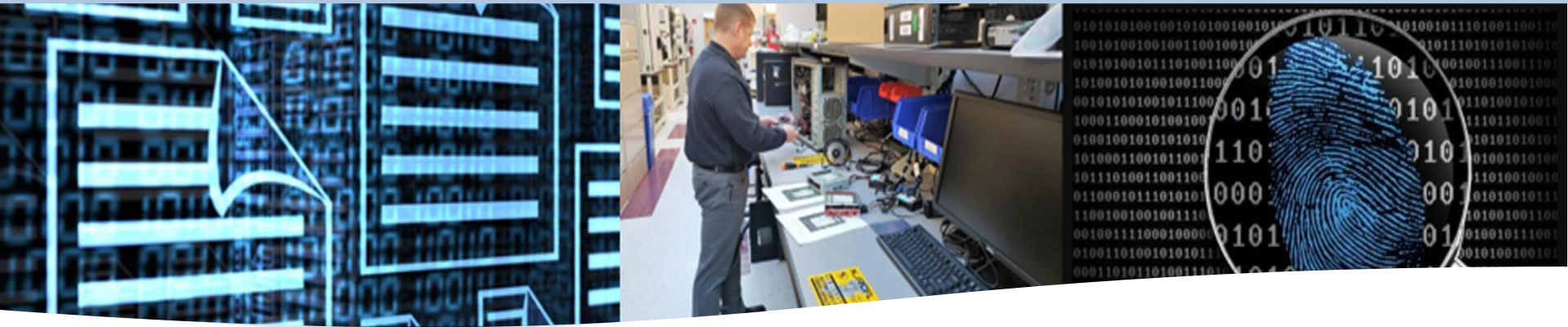




State of Connecticut
Criminal Justice Information System (CJIS-CT)

Digital Evidence Storage Management Study Steering Committee Meeting

April 11, 2024



CJIS-CT Contacts

Sean Bucher
CJIS-CT Sr Project Manager
Sean.Bucher@ct.gov

Evan Martucci
CJIS-CT Business Analyst/Technical Writer
Evan.Martucci@ct.gov

Maureen Klinkert
CJIS-CT Project Coordinator
Maureen.Klinkert@ct.gov

Tamika Potts
CJIS-CT Communications
Tamika.Potts@ct.gov



Agenda

April Steering Committee

- Study Purpose Summary
- Open Discussion Time
- Milestones and Progress (focus on items completed since last meeting)
 - Chain of Custody Stack (tiers)
 - As-Is Current State Use Cases (Scenarios)
 - Forensics and the Regional Centers for Digital Investigation (Regional CDIs)
 - Interview Schedule
 - Newest Interview Results
 - AG's Office Collaboration
 - Current State As-Is Study Document
- Upcoming Milestones
- Conclusion and Next Steps



Study Purpose Summary

The Study Should Determine:

- ✓ • Boundaries of the Opportunity Space, Interface Requirements to other systems (e.g. DCJ, Judicial, PDs)
- ✓ • Cost of Equipment and Licensing to LEAs, Cost of Labor and Administration to LEAs
- ✓ • GAP of smaller PDs to the most capable PDs
- ✓ • CISS can be used to perform Chain-Of-Custody of Digital Evidence as part of the Electronic Workflow of Arrest Documents
- ✓ • CJIS-CT can provide value in hosting centralized contracts and DEMS Software
- ✓ • CISS can be leveraged as a cost-effective centralized storage for Bulk Media
- ✓ • Regional Municipal Digital Evidence Software Collaboration Centers (Regional CDI)
- **The Study should conclude 4 – 6 potential solutions covering the SUCCESS FACTORS**



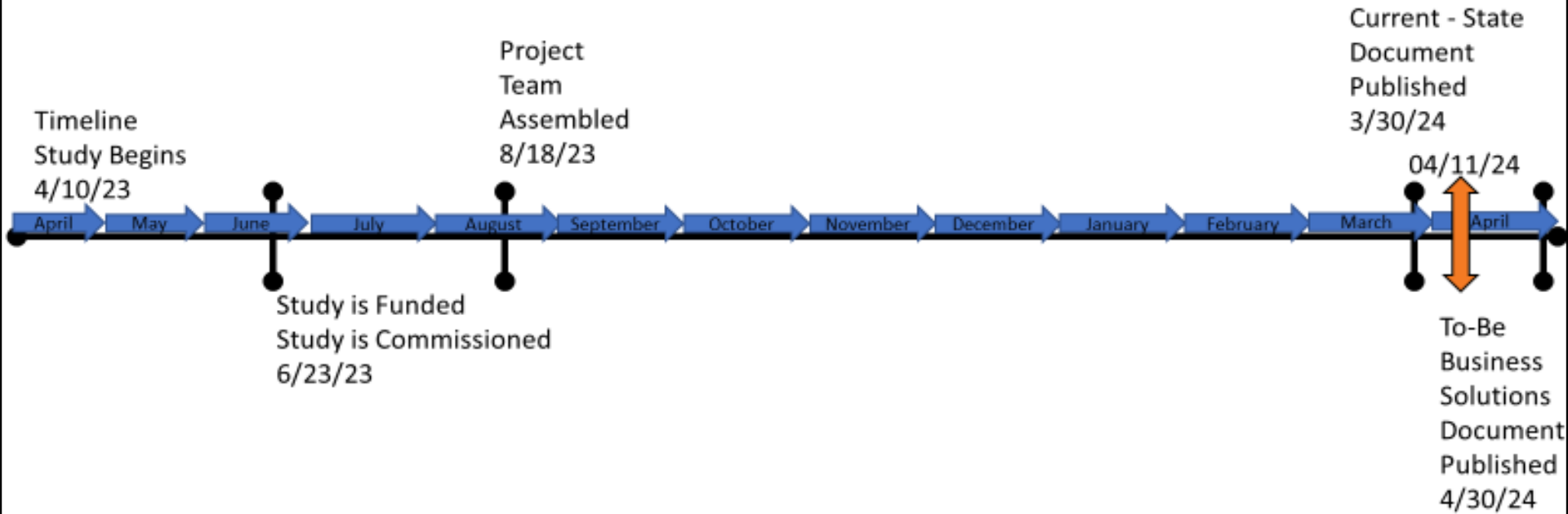
Open Discussion with Steering Committee

- **Current State Document**
- **Looking for Stakeholder Feedback on Draft**
 1. Create a separate Current State Document –DRAFT, Publish for Stakeholder Review
 - Example - MTG Model – As-Is Business Model
 - Put all of the detailed Interview Notes, Internet Research, Meeting Presentations, etc. in the Appendices as part of the published report
- **Next**
 2. Create separate Requirements/Gap/To-Be Potential Solutions Document
 - To-Be Business Solutions Document
 - Example – MTG Model – Technical Requirements, GAP Analysis, To-Be Business Model
 3. Create a separate Executive Summary Report



Study Timeline

Bulk Media and Digital Evidence Study



The Study Project Plan and Timeline:

- Current State Document by 3/30/24
- To-Be Business Solutions by 4/30/24
- New Scope – Related to Regional Centers for Digital Investigation – Active
- Legal Review with AG's Office – Ongoing meetings and collaboration



