computers; different CPUs; different instances of OS; different network addresses

**Virtualization**
- Virtualization is allowed, however host must be isolated from VM
- If CJI is commingled with non-CJI, CJI must be encrypted when stored and network traffic within the virtual environment must be encrypted.
- Best practice to firewall each VM within the virtual environment
CJIS Systems Access and Data Security

Personnel Screening

Physical Security

Logical Security

Questions?
DATA BREACH IMPACTS AT A GLANCE

A data breach is defined as an event in which an individual’s name and a medical record and/or a financial record or debit card is potentially put at risk, either in electronic or paper format.

United States Data Breaches (IBM/Ponemon, 2019)

• Average Cost of a Data Breach : $8.19M
• Cost per record (all industries): $219 per record
• Cost per record (HealthCare): $429 per record
• Average Number of Records Stolen per Breach: 32,434
• Data Breach Lifecycle (time to identify and contain) (U.S.): 235 Days
  – Mean Time to Identify a Breach: 196 Days
  – Mean Time to Contain a Breach: 49 Days
• Breach Causes: 51% Malicious Attacks, 25% System Glitch, 24% Human Error
DATA BREACH COST BY INDUSTRY

Average total cost of a data breach by industry
Measured in US$ millions

Health: $6.45
Financial: $5.86
Energy: $5.60
Industrial: $5.20
Pharma: $5.20
Technology: $5.05
Education: $4.77
Services: $4.62
Entertainment: $4.32
Transportation: $3.77
Communication: $3.45
Consumer: $2.59
Media: $2.24
Hospitality: $1.99
Retail: $1.84
Research: $1.65
Public: $1.29
THE CHALLENGES OF EVOLVING HEALTHCARE DATA ECO-SYSTEMS

- Velocity
- Complexity
- Consumer Expectations
INFORMATION VELOCITY

• Healthcare data is diverse, moving at increasing velocity, and evolving.

• Faster data throughout the information lifecycle empowers better outcomes.

• The secure, trusted delivery of meaningful, data-driven healthcare experiences.

• Transforms how Information Security is engaged
COMPLEXITY OF THE DATA

• The information fabric of healthcare systems varies in complexity

• Information Security and Data Governance must understand the use of data, and understanding what makes up the information supply-chain

• Third-party integrations, Cloud-hosted partnerships, and Cloud enabled infrastructure are key parts of the information supply-chain.

• Data systems, tools, and platforms are continuing to evolve at a faster rate.
CONSUMER EXPECTATIONS

• Innovative and disruptive health technologies for consumers, patients, and care givers are changing how we think about healthcare delivery.
• Digital Experience is the priority (personal experience and ease of use)
• Better, Faster Data = Better Health Outcomes
UNDERSTANDING DATA CLASSIFICATION AND DATA GOVERNANCE

• Classifications are business definitions driven by business processes and needs
• Governance is the practice of oversight and enablement of data solutions
• Classifications should include definitions about the structures (columns) and the values
• Metadata is the “stuff about the stuff”
• Meaningful, actionable, and correct Metadata is the key enabling classifications
• Data is an asset.
• Metadata enabled classifications are the building blocks for Information Security program Technical Controls
• Classifications are also critical for the enablement of Administrative Controls, Audit readiness, and security framework adoption
• Data Classification and Data Governance programs should be owned by business stakeholders (data owners) and enabled through technology practices (custodians).
EMPOWERING BUSINESS DATA OWNERS AND DATA GOVERNANCE

• The data owners have an understanding of how and where the data for which they are accountable is used and to whom access has been granted
• The data owners approval process is optimized for ease of use for the owners as well as the requestors
• A data owner may have several data stewards with oversight responsibility for various scopes of a data owner’s accountable domain or subject area
• IT resources are committed to informing, enabling, and partnering with data owners and data stewards
• Data Classification stakeholders for organizational effectiveness includes a broad range of business, IT, and Legal teams.
• The users are your most important stakeholder
SECURE ENABLEMENT IS MORE THAN ENCRYPTION

• The Confidentiality, Integrity, and Availability Triad is fundamental to the design and enablement of data solutions
• Data Classification and Classification Enabled Records Retention enables visibility and reduces the volume risk
• Vulnerability scanning can identify database vulnerability exposures and misconfigurations
• Data loss prevention based on data classifications integrated with email, web proxy servers, and end-point devices enables visibility and controls data egress
• Cloud Access Security Broker (CASB) and Cloud-based data management tools help enable a secure cloud perimeter
TECHNICAL CONTROLS AS ENABLING TOOLS

• Technical controls safeguard the data at rest, in use, and in transit
• The access controls are managed through a streamlined process, role-based, and aligned to the principles of minimum necessary (least privilege) access and need-to-know
• Technical controls include technologies and processes for protecting hosts, networks, storage, and endpoints
• Cloud-based technical controls can have complexities and opportunities.
• Technical controls require investment in tools, maintenance, staff, and infrastructure
• Controls Assurance is key to validate protective capabilities and provide Audit Readiness
TYING IT ALL TOGETHER

- Data Governance and classification process allow us to navigate a disruptive technology landscape while securely enabling the use of healthcare data.
- Understand the value of the information
- The value of information is the determining factor for the complexity of capabilities and solutions that address privacy vulnerabilities.