April 4, 2019

Mr. Brandon McClain, Chair
Automatic Data Processing Board
451 West Third Street
Dayton, OH  45402

Dear Mr. McClain:

An Automatic Data Processing Board meeting has been scheduled for
Wednesday, April 10, 2019 at 9:00 a.m. in the 6th floor Data Processing
Training/Conference Room. The agenda will be as follows with
supporting documentation attached.

(1) Minutes from March 13, 2019 meeting

(2) Sheriff's Office - Purchase of Command Central Vault, a
digital evidence management solution, from Motorola
Solutions (total cost not to exceed $141,600.00)

Sincerely,

[Signature]

KARL L. KEITH, Secretary
Automatic Data Processing Board

KLK/bru

Attachments

Cc:  ADP Board Members
     James Alford, Data Processing Director
     Tina Ratcliff, Records Manager
     Steven Hollon, Common Pleas Court Administrator
     Kate Evans, Auditor’s Office
     Lynn Cooper, Treasurer’s Office
     Mary Montgomery, Prosecutor’s Office
     Erik Blaine, Coroner’s Office
Mr. McClain
Page 2
April 4, 2019

Cc: Jonathan Rike, BCC IT
    Chris Boyd, Data Processing
    Ellis Shockley, Data Processing
    Eric Armstrong, Domestic Relations Court
    Jennifer Petrella-Ahrens, Domestic Relations Court
    Tyler Small, Administrative Services
    Bart Kincaid, Sheriff’s Office
    Debra Harden, Recorder’s Office
    Herb Davis, Clerk of Courts’ Office
    Edward McNachtan, Common Pleas Court
    Ashley Kohl, Auditor’s Office
    Zach Zugelder, Treasurer’s Office
    Marsha Shaffer, Purchasing
    Kery T. Gray, Commissioner Carolyn Rice’s Office
    News Media
AUTOMATIC DATA PROCESSING BOARD MEETING
March 13, 2019

PRESENT: Brandon McClain, Chair
Erik Blaine for Dr. Kent Harshbarger, Vice-Chair
Karl Keith, Secretary
Bart Kincaid for Sheriff Rob Streck, Member
Mike Foley, Member
Steve Harsman, Member
Jan Kelly, Member
Russell Joseph, Member
Steve Hollon for Judge Gregory F. Singer, Member
Kery Gray for Carolyn Rice, Member
Tina Ratcliff, Records Management
Eric Armstrong, Domestic Relations Court
Jonathan Rike, BCC/IT
Katie Joseph, Auditor’s Office
Jeff Jordan, Office of Emergency Management
Edward McNachtan, Common Pleas Court-General Division
Bethany Colby-Lauffenburger, BCC/IT
Kristen Nastar, Coroner’s Office/ Crime Lab
Dr. Matthew Juhascik, Coroner’s Office/ Crime Lab
Mary Montgomery, Prosecutor’s Office
James Alford, Data Processing
Ellis Shockley, Data Processing
Betty Upshaw, Data Processing Administrative Assistant

The March 13, 2019 Automatic Data Processing Board meeting was called to order by the Chair, Brandon McClain. (A copy of the agenda is attached hereto for reference.)

The first item of business was the approval of the minutes from the February 13, 2019 meeting. Kery Gray moved to approve the minutes. His motion was seconded by Russell Joseph. Motion carried unanimously.

The Office of Emergency Management brought two requests before the Board for approval (Agenda item number two and three). The first request sought the Board’s approval of the purchase of 25 Radiation Detection Pagers and accessories from Thermo Eberlin (Bid #S0800019) for Homeland Security Region III Law Enforcement Agencies at a cost not exceed $96,000.00. Director Jeff Jordan explained the items would be purchased for law enforcement officers and Homeland Security Region III. He explained the use of pagers and briefed the Board on how the pagers would function. The second request sought approval to purchase 38 portable radios and accessories at a cost not to exceed $60,000.00 from J&K Communications (Bid # 800016). Mr. Jordan explained these radios would be used by various agencies within Homeland Security Region III. He said funding for both these purchases would come from
the FY16 Law Enforcement State Homeland Security (LE SHSP) grant. Following a brief discussion about how the radiation detection pagers would work with further explanation from Mr. Jordan, Erik Blaine made motion to approve both requests, agenda items two and three. Mr. Blaine’s motion was seconded by Russell Joseph. Motion carried unanimously.

Agenda number four was a request from Environmental Services seeking the Board’s approval to purchase from Emerge IT Solutions, off of OAKS Contract ID 533110-3-84, two (2) Cisco Stackable Managed Switches, one (1) Nimble Array and components along with professional services to install and transfer data. Bethany Colby-Lauffenburger, the BCC IT Manager representing Environmental Services, explained the need for the new equipment to replace old equipment. After a question from James Alford, the IT Director of Data Processing, about the capacity of the Nimble SAN, Ms. Colby-Lauffenburger informed him the change in the model number gives them additional storage and speed at the same cost. She reported the costs for these items, including hardware and professional services, would be $61,692.62. Following the request presentation, Steve Hollon moved for approval of the request. Motion seconded by Karl Keith. Motion carried unanimously.