Digital Evidence Study Checklist

Bulk Media and Digital Evidence Study Completion Checklist		March '24	April '24			May '24		
Task and Activities that are still outstanding to completing the delivery of the Study Documents.								
Interviews and Outreach								
The Miller Center – Select Individuals	Sean	Green	Blue					
Larry Compton – Internet Consultant – now with Magnet Software fulltime	Maureen	Blue						
The Major Regional Representative Municipal Police Departments	Evan	Green	Blue					
New Haven Police Department	Evan	Blue						
Bridgeport Police Department	Evan	Green	Blue					
New London Police Department	Evan	Green						
East Lyme Police Department	Evan	Green						
Current State Document								
Current State Document – Stand Alone	Sean/Evan/Maureen	Green	Blue					
Complete DRAFT	Evan	Green	Blue					
Socialize with Stakeholders DRAFT Document - ALL Stakeholders	All	Green	Blue					
Current State Stakeholder Use Cases - Scenarios - Final Templates	Sean/Sridhar	Green	Yellow	Blue				
Legal Compliance								
AG's Office Legal Guidance – Exec Team	Sean	Green	Blue					
Legal Compliance Summary	Sean/Evan/Maureen	Green	Yellow	Green				
Investigative Center Lab								
Interview Manchester Investigative Center	Sean/Evan/Maureen	Blue						
Interview Wilton\Weston Investigative Center	Sean/Evan/Maureen	Blue						
Forensic Software brands analysis	Sean/Evan/Maureen	Blue						
Compilation of software into functional categories and industry leaders	Maureen	Blue						
Details of the Regional Municipal Crime Labs	Sean/Evan/Maureen	Green	Yellow	Blue				
Design Mock “Digital Investigation Center” Lab with Products and Costs Estimates	Maureen	Green	Yellow	Green				
Future State Solution Hardware								
Hybrid Solution Specification	Sean	Green	Yellow	Green				
CJIS-CT Hybrid Solution cost projection	Anatolie	Green	Yellow	Yellow				
Chain-of-Custody SharePoint Solution Specification	Sean	Green	Yellow	Yellow				
CJIS-CT SharePoint Chain of Custody Solution cost projection	Saket and Anatolie/Archana Other Design Ops Team	Green	Yellow	Yellow				
Future State Solution Software								
Proposed Software Stacks	ALL	Green	Yellow	Yellow				
Future State Document Analysis								



Digital Evidence Study Checklist

- Next Milestone(s)
 - To-Be Business Solutions Document
 - Executive Summary Document

Bulk Media and Digital Evidence Study Completion Checklist	Assignee	March '24	April '24	May '24
Proposed Software Stacks	ALL	Complete	Watch	
Future State Document Analysis				
Solution Approach Specifications (analysis and summaries)	Sean	Complete	Watch	
Solution Specifications (detailed build specifications)	Sean/Evan	Watch	Complete	
Financial Models for each solution specification	Sean	Watch	Watch	
Future State Solutions Solution cost projection	Saket and Anatolie/Archana	Complete	Watch	
Chain-of-Custody Model – Model Specification	Other Design Ops Team	Complete	Watch	
Current State Stakeholder Use Cases - Scenarios	Sean	Watch	In Progress	
Future Solutions State(s) Proposed Use Cases - Scenarios	Sean/Evan	Complete	Watch	
	Saket and Anatolie/Archana			
Future State Proposed Solutions Document				
Solution Comparison Matrix Rankings Analysis	Sean	Watch	In Progress	
Complete DRAFT Document	Evan	Watch	In Progress	
Final Graphics and Charts	Evan/Tamika	Watch	Watch	
Final Document Reviews	Sean/Evan/Maureen	Watch	Watch	
Publish Final Document	ALL	Watch	Watch	
Future State Stakeholder Use Cases - Scenarios - Final Templates	Sean/Sridhar	Complete	Watch	
CPCA - Identify Pilot PDs		Complete	Watch	
Executive Summary Document				
Solution Comparison Matrix Rankings Analysis	Sean/Evan	Complete	Complete	
Solution Financial Model Comparisons	Sean/Evan	Complete	Complete	
Current State	Sean/Evan	Complete	Complete	
Future State	Sean/Evan	Complete	Complete	
Gap Analysis	Sean/Evan	Complete	Complete	
CPCA - Identify Pilot PDs - Queue Up Demand and Early Adopters				

Notes:

CISS Digital Evidence File through Electronic Arrest – Involve Dmitry, Sergey, Anatolie

Complete
In Progress
Watch
Barrier



Current Milestones and Progress



In Progress

- Final Planned Interviews
- Financial Models for alternate solutions approaches
- Solution Specifications and Rankings



Upcoming

- Publish Study Documents
 - To-Be Business Solutions Document
 - Executive Summary Report



Chain of Custody Model - Overview

Overview of the Digital Evidence Chain-of-Custody Model

The Chain-of-Custody Model for Digital Evidence is a procedural framework used in forensic investigations to maintain the integrity and admissibility of digital evidence in legal proceedings. It involves documenting the chronological record of custody, control, transfer, analysis, and disposition of digital evidence throughout its lifecycle.

Key components of the Chain of Custody Model include:

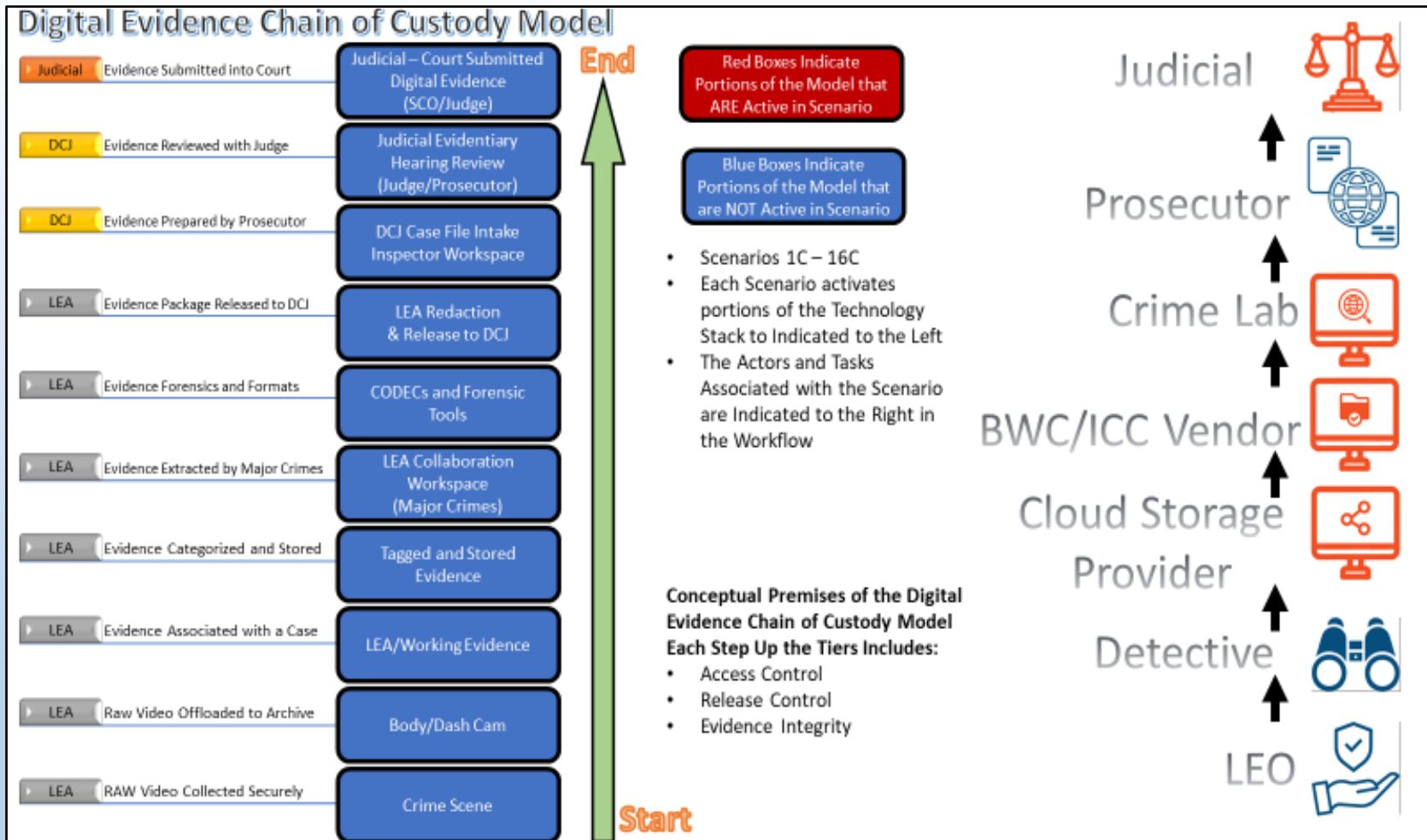
1. **Identification:** Clearly identifying the digital evidence, including its source, location, and relevance to the investigation.
2. **Collection:** Collecting digital evidence using proper methods and tools to preserve its integrity and authenticity. This may involve making forensic copies of digital media to prevent alteration or corruption of the original evidence.
3. **Documentation:** Thoroughly documenting every step of the evidence handling process, including who collected the evidence, when and where it was collected, and any changes in custody or control.
4. **Preservation:** Safeguarding the integrity of digital evidence by storing it securely in a controlled environment to prevent tampering, alteration, or unauthorized access.
5. **Analysis:** Conducting forensic analysis on the digital evidence using specialized tools and techniques to extract relevant information and establish its authenticity and reliability.
6. **Presentation:** Presenting the findings of the forensic analysis in a clear and understandable manner, including any conclusions drawn from the evidence.
7. **Transfer:** Ensuring the secure transfer of digital evidence between parties involved in the investigation, while maintaining a documented record of custody and control.
8. **Disposition:** Properly disposing of digital evidence in accordance with legal and regulatory requirements once it is no longer needed for the investigation.

Adherence to the Chain of Custody Model helps to establish the reliability and admissibility of digital evidence in court, by demonstrating that it has been handled and preserved in a manner that maintains its integrity and authenticity throughout the investigation process. Failure to maintain a proper chain of custody can result in evidence being challenged or excluded from legal proceedings.



Chain of Custody Model – Scenario View

- Scenario Drawings
- Converted to Timeline Narratives
- Indicates Portion of the Technology Infrastructure is Active





Chain of Custody Model - Use Cases (Scenarios)

Current State Scenarios

Scenario #1C – PD – All BWC/Dash Cam video is stored locally

Scenario #2C – PD – All BWC/Dash Cam video is stored in a CJIS Vendor Cloud

Scenario #3C – PD – All BWC/Dash Cam video is stored in the BWC/Dash Cam Vendor storage service

Scenario #4C – CT State Police - All Body Cam/Dash Cam video is stored in the Panasonic Vendor Cloud

Scenario #5C – PD – Officers and Detectives gather large amount of media files

Scenario #6C – PD – Major Crimes Division Stores Evidence Onsite and/or with a CJIS Cloud Provider

Scenario #7C – PD – Major Crimes Division Stores Evidence with the BWC/Dash Cam Vendor storage service

Scenario #8C – PD – Major Crimes Division uses forensic software to analyze Digital Evidence

Scenario #9C – PD – LEA Evidence Officer uses video codec conversion software for standardization of video type

Scenario #10C – PD – Delivers Evidence to the Prosecutor on DVD, Flash Drive, or External Hard Drive

Scenario #11C – DCJ – Prosecutor – Accepts all Evidence through Axon “Evidence.com” service into Axon Justice Evidence Intake Portal

Scenario #12C – DSS Crime Lab – Returns Reports back to the PD by email, Evidence is returned to Officer in person who come to retrieve it

Scenario #13C – Medical Examiner – Returns Reports back to the PD by email

Scenario #14C – DCJ – Prosecutor – Presents Prospective Digital Evidence at Evidentiary Hearing

Scenario #15C – DCJ – Prosecutor – Releases Digital Evidence to Public and Private Defenders and Other Entitled Parties Using a “Discovery” Web Portal

Scenario #16C – DCJ Prosecutor – Presents Approved Digital Evidence at Court Hearing



Chain of Custody Model – Scenarios (Example)