The Board was informed by the Chair that Agenda item number five had already been handled and would not be presented to the Board. It was pulled from the agenda.

The next item of business, agenda item number six, was a request the Coroner’s Office which sought the Board’s approval to purchase a Liquid Chromatography Mass Spectrometry (LCMSMS) machine, including licenses and installation, at cost of $260,062.54. Erik Blaine, the Coroner’s Office/Crime Lab Director, apprised members this purchase would be a replacement for the system they have been using for some time and was put in their budget for this year during last year’s budgeting process. Dr. Matthew Juhascik, the technical expert for the Coroner’s Office/Crime Lab, explained to Board members that the machine is an instrument used in the Toxicology Lab for the detection and quantitation of drugs and poisons. Karl Keith asked if this purchase, which would be made from Agilent Technologies, was made through the competitive bidding process. Mr. Keith was informed this equipment is considered sole source. Dr. Juhascik explained why the purchase would be considered sole source. Following this explanation, Karl Keith made a motion to approve the request. Kery Gray seconded the motion. Motion carried unanimously.

Agenda item number seven was also a request from the Coroner’s Office seeking approval to purchase Applied Biosystems genetic analyzer models 310, 3130, 3130XL, 3500, and 3500XL, the 7500 Real-Time PCR instruments, Quant Studio 5, HID 1.3 software, and 9700,
Veriti, and ProFlex Thermal Cycler instruments necessary for the processing of DNA analysis at a cost of $161,829.60. Kristen Nastar from the Coroner’s Office/Crime Lab explained they won a competitive grant, the FY 2018-20 Forensics DNA Lab Efficiency Improvement grant, to purchase this instrument from Life Technologies/Applied Biosystems, the sole source provider. Ms. Nastar explained the instrument is used in their DNA casework. She stated the one they currently have would be obsolete in 2020. After a brief discussion, Karl Keith moved for approval of this purchase. Motion seconded by Kery Gray. Motion carried unanimously.

The next agenda item (number eight) was one from the Common Pleas Court-General Division asking for approval to purchase the Ohio Community Supervision System also known as OCSS, web-based case management system hosted at the State of Ohio SOC in Columbus, Ohio. Ed McNachtan, the Deputy Court Administrator, apprised Board members they were working with the vendor, Cobra Systems (STS# 534497) to onboard the product at a cost of $51,400.00. Mr. McNachtan explained this product would replace the CourtView’s Pre-Trial and Probation modules. James Alford asked if there were any contingency plans in the event of internet problems since the system is web based. After further discussion, it was decided there would be more discussion between the Data Processing IT staff and the Court IT staff about how to mitigate potential internet problems. Following the presentation, Jan Kelly made a motion to approve the request. Motion seconded by Erik Blaine. The motion carried unanimously.

The last agenda item (number nine) was a request from the Montgomery County Microsoft Dynamics 365 Implementation team requesting approval of a Contract Management Change Order to the original contract awarded to Crowe LLP. Katie Joseph, the joint Project Manager for the project team, sought approval for services from the vendor to implement Contract Management Functionality utilizing the CRM (Customer Relationship Management) Module of Microsoft Dynamics 365 ($178,000.00) as well as Microsoft Dynamic 365 CRM Licensing from Dell Marketing LP as an annual operating cost of $26,040.00. Ms. Joseph explained this additional module, which was not included in the original contract, would allow the County to create, monitor, maintain and manage all the contracts that are under the Board of County Commissioners, the Department of Public Health, and any other contracting agencies with outside boards. After further discussion, Karl Keith moved for approval. Erik Blaine seconded the motion. Motion carried unanimously,
There being no further business, Steve Harsman made a motion to adjourn the meeting. Erik Blaine seconded the motion. Motion carried unanimously.

Respectfully submitted,

[Signature]

KARL L. KEITH, Secretary
Automatic Data Processing Board

KLK/bru
Attachment
Mr. Brandon McClain, Chair
Automatic Data Processing Board
451 West Third Street
Dayton, OH 45402

Dear Mr. McClain:

An Automatic Data Processing Board meeting has been scheduled for
Wednesday, March 13, 2019 at 9:00 a.m. in the 6th floor Data Processing
Training/Conference Room. The agenda will be as follows with
supporting documentation attached.