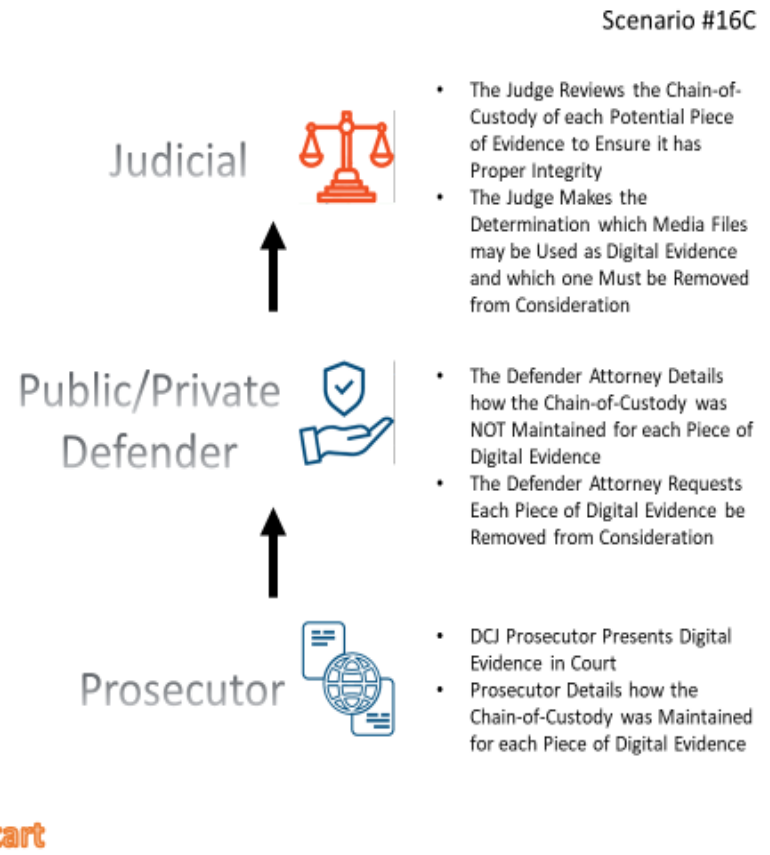
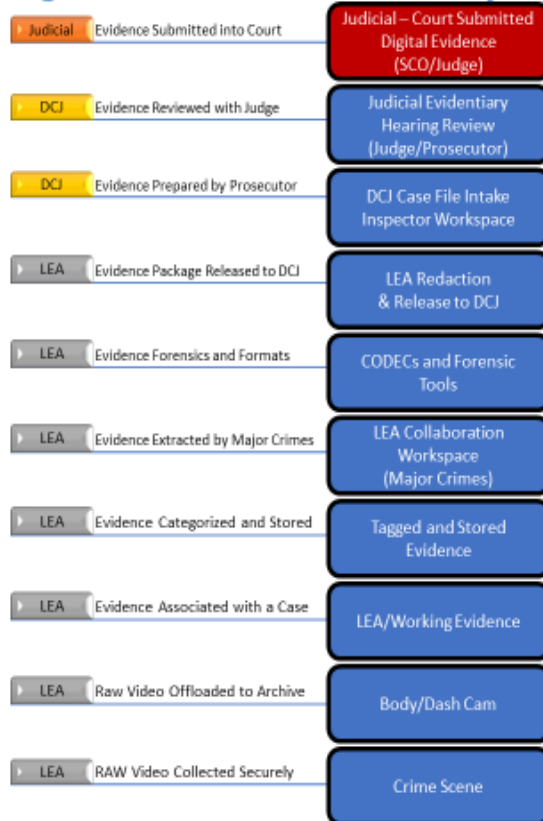
Scenario Summary - DCJ – Prosecutor Presents Approved Digital Evidence at Court Hearing

Agency	Scenario #
Department of Criminal Justice - Chief State's Attorney	16C
Use Case Description	
DCJ – Prosecutor Presents Approved Digital Evidence at Court Hearing	
Objective of Use Case Scenario	
To Provide <u>all</u> of the Digital Evidence that has been Approved for Use in Court	
Commonly Occurring Difficulties and Challenges	

- The Digital Evidence may need to be re-burned to physical media, or burned to DVDs after adjustments to which portions of the evidence are used.
- The cost of physical media is significant.
- The time required to create additional copies is significant.
- It is challenging to have a standard playback in Court.
- Sometimes an outside company is used for playback which is costly.

- Scenario Drawings
- Converted to Timeline Narratives
- Indicates Portion of the Technology Infrastructure is Active

Digital Evidence Chain of Custody Model



- The Judge Reviews the Chain-of-Custody of each Potential Piece of Evidence to Ensure it has Proper Integrity
- The Judge Makes the Determination which Media Files may be Used as Digital Evidence and which one Must be Removed from Consideration
- The Defender Attorney Details how the Chain-of-Custody was NOT Maintained for each Piece of Digital Evidence
- The Defender Attorney Requests Each Piece of Digital Evidence be Removed from Consideration
- DCJ Prosecutor Presents Digital Evidence in Court
- Prosecutor Details how the Chain-of-Custody was Maintained for each Piece of Digital Evidence



Regional Centers for Digital Investigations (Regional CDIs)

Forensic Software

- Provides **ability to extract, analyze, and/or manage data** from computers, mobile devices, etc.
- Can be **cost-prohibitive**
- Some municipalities formed **regional CDIs** to address growing needs
 - CT CDI (in Manchester, 10 departments)
 - Fairfield County Technical Investigation Unit (in Weston, 12 departments)

Needs:

1. Software licenses

- To address common needs, e.g., phone & computer decryption/analysis; video review/analysis; redaction

2. Advanced computer hardware

- State-of-the-art Central Processing Unit (CPU)
- Significant Random Access Memory (RAM)

3. Servers and Storage

- Servers with many terabytes (TB) storage
 - Ex. CT CDI has total 770 TB storage over four servers and backup server



Regional CDIs, Potential Future

Potential Future

Provide **key forensic software products** as hosted applications **within the Digital Evidence Chain-of-Custody Stack**:

- **Software Licenses**
 - Provide software addressing common needs
 - Manage software contracts and licenses at state level
- **Advanced computer hardware**
 - Utilize regional hardware, as needed
- **Servers and Storage**
 - Leverage state servers and storage





Interview Schedule – Completed/Remaining

Agency Name	Primary Contact	Date		Category
CT Center for Digital Investigations	Sgt. Ryan Bycholski	3/14/24	✓	Stakeholder
Legal Consultation	AG's Office	3/19/24	✓	Legal Compliance
Bridgeport PD	Sgt. Joel Carley	3/19/24	✓	Stakeholder
Legal Consultation (2 nd meeting)	AG's Office	4/2/24	✓	Legal Compliance
Fairfield County TIU	Capt. Matt Brodacki	4/4/24	✓	Stakeholder/Industry Expert
DESPP CSO	Glory Bulkley	TBD		Primary Stakeholder
New London PD	TBD	TBD		Solution Leader



Newest Interviews

- **CT CDI**
 - Shared digital investigative resource center for member PDs
 - Collaborated to gain collective access to software and equipment municipal PDs would not otherwise have
 - Expensive to maintain software and equipment, no easy way to store/share digital evidence
- **Fairfield County TIU**
 - Created due to a backlog with the state lab over 10 years ago
 - Not a crime lab, but a shared digital investigative center with members dedicated from each PD
 - High costs for equipment, software and storage. Would be interested in a state solution if it alleviated burden.
- **Bridgeport PD**
 - Video storage is expensive and growing (400 new videos per day)
 - Sharing solution is fairly simple, but allows third party sharing with limited security
 - Would use a future storage and sharing solution



AG's Office Collaboration

Legal Analysis and Opinions

- **Retention Policies**
 - Clarified a 30 day minimum as part of State Librarian requirements
 - New POST guidelines call for 90 day minimum
- **Freedom of Information**
 - CJIS is protected under current statute. FOI requests must be made to originating agency.
 - If a solution was built as a part of CISS, likely protected under current statute. However, recommendation would be to modify statute to include any “digital evidence repository”.
- **Subpoenas from State or Federal Entities**
 - Could write protections into state legislation. Would need to consider federal ramifications
- **Police Department Rights to the Data**
 - Storage location/method should not modify the originating agency's control of the data

Upcoming Discussions/Considerations

- Sole source vendor contract option
- CJIS Obligations



Current State Document Updates

- Final Design Template and Formatting have been selected
- Modifications and additions from recent interviews
- Looking for feedback from stakeholders before publishing a final version at the conclusion of the study



A Study of Centralized Data Storage for Recordings from Body-Worn Recording Equipment and Dashboard Cameras: Current State

Contents

1. Executive Summary
2. Introduction
3. Digital Evidence Business Environment
4. Digital Evidence Technical Environment
5. Contracts and Labor Costs