(1) Minutes from February 13, 2019 meeting

(2) Office of Emergency Management - Purchase of Radiation
Detection Pagers and Accessories from Thermo Eberlin (cost
not to exceed $96,000.00)

(3) Office of Emergency Management - Purchase of Portable Radios
and accessories from J & K Communications (cost not to
exceed $60,000.00)

(4) Environmental Services - Hardware and professional services
purchases ($61,692.62)

(5) Environmental Services - Professional services for technical
support with Cityworks (cost not to exceed $87,000.00)

(6) Coroner's Office - Purchase of Liquid Chromatography Mass
Spectrometry (LCMSMS) machine including licenses and
installation ($260,062.54)

(7) Coroner's Office - Life Technologies/Applied Biosystems
Purchase and Integration including system, licenses and
installation ($161,829.60)

(8) Common Pleas Court-General Division - Purchase of the Ohio
Community Supervision System (OCSS) ($51,400.00)
(9) Microsoft Dynamics 365 Implementation Team - Contract Change Order ($178,000.00) + 26,040 \approx 204,040

Sincerely,

[Signature]

KARL L. KEITH, Secretary
Automatic Data Processing Board

KLK/bru

Attachments

Cc: ADP Board Members
   James Alford, Data Processing Director
   Tina Ratcliff, Records Manager
   Steven Hollon, Common Pleas Court Administrator
   Kate Evans, Auditor’s Office
   Lynn Cooper, Treasurer’s Office
   Mary Montgomery, Prosecutor’s Office
   Erik Blaine, Coroner’s Office
   Jonathan Rike, BCC IT
   Chris Boyd, Data Processing
   Ellis Shockley, Data Processing
   Eric Armstrong, Domestic Relations Court
   Jennifer Petrella-Ahrens, Domestic Relations Court
   Tyler Small, Administrative Services
   Bart Kincaid, Sheriff’s Office
   Debra Harden, Recorder’s Office
   Herb Davis, Clerk of Courts’ Office
   Edward McNachtan, Common Pleas Court
   Marsha Shaffer, Purchasing
   Ashley Kohl, Auditor’s Office
   Zach Zugelder, Treasurer’s Office
   Jeffrey Jordan, Office of Emergency Management
   Bethany Colby-Lauffenburger, BCC-IT
   Janet Holman, OMB
   Katie Joseph, Auditor’s Office
   News Media
April 1st, 2019
Mr. Karl Keith
Montgomery County Administration Building
451 W. Third St.
Dayton, OH 45422-1027

Mr. Keith,

The Sheriff’s Office would like to be added to the April, 2019 Data Processing Board agenda to request approval to purchase Command Central Vault, a digital evidence management solution from Motorola Solutions. The Vault application, which is part of the Command Central platform that we already own, provides us with a comprehensive solution that integrates directly with our existing Motorola products. It allows us to store, search, review, and audit all of our digital evidence files with access accountability and safeguarding against accidental deletion. This product is being purchased as an amendment to Resolution 15-1783, which is when we initially purchased the Motorola CommandCentral product suite, along with the Motorola PremierOne public safety application suite. We are expanding our existing use of the solution by purchasing the CommandCentral Vault solution. It was designed to integrate directly with our PremierOne Records and CAD system to enable advanced capabilities in the system for evidence gathering that we currently can’t use without CommandCentral Vault. The pricing breaks down as follows:

Year 1: $45,120 – Development & Implementation / Annual Subscription Fee 15TB Storage Plan
Year 2: $24,120 – Annual Subscription Fee 15TB Storage Plan
Year 3: $24,120 – Annual Subscription Fee 15 TB Storage Plan
Year 4: $24,120 – Annual Subscription Fee 15 TB Storage Plan
Year 5: $24,120 – Annual Subscription Fee 15 TB Storage Plan

Total Cost Not To Exceed: $141,600.

This money has been appropriated in OCA 136385/9110 and was approved in the 2019 Budget Request. There are no additional maintenance costs associated with the five year term and no Data Processing support is needed for this project.

Respectfully,

Bart Kincaid
COMMAND CENTRAL VAULT

OPERATIONS SIMPLIFIED

REQUEST A DEMO:
Register online at motorolasolutions.com/spssdemo

SOLID SECURITY
Content captured in the field is digitally signed to ensure authenticity when stored in CommandCentral Vault. The original content is always preserved and every action taken on content is logged for comprehensive audit and chain of custody needs.

CommandCentral Vault is built on the CJIS compliant, Amazon Web Services GovCloud from the moment content is created and stored to when it’s shared, it is fully secured.

You need a digital evidence management solution that securely and efficiently stores all forms of multimedia and allows your agency to easily review, manage and share content, including evidence. CommandCentral Vault provides an advanced end-to-end content management solution that is secure and feature-rich with predictable pricing designed to streamline your operations. With CommandCentral Vault you can reduce administrative overhead and simplify workflows while maintaining policy and compliance to help save time and enhance community support.

TRANSFORMING DIGITAL EVIDENCE MANAGEMENT
Motorola’s CommandCentral Vault is more than just storage, it’s true end-to-end content management. All content is securely stored, simple to manage and easy to share with judicial personnel, citizens and media. CommandCentral Vault provides all the tools necessary to streamline workflows. Now your agency can reduce administrative time, simplify management and provide greater transparency faster than ever.

Example: A citizen recorded altercation goes viral and the officers are accused of excessive force. After they return to the station, video is automatically uploaded without user intervention. Simplified content management allows the officers to annotate, add additional tags and mark the videos for additional review. Command staff and the public information officer are able to easily search and review the marked videos from their mobile devices and prepare them for distribution. An analyst using auto-redaction quickly edits the videos to protect the privacy of innocent individuals. Using the FCIA workflow, the agency provides the redacted video to the media within hours, showing the officers’ response was warranted and legal.

KEY USERS

Officer
Upload content, then search, review, annotate, mark, tag, clip and organize efficiently.

Detective
Easily search and review content details in a geospatial view with audit and retention control.

Records Specialist
 Expedite redaction through automation, create clips, control content, set policies and securely distribute content with ease.

Citizen
Request content through a web-based portal, make payments easily and get secured, restricted access to approved content.
FEATURES

- **Secured Content:**
  Original content is never editable and digitally signed to provide a cryptographically secure method to prove authenticity and chain-of-custody with cloud storage that meets CJJS standards.

- **Automated Redaction:**
  Eliminate tedious frame-by-frame redaction. Simply select the objects or people in a video and the redaction is applied across all frames automatically.

- **Automatic Correlation:**
  When linked to your CAD system or RMS, CommandCentral Vault can automatically correlate related evidence from external systems and group them in case folders to reduce administrative overhead searching for content (requires Manage module).

- **Complete Auditing:**
  Every action taken on stored content is tracked for greater transparency and accountability.

- **Evidence Sharing:**
  Customizable, easy-to-understand forms and workflows are available to distribute content to judicial personnel as well as citizens and media (requires Judicial or FOIA module).

- **Geospatial Video Review:**
  Integrated maps with geotagged locations of recorded content allows for simplified content review.

- **CommandCentral Integration:**
  Metadata stored in CommandCentral Vault can be reused in other CommandCentral applications to increase actionable intelligence.

- **Retention Policies:**
  Flag evidence to prevent deletion and retain content for different lengths based on incident type, capture date and case association based on your agency’s policies.

AVAILABLE MODULES

**Store**
The Store module is the baseline package provided for CommandCentral Vault and is offered on a per user license basis.

- Store users can seamlessly upload content into secure cloud storage that meets CJJS standards.
- It provides the following additional capabilities:
  - Annotate images and video during review
  - Automatic association of stored content with CAD/RMS data
  - Review content and associated metadata with geospatial mapping playback
  - Chain of custody controls to preserve and verify original content
  - Mark content to adhere to retention policies

**Manage (Optional)**
In addition to Store capabilities you receive:
- Agency-wide content search for permitted users
- Enhanced review functionality with playback speed controls
- Additional administrative content restriction controls
- Automated redaction based on facial and/or object recognition

**Judicial (Optional)**
In addition to Store capabilities you receive:
- The ability to create video clips of specific evidence related to a judicial request
- The ability to restrict access based on permissions
- Secure links to requested content to maintain chain of custody
- Automated redaction based on facial and/or object recognition

**FOIA (Optional)**
In addition to Store capabilities you receive:
- A secure, agency-branded web portal to enable FOIA requests from the public
- The ability to collect payments for FOIA requests
- The ability to tailor customizable workflow forms to your agency needs
- Automated redaction based on facial and/or object recognition

PREDICTABLE COSTS
CommandCentral Vault provides your agency with simplified, predictable pricing to easily plan and budget expenses for a body-worn camera (BWC) program.

As a cloud-based application, there is no complex integration or need for infrastructure and additional IT administrative overhead.

Monthly subscription costs are based on the number of BWC users and role-based access is available to all agency personnel at no additional cost.

DIGITAL EVIDENCE MANAGEMENT SOLUTION
CommandCentral Vault, when combined with the S/300 or S/500 video speaker microphone, creates a complete digital evidence management solution.

The combined solution features wireless upload and automatic metadata correlation to simplify content management and reduce administrative overhead.