Current State Document Outline

- Executive Summary
- Introduction
- Digital Evidence Business Environment
- Digital Evidence Technical Environment
- Contracts and Labor Costs



Table of Contents

I. Executive Summary	6
A. Digital Evidence Business Environment.....	6
B. Digital Evidence Technical Environment.....	8
C. Summary.....	9
II. Introduction	11
D. A. Purpose.....	11
E. B. Document Scope.....	12
F. C. Assessment Approach.....	13
G. D. Key Terminology/Background.....	17
III. Digital Evidence Business Environment	20
A. BWC and Dash Camera Video Capture.....	20
B. BWC and Dash Camera Video Upload.....	21
C. BWC and Dash Camera Video Retention Storage.....	22
D. Crime Scene and Bulk Media Capture and Storage.....	23
E. Digital Forensic Data Capture and Storage.....	23
F. Stakeholder Agencies.....	24
1. CT State Police.....	25
2. Municipal Police Departments.....	28
3. DCJ.....	42
4. Division of Public Defender Services.....	45
5. Judicial Branch.....	46
IV. Digital Evidence Technical Environment	51
A. Methodology.....	52
1. DCJ CITS-CT Survey.....	52
2. In-Depth Representative Sampling Questionnaire.....	53
3. All Department Outreach.....	53
B. Key Findings.....	54
C. Data Storage.....	55
D. Vendors and Applications.....	56
E. Digital Forensic Technology.....	59
F. Identified Issues.....	61
V. Contracts and Labor Costs	64
H. BWC and Dash Cam Storage.....	64
1. Vendor Contracts Analysis.....	64
2. Survey Results Analysis.....	65
3. Comparative Results Analysis.....	66
I. On-premises Storage.....	67
J. Labor.....	68
K. Total Overall Costs.....	72

Appendix A – Assumptions.....	75
Appendix B – Glossary of Terms.....	77
Appendix C – Glossary of Acronyms.....	80
Appendix D – Cost Analysis Worksheets.....	83
Appendix E – Information Exchange Use Cases.....	86
Appendix F – Participant Agencies and Identified Issues.....	107
Appendix G – Key Points by Interview.....	111
Appendix H – Technology Initiatives by Agency.....	119
Appendix I – Survey Questions and Response Data.....	121



Current State Document Features

- Margin notes to highlight key points
- Footnotes for added context
- Appendices for detailed info and raw data



Despite little standardization across Connecticut's LEAs, departments are experiencing the same data growth and need for greater storage and digital resources.

incidents or serious crimes may be kept for years or indefinitely, meaning a consistently growing need for long-term video storage.

- Storage needs of police departments across the board is increasing due to the growing number of digital evidence collection methods and increasing quality of evidence, highlighting the need for reliable, scalable storage solutions.
- There is a growing need for LEAs to have access to easy-to-use video redaction software and digital forensic tools to prepare video for court or public release in the case of Freedom of Information (FOI) requests.
- CJIS-CT has discovered that LEAs are cooperating and forming regional digital forensics units to manage requests for processing digital evidence. Examples include advanced forensic analysis of computer hard drives and mobile devices. This is a new finding which is noteworthy regarding a solution definition and will be discussed in this report.

B. Digital Evidence Technical Environment

The current technical environment is comprised of a wide range of on-premises and cloud solutions² that allow LEAs to fulfill their individual business processes. Interviews, surveys, and other outreach efforts conducted from August 2023 to March 2024 yielded the following information:

- BWC and Dash Camera video are largely stored on a vendor's cloud storage solution. On the contrary, Crime Scene data and other digital media³ are largely stored on-premises, utilizing a server, physical devices like thumb drives or external drives, or a combination of servers and devices.

² On-premises solutions are software and storage solutions that utilize hardware or software located onsite at the police department. Cloud solutions utilize offsite hardware or software, typically at an offsite datacenter run by an organization or a cloud vendor.

³ Digital media is any software, images, video, or other data in digital form that is maintained by a police department. Complete definitions are available in Appendix B, Glossary of Terms.



To Be Business Solution Process

1. Consider GAP Analysis
2. Determine Critical to Success Factors
3. Determine Framework Model – Chain-of-Custody Workflow Framework
4. Determine Framework Scenario Actors
5. Determine Scenario Workflows (Future State Scenarios 1-X)
6. Choose Solution Creation Methodology
7. Create Solution Descriptions
8. Choose Solution Comparison for Suitableness Methodology
9. Create Financial Models
10. Incorporate historical pricing of Disk and Usage Projections
11. Table of Solution Companies to Address the GAP Issues from the Context of the Whole Chain of Custody Model
12. Final Solution Comparison Section (Matrix Ranking) and Cost Comparison and Success Factors ADDRESSED by each in a comparison Table.
13. TBD - Additional Steps



Digital Evidence Solution Models

1. Purchased Solution – 3rd party vendor-requires CISS integration for sharing
2. DCJ Axon Sharing Solution – no Internal State of CT storage for PDs
3. CT State-built sharing workflow and portal for PDs, Prosecutors and Court – storage included
4. CT State-built Storage and Portal Solution will integrate with CISS for sharing
5. CJIS-CT Builds and Maintains the Entire Chain-of-Custody Architecture with Storage Infrastructure



Digital Evidence Solution Model #1

1. Purchased Solution – 3rd party vendor-requires CISS integration for sharing
 - The State purchases and manages the contracts for the market leader bundle of body and dash camera footage storage and video storage software solution (RFQ, Market Leader is Axon) and hosts the software internally
 - BWC/ICC Videos and Crime Scene Bulk Media files are all stored in a PD Specific file storage area in the CJIS-CT Datacenter Infrastructure using the BWC/ICC software services
 - Axon is the Solution Provider to DCJ for the inbound interface “Evidence.com” portal
 - The PD can copy (release) files to DCJ using the “Evidence.com” or the “Justice.com” inbound file intake service for DCJ
 - Primarily benefits are the lower cost for the LEAs and the streamline of Digital Evidence workflow to and through the interface with the Prosecutors Axon System
 - Specifics:
 - BWC\ICC and Bulk Media are Stored at CJIS-CT using the Vendor Software
 - No direct integration with CISS Electronic Arrest Workflow to deliver Digital Evidence to the Prosecutors



Digital Evidence Solution Model #2

2. DCJ Axon Sharing Solution – no Internal State of CT storage for PDs
 - No CT State-Solution and then fully leverage the Axon-DCJ “Cloud” Current solution option
 - Each LEA and PD can continue with their own methods and process, Axon Security IDs
 - The submission of Digital Evidence is standardized around the DCJ Axon intake process using the “Evidence.com” Cloud Service
 - Axon would have the lead to consume videos from other vendors and file types and expand this capability



Digital Evidence Solution Model #3

3. CT State-built sharing workflow and portal for PDs, Prosecutors and Court – storage included
 - State Built software/DB and infrastructure to allow PDs to store BWC\ICC and Bulk Media at the State of CT run Datacenter “On-Premise”
 - Digital Evidence files as part of a storage and sharing work area to collaborate, File Retention, Codec Conversion Solutions, Promote to Prosecutors
 - Digital Evidence files can be transmitted through “Justice.com” directly to the Prosecutor
 - Prosecutors can refer to Digital Evidence Files directly “On-Premise” for Evidentiary Hearings
 - User IDs are controlled and managed by the CJIS-CT CISS Identity Manager



Digital Evidence Solution Model #4

4. CT State-built Storage and Portal Solution will integrate with CISS for sharing
 - Using CISS electronic arrest workflow to include Digital Evidence files as part of the arrest package of documents
 - State Built software/DB and infrastructure to allow PDs to store BWC\ICC and Bulk Media at the State of CT run Datacenter “On-Premise”
 - Digital Evidence files as part of a storage and sharing work area to collaborate, File Retention, Codec Conversion Solutions, Promote to Prosecutors
 - Digital Evidence files can be transmitted through CISS to the Prosecutor
 - User IDs are controlled and managed by the CJIS-CT CISS Identity Manager



Digital Evidence Solution Model #5

5. CJIS-CT Builds and Maintains the Entire Chain-of-Custody Architecture with Storage Infrastructure

- CJIS-CT would leverage the CISS Certified Data Center
- A modern Document Storage and Workflow solution would be the backbone of the solution (e.g. Microsoft SharePoint)
- All Tiers would be secured to each Police Department for full separation of media and video files
- Digital Evidence from On-Premise Storage could be Promoted and Released to DCJ:
 - As part of the Arrest Paperwork from the RMS through CISS directly to DCJ
 - As part of the DCJ Axon “Justice.com” DCJ file Ingestion Portal Cloud Service



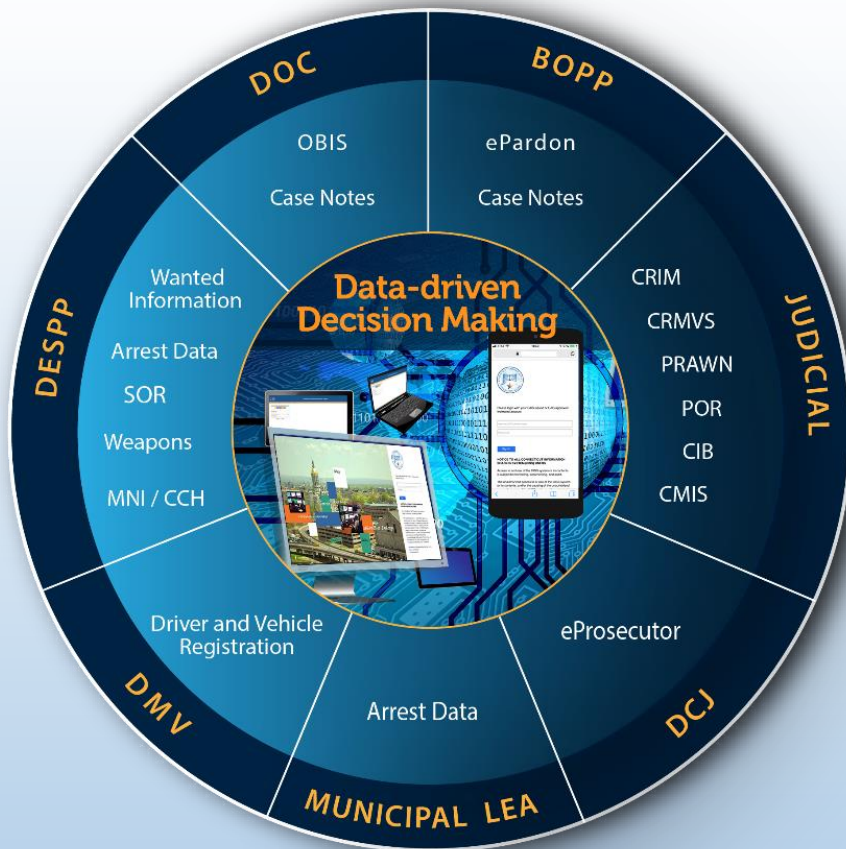
Upcoming Milestones

April

- Published Study Document (Current State/As-Is Business Model)
- Security Assessment with AG's Office
- Security Assessments with Judicial's Legal Office
- Published Study Document (Requirements/Gap/To Be Solutions) – 4/30/24
- Published Study Document (Executive Summary Document)



Digital Evidence Study – Project Steering Committee 2024 Meeting Schedule



Next Meeting

May 9, 2024

For questions and comments email
CJIS.HelpDesk@ct.gov

CISS Dashboard
<https://dashboard.cjis-ciss.ct.gov>



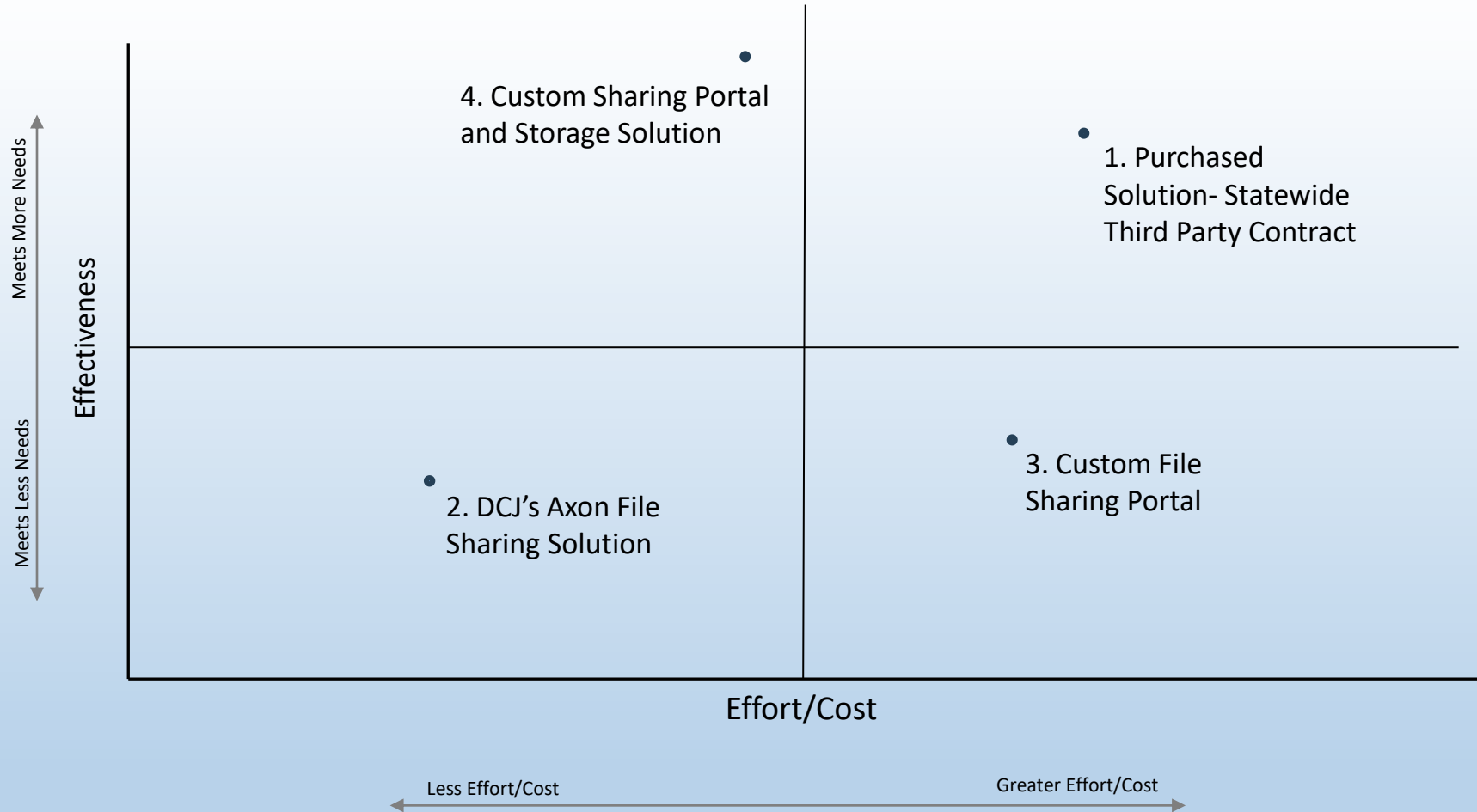
Closing Remarks/Adjournment



Appendix-Reference Material



Solutioning Matrix





Solution Space of Approaches

- 1. Purchased Solution-3rd party vendor-requires CISS integration for sharing**
 - The State purchases and manages the contracts for the market leader bundle of body and dash camera footage storage and video storage solution
 - Primarily benefits are the cost for the LEAs and the streamline of Digital Evidence workflow to and through the interface with the Prosecutors Axon System
- 2. DCJ Axon Sharing Solution – no storage for PDs included**
 - Each LEA and PD can continue with their own methods and process
 - The submission of Digital Evidence is standardized around the DCJ Axon intake process
- 3. CT State-built sharing workflow and portal for PDs, Prosecutors and Court – storage included**
 - Digital Evidence files as part of a storage and sharing work area to collaborate, File Retention, Codec Conversion Solutions, Promote to Prosecutors
- 4. CT State-built Storage and Portal Solution-will integrate with CISS for sharing**
 - Using CISS electronic arrest workflow to include Digital Evidence files as part of the arrest package of documents



Project Overview

What is the purpose of the Study?

The purpose of the steering committee is to *provide advice* and *guidance* from a cross branch/cross agency point of view regarding the Digital Evidence Storage and Management Study undertaken by the Criminal Justice Information Systems Governing Board, in collaboration with State agencies, branches and municipal police departments.

- The CJIS-CT Governing Board Executive Director and staff will provide necessary project management and technical support for the project.
- The CJIS-CT Governing Board retains overall authority for the study.

Scope

The Steering Committee will oversee the study phase of the project. At a high level, the scope of the steering committee is to assist the CJIS-CT team and cross branch/agency project management team in developing a statewide digital evidence storage and management plan and to identify and estimate the projects that are needed to implement this plan. The steering committee will provide advice and guidance on the overall project and provide requirements pertaining to their agency or branch. Each members also serves as a point-of-contact for their agency or branch for this project.



The Study – The Essentials

The Study Should Determine:

- Boundaries of the Opportunity Space, Interface Requirements to other systems (e.g. DCJ, Judicial, PDs)
- Cost of Equipment and Licensing to LEAs, Cost of Labor and Administration to LEAs
- GAP of smaller PDs to the most capable PDs
- CISS can be used to perform Chain-Of-Custody of Digital Evidence as part of the Electronic Workflow of Arrest Documents
- CJIS-CT can provide value in hosting centralized contracts and DEMS Software
- CISS can be leveraged as a cost-effective centralized storage for Bulk Media
- The Study should conclude 4 – 6 potential solutions covering the SUCCESS FACTORS



The Study Outputs

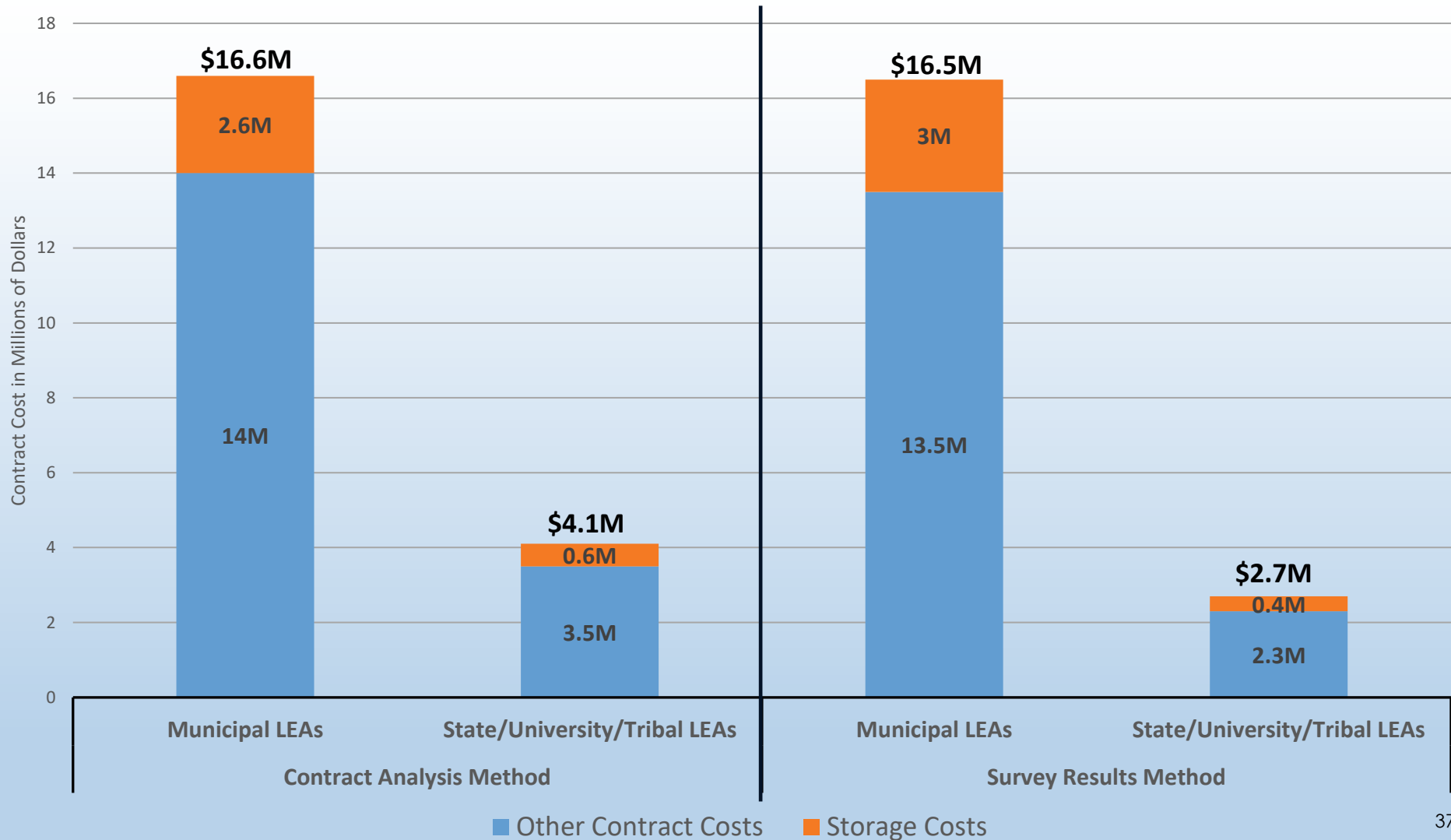
- The Study should conclude 4 – 6 potential solutions covering the SUCCESS FACTORS
 - Potential Success Factors
 - Lower Cost for LEAs
 - Remove labor burden of LEAs Staff and Resources
 - Centrally Manage Contracts and Equipment at the State Level
 - Improve access for smaller LEAs to top level technologies of the big PDs
 - Centralize Data Retention and Compliance activities and labor
 - Create a Highly Functional Interface to Prosecutors Office
 - Ensure Judicial has a class-leading Chain-of-Custody ingestion workflow/process
- Degrees of Freedom of Solution Chart is
 - Either two (2D) or three (3D) degrees
 - Cost, Completeness of Solution, Time to Implement, etc.
- Solutions selected envelop the Degrees of Freedom Space
 - Maximize certain Pro's
 - Minimize certain Con's





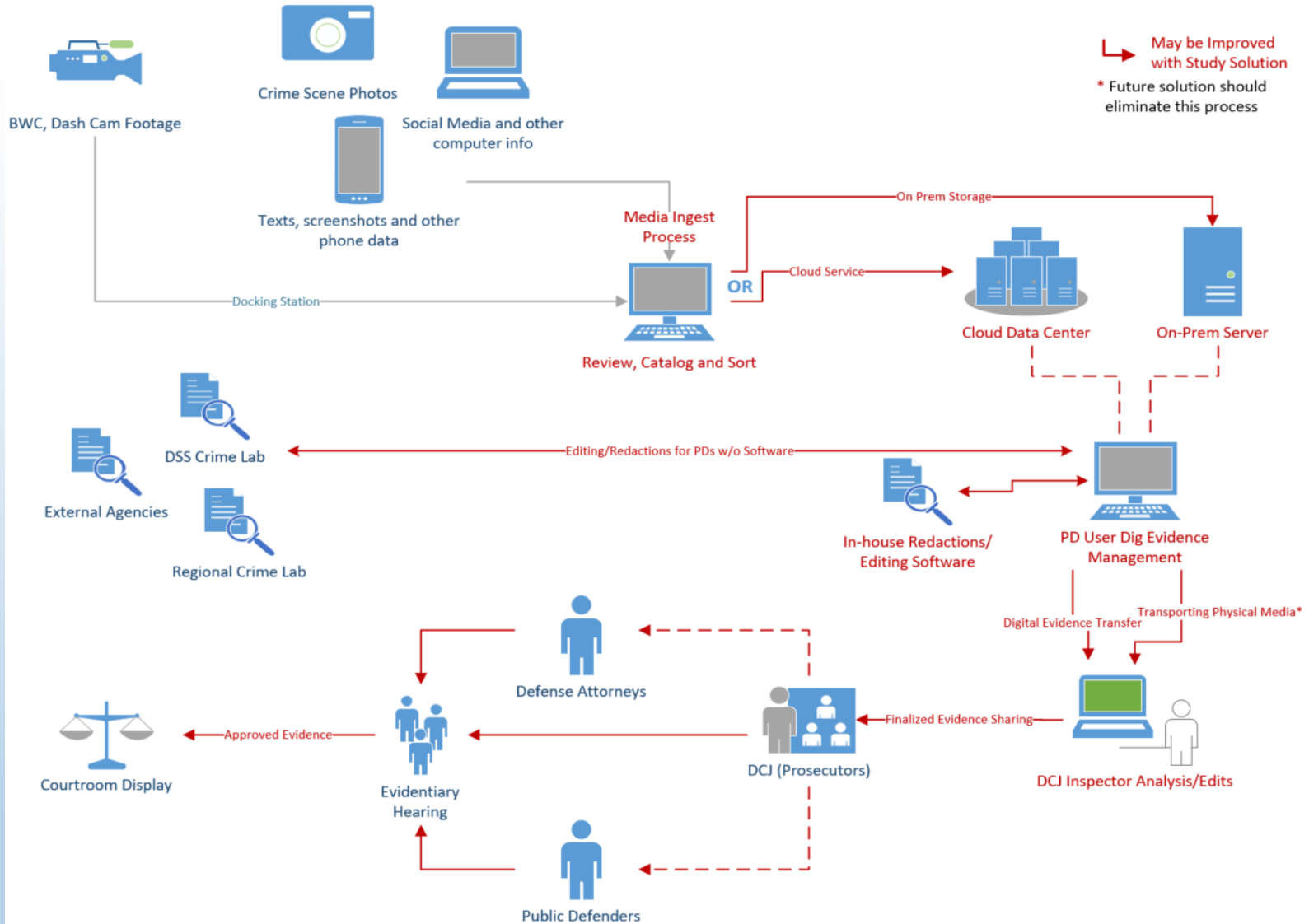
Statewide Annual Cost Estimate Comparison

Estimated Costs for Statewide Third Party Vendor Contract by Method





High-Level Diagram Concept





Prosecutor Success Factors

1. Standardizing how evidence is received and shared ✓
2. Eliminating CDs, DVDs and USB drives that can bog down the intake process ✓
3. Digitally transforming time-consuming manual processes so prosecutors can spend more time building and prosecuting cases
4. Digital Evidence Management Systems speed up the flow of evidence ✓
5. Taking the worry out of missing evidence ✓
6. Empowering prosecutors with built-in tools to play, redact and transcribe video ✓
7. Built-in state-of-the-art transcription and keyword search tools
8. Streamlining discovery with defense and reducing discovery backlogs
9. All discovery workflows are managed electronically with full tracking ✓
10. Overcoming file size limitations in sharing evidence with courts.

From <<https://www.nicepublicsafety.com/resources/digital-evidence-management-system-dems-guide>>

✓ Indicates the CT DCJ noted these as primary challenges



Technology Stack Considerations

- 1. Document and File based Workflow with Storage – Security at each level**
 - **Several Studies available on the internet have ranked MS SharePoint as the leading Enterprise Solution**
 - **Access Control (coupled to Identity Management System)**
 - **Release and Promotion control of files**
 - **Integrated database storage**
 - **On Premise**
 - **Off Premise tie in interface**
 - **Collaboration Areas where software applications can be published**
 - **No need for local versions of the software**
 - **CPU Intensive Forensic Applications can run on DataCenter Servers linked directly to storage (much faster than local software running on PCs)**
- 2. Data Storage of files must be on CJIS Compliant Data Centers**
 - **On-Premise or Cloud based**
 - **Storage must be tightly coupled to generation event to determine file type and storage retention requirements**
- 3. Users IDs and Access Control should be tightly controlled and CJIS Compliant**