With intuitive and intelligent software automating actions for personnel in the street and back office, this end-to-end solution is paving the way for a new era in digital evidence management. Learn more at www.motorolasolutions.com/dems

For more information about CommandCentral Vault, contact your Motorola representative or visit motorolasolutions.com/commandcentralvault

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2016 Motorola, Inc. All rights reserved 05-2016
### 5.1 PRICING

**PRICING SUMMARY:**
- Five (5) Year Contract, CommandCentral Vault
- 15TB of storage for the 5 year term
- Integration with PremierOne CAD/RMS

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSRP</td>
<td>$201,000</td>
</tr>
<tr>
<td>System Discount</td>
<td>($59,400)</td>
</tr>
<tr>
<td><strong>Grand Total System Price</strong></td>
<td><strong>$141,600</strong></td>
</tr>
</tbody>
</table>

### 5.2 PAYMENT TERMS

**PAYMENT SCHEDULE:**

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount</th>
<th>Payment Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upfront Costs for development &amp; implementation - Year 1</td>
<td>$21,000</td>
<td>Net 30 days from Contract Execution</td>
</tr>
<tr>
<td>Annual Subscription Fee - Year 1</td>
<td>$24,120</td>
<td>Net 30 days from Contract Execution</td>
</tr>
<tr>
<td>Annual Subscription Fee - Year 2</td>
<td>$24,120</td>
<td>Each Anniversary of Contract Execution</td>
</tr>
<tr>
<td>Annual Subscription Fee - Year 3</td>
<td>$24,120</td>
<td>Each Anniversary of Contract Execution</td>
</tr>
<tr>
<td>Annual Subscription Fee - Year 4</td>
<td>$24,120</td>
<td>Each Anniversary of Contract Execution</td>
</tr>
<tr>
<td>Annual Subscription Fee - Year 5</td>
<td>$24,120</td>
<td>Each Anniversary of Contract Execution</td>
</tr>
<tr>
<td><strong>Grand Total System Price</strong></td>
<td><strong>$141,600</strong></td>
<td></td>
</tr>
</tbody>
</table>
RESOLUTION NO. 15-1783
DECEMBER 22, 2015

RESOLUTION AUTHORIZING AN AGREEMENT WITH MOTOROLA SOLUTIONS INC. FOR THE PURCHASE OF PUBLIC SAFETY SOFTWARE SOLUTIONS FOR THE MONTGOMERY COUNTY SHERIFF’S OFFICE AND A TEN YEAR MAINTENANCE AGREEMENT AT A COST NOT TO EXCEED $7,180,429.00 THROUGH DECEMBER 31, 2025.

2016 FUNDING SOURCES FOR THE PURCHASE OF SOFTWARE & EQUIPMENT IN THE AMOUNT OF $3,218,402.00: CE600156
DEPT 36, S$580,557.00, OCA 236351, OBJ 3 9105
DEPT 36, S$618,801.00, OCA 236351, OBJ 3 9110
DEPT 36, S$180,642.00, OCA 236351, OBJ 3 9135
DEPT 04, S$427,902.00, OCA 404201, OBJ 3 9135
DEPT 36, S$209,404.00, OCA 436100, OBJ 3 9105
DEPT 36, S$402,254.00, OCA 436100, OBJ 3 9110
DEPT 36, S$607,837.00, OCA 436100, OBJ 3 9135
DEPT 36, S$191,005.00, OCA 436100, OBJ 3 7195

WHEREAS, Resolution No. 15-1496, dated October 27, 2015, authorized the Purchasing Director to Request Proposals for Public Safety Software Solutions (SO500037); and

WHEREAS, the Purchasing Department and Sheriff’s Office recommend that said Agreement be awarded to Motorola Solutions Inc.

WHEREAS, this agreement outlines annual maintenance for a period of 10 years in an amount not to exceed $3,962,027.00 as stated in Exhibit B-1 of the agreement.

WHEREAS, this purchase was approved by the Automatic Data Processing Board on December 9, 2015.

NOW, THEREFORE, BE IT RESOLVED that the Resolution authorizing an agreement with Motorola Solutions Inc. for the purchase of public safety software solutions and a 10 year maintenance agreement in an amount not to exceed $7,180,429.00 through December 31, 2025 be and is hereby approved.

BE IT FURTHER RESOLVED that the Clerk of Commission certify this Resolution and make an imaged copy of this Resolution available on the Montgomery County, Ohio website at http://www.mcohio.org.
### 1.10.3 Additional Mobile (10) Client Licenses

<table>
<thead>
<tr>
<th>Mobile Licenses, Quantity 10</th>
<th>$14,740</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Additional Mobile Licenses (10) Standard Maintenance Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Year 1</td>
<td>Warranty</td>
</tr>
<tr>
<td>Year 2</td>
<td>$2,500</td>
</tr>
<tr>
<td>Year 3</td>
<td>$2,588</td>
</tr>
<tr>
<td>Year 4</td>
<td>$2,678</td>
</tr>
<tr>
<td>Year 5</td>
<td>$2,772</td>
</tr>
<tr>
<td>Year 6</td>
<td>$2,869</td>
</tr>
<tr>
<td>Year 7</td>
<td>$2,969</td>
</tr>
<tr>
<td>Year 8</td>
<td>$3,073</td>
</tr>
<tr>
<td>Year 9</td>
<td>$3,181</td>
</tr>
<tr>
<td>Year 10</td>
<td>$3,292</td>
</tr>
</tbody>
</table>

### 1.10.4 Command Central Analytics

<table>
<thead>
<tr>
<th>Users Conference</th>
<th>$191,005</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Central Analytics and Social Monitor</strong></td>
<td></td>
</tr>
<tr>
<td>Initial Five (5) year, Regional subscription to the Command Central Analytics, SocialMonitor as well as CrimeReports.Com and Camera Registration Public engagement tools. These powerful tools will be provided with the purchase of PremierOne CAD, Mobile and RMS. The subscription is provided for the RDC's entire customer base.</td>
<td></td>
</tr>
</tbody>
</table>
1.1 MOTOROLA SOLUTIONS PACKAGE OFFERS:

- Command Central Vault: a secure, CJIS compliant cloud based solution consisting of the following:
  - CommandCentral Store: Be confident that your data is securely stored and protected from system failures.
  - CommandCentral Manage: Handle all aspects of your digital evidence.
  - CommandCentral Judicial: Share evidence online with your judicial partners.
  - Built-in Redaction of all video content managed by CommandCentral Vault.
  - Ability to import third-party open source digital media evidence and make it part of your chain of custody such as CCTV, social media videos, PDF’s and any content in MP4, JPEG, MP3, PNG, H.264, AAC, GIF, and BMP format.
  - Unlimited Vault user accounts, allowing chain of custody to never be broken as officers leave your agency.
- Storage as quoted (1TB, 5TB, 10TB, 25TB or 50TB)

1.2 COMMANDCENTRAL VAULT

CommandCentral Vault is a cloud-based content management solution to securely store, review, manage, and share all forms of digital evidence. It provides a single place to aggregate evidence from multiple sources such as fixed video, social media, body worn cameras (such as the Si500), in-car camera (such as the Sr600), audio notes and other multimedia sources. Supporting both automatic and manual uploads combined with end-to-end streamlined content management enables agencies to simplify workflows and the overhead of dealing with increasing amounts of content.

1.2.1 SIMPLIFIED STORAGE

Multimedia stored in CommandCentral Vault can be automatically tagged and grouped with associated events from Central Dispatch Agency’s CAD and further associated to a record ID or case within your RM system. This will dramatically reduce manual administrative workload from the staff as compared to other systems where you would have to enter in this information manually.

1.2.2 SECURITY COMPLIANCE

CommandCentral Vault utilizes Amazon Web Services (AWS) Gov-Cloud as our cloud service provider partner. AWS complies with CJIS standards, and hosted within Country. Data never crosses the border. The CommandCentral Vault content repository is built on Adobe AEM which has received Federal Risk and Authorization Management Program (FedRAMP) Certification.

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is mandatory for Federal Agency cloud deployments and service models at the low and moderate risk impact levels. Numerous government agencies and other entities that provide systems integration and other products and services to governmental agencies are using this same wide-range of AWS FedRAMP services that are incorporated into our CommandCentral Vault evidence manager.

Motorola Solutions recognizes that when you place data in the cloud it puts an absolute priority on timely and secure access to information, wherever and whenever it is needed.
To meet these needs, the CommandCentral Vault cloud infrastructure has been architected to be one of the most flexible and secure cloud computing environments available for storing criminal justice information.

Allowing easy and secure access from within City IT infrastructure. Our architecture provides an extremely scalable, highly reliable platform enabling you to deploy CommandCentral Vault quickly and securely in support of a wide variety of security and regulatory requirements, to include CJIS workflows according to the CJIS Security Policy (CJISD-ITS-DOC-08140-5.4).

Motorola Solutions complies with the FBI’s CJIS standard. Motorola Solutions along with our partner AWS, will sign the CJIS security agreements (CJISD-ITS-DOC-08140-5.4), including allowing or performing any required employee background checks according to the CJIS Security Policy. We will continually support any changes to The Security Addendum requirements as we assume there may be future security requirement changes.

1.2.3 AUTOMATED CAD DATA CORRELATION

Automated Data Correlation: CommandCentral Vault and PremierOne/Spillman Flex CAD/RMS

When linked to PremierOne/Spillman Flex CAD or RMS, CommandCentral Vault (at no additional cost) can automatically correlate related evidence from external systems and group them in case folders to reduce administrative overhead searching for content. CommandCentral Vault has an auto-correlate feature that allows multiple sources of video and audio to be grouped together. The videos can be tied to a specific case from the CAD. Multiple files from multiple officers can be tied to a single incident.

CAD/RMS connector software can be installed on your network to automatically send data from your CAD/RMS systems to the CommandCentral cloud. The following data can be received per incident/report from the majority of CAD/RMS systems:

- ID, Type, Location, Time & Date, Associated Officer Names, & Associated Officer IDs

This information is then correlated and associated automatically to files in CommandCentral Vault, saving officers time in the field.

Links to digital files stored in CommandCentral Vault can be automatically added to Flex Records case folders. Likewise, file attachments currently stored in Flex Records can be stored in CommandCentral Vault. Providing these connectors for customers using Motorola Solutions Flex CAD/RMS products is standard, and provided at no additional cost.

Further, Motorola Solutions is the ONLY vendor who can offer one integrated approach to the Smart Command Center, from initial Citizen Engagement, 911 call taking, Land Mobile Radio and FirstNet Dispatch, CAD/RMS, Evidence and Analysis.
# CommandCentral Vault Key Features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CJIS-capable via AWS GovCloud.</td>
<td>Review content and associated metadata with geospatial mapping playback.</td>
</tr>
<tr>
<td>Automated redaction, eliminating tedious frame-by-frame process.</td>
<td>Chain of custody controls to preserve and verify original content.</td>
</tr>
<tr>
<td>Dynamic watermarking to prevent unauthorized screen capturing and sharing.</td>
<td>Mark content to adhere to retention policies.</td>
</tr>
<tr>
<td>Secure chain of custody with cryptographically signed content, preventing manipulation.</td>
<td>GPS Visualization of all evidence as video is played back and reviewed, second by second.</td>
</tr>
<tr>
<td>Role-based access.</td>
<td>Command Central Vault has simple language query that can reference any data field or a combination of fields. All content uploaded has META data attached to it which enables filter/search/sort/groupings in a hierarchical way that is fit for the needs of the particular user. As this data is sensitive granular audit logs provide traceability to all actions taken on the content including but not limited to view, share, download, , creating clips, adding annotations, adding metadata tags etc.</td>
</tr>
<tr>
<td>Advanced end-to-end content management: capture, review, manage, and share.</td>
<td>Agency-wide content search for permitted users.</td>
</tr>
<tr>
<td>Annotate images and video to provide additional context during review.</td>
<td>Enhanced review functionality with playback speed controls.</td>
</tr>
<tr>
<td>Automated redaction based on object recognition.</td>
<td>Automatic association of stored content with CAD/RMS data to group related case files and provide faster search for case related content.</td>
</tr>
</tbody>
</table>
1.2.4 SIMPLE SHARING

CommandCentral Vault–Judicial Module

With the Judicial module, you can rapidly share evidence and other content with legal personnel reducing administrative overhead and delays. With the Judicial module, your agency is provided all the capabilities of the Store and Manage modules, including:

- Creating video clips to provide specific evidence related to a judicial request.
- Restricted distribution to ensure only permitted individual have access to necessary content.
- Secure links to requested content to maintain chain of custody.

1.2.5 REDACTION

CommandCentral Vault supports an automated redaction capability to facilitate the processing of digital evidence prior to release pursuant to a public information request. Utilizing “object tracking” technology, a FOIA/FOIL compliance officer can easily obscure the identity of juveniles, domestic battery and sexual battery or undercover police officers that are included in the initial evidence capture. CommandCentral Vault ensures end-to-end security of stored content, and original content is never edited to reduce challenges to the chain of custody. Full auditing allows your agency to track all activity on content from the moment it’s stored and classified.

1.2.6 SIX KEY FUNCTIONS OF OUR COMMANDCENTRAL VAULT OFFER

- **END-TO-END CONTENT MANAGEMENT**
  - Powerful, simple workflows to capture, store, manage, and share

- **END-TO-END SECURITY**
  - Digital-borne content ensures cryptographically secure verification of authenticity with storage that meets FIPS standards

- **AUTOMATED REDACTION**
  - Eliminate tedious frame-by-frame redaction
  - Select object person and process across entire video

- **AUTO-CORRELATE METADATA**
  - Link to CAD and RMS data minimizing administrative overhead

- **CHAIN OF CUSTODY**
  - Prevent tampering and editing. Track all activity with full auditing capability

- **EVIDENCE SHARING**
  - Simplify and reduce time to fulfill requests with customizable, easy-to-understand forms and workflows
1.2.7 COMMANDCENTRAL PORTFOLIO

CommandCentral Vault is just one application in the greater Intelligence Lead CommandCentral Portfolio. CommandCentral makes it easy to interpret vast amounts of data for planning, operational support, investigations and content collection. Make your agency more effective, without adding headcount, through a robust suite of purpose-built applications that adapt to your workflows.

Pre-defined dashboards and data visualizations help to quickly uncover information in a few clicks and automatic alerting and reporting make applications simple enough for anyone in the department to use. Geospatially plotted data also provides another way applications make digesting information quick and easy to aid in pre-, mid-, or post-incident activities, whether from the command center or in the field.
SECTION 2

KEY DIFFERENTIATORS

2.1 COMMANDCENTRAL VAULT ADVANTAGES

- Command Central Vault is an part of the CommandCentral Suite of Intelligent Lead Policing applications:
  - CommandCentral Analytics: Easily turn strategic planning into measurable action by automating advanced data analysis.
  - CommandCentral Aware: Better support real-time operations from the command center by combining voice, data and video into a single, integrated position.
  - CommandCentral Inform: Enhance decision making across your entire operation by consolidating real-time event data into one, map-based view.
  - CommandCentral Vault: Minimize administrative time wasted with a complete workflow to store, manage and share digital records and content.

- CommandCentral Vault's redaction quality and the speed are best in the industry.
  CommandCentral Vault is capable of redacting 60 minutes of video in 90 minutes, while others take 4 hours. That saves 3 hours and a half of work on one video.

- Seamless integration with Motorola Solution's TipSubmit storing all multimedia related with the tips provided through the TipSubmit application (video, voice, pictures, and messages).

- The data lake for the whole SPSS portfolio, having all the data stored in one repository (CommandCentral Aware, CommandCentral Inform, CAD, RMS, Responder Alert). Meaning that there will be one repository for all the data stored in an agency. This is not yet available but it will come in the near future (road mapped). This integration of data will allow agencies to perform a seamless workflow, instead of having many silo'd systems.

- Ability to work with non-proprietary file formats: CommandCentral Vault supports all non-proprietary file formats. If a codec is provided, Vault can even work with proprietary file formats.

- Ability to import/store 3rd party, non-proprietary digital data such as CCTV surveillance video systems, Digital audio (911 calls, wiretaps, and surveillance audio), Digital video interrogation, Digital images (photos, scanned film/prints), Body worn cameras, smartphone and In-car video.

- Administrators can define an unlimited amount of tags within CommandCentral Vault. While tags can be pre-defined, a free-form field also exists for any additional user entered metadata. Annotations can be made in reference to designated points in the video. Different users can click these annotations to jump to the corresponding point in the video.

- Ability to create and set bookmarks on videos for later reference. This bookmark will be reflected upon playback within the CommandCentral Vault.

- Video and audio files can easily be exported into standard open formats (MP4 video, AAC audio) to be easily imported into transcription software.

- Automated monitoring systems are used to provide a high level of service performance and availability. Monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. Systems are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics.
The network provides significant protection against traditional network security issues including but not limited to Distributed Denial Of Service (DDoS) Attacks, Man in the Middle (MITM) Attacks, IP Spoofing, Port Scanning and Packet sniffing.

- Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

- Retention policies can be administratively applied to different tags to automatically delete content. When applied to multimedia, the tags can define the retention policy. Evidence can be retained indefinitely when a “manual hold” is initiated by a user or by flagging the evidence for an internal investigation audit.

- Server-Side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt customer data. CommandCentral Vault is completely scalable as the solution is Cloud based.

- CommandCentral Vault features integrated role based privilege user management system. Roles and permissions can be configured to prevent or allow actions taken on video and metadata. Including but not limited to viewing, editing, annotating, downloading, redacting, sharing, clipping and adding.

- CommandCentral Vault supports Active Directory/Single Sign On (SSO) and federated directory services that use of SAML protocol. Basically, whatever your policies are for unsuccessful attempt in your IT infrastructure will be able to be carried forward to CommandCentral Vault.

- CommandCentral implements a number of security controls and 3rd party commercial scanning tools to detect anomalous behavior, advanced persistent threats, malware, viruses, and other compromises that would bypass safeguards.
SECTION 3
TRAINING

3.1 TRAINING OVERVIEW

Motorola Solutions understands that successful implementation and use of your communications system depends on effective training. We have developed a training proposal to ensure a comprehensive understanding of your proposed system and all user equipment. We are leveraging over 85 years of training experience working with customers just like you to provide recommendations for your consideration. The training proposal detailed in the following pages incorporates customer feedback coupled with a best practices systematic approach to produce effective course delivery and content.

Our commitment is to provide unsurpassed services that ensure the equipment operates efficiently for the life of the system. To do so, we directly train your personnel to utilize the system to its maximum potential.

Your personnel will gain in-depth understanding of the power of your new system through education and proficient daily use. Our high-quality training focuses on student needs. The training is complemented by detailed documentation and available continuing education programs.

We will collaborate with the department to develop a final customized training plan that fits your needs. Our goal is to insure system administrators, technicians and end users are skilled in using your new system.

3.2 TRAINING APPROACH

Our training solutions deliver a combination of online training and field based instructor-led training in classrooms at your Department locations using operational equipment. Motorola Solutions will employ knowledgeable and experienced instructors to deliver well-designed courseware and integrated lab activities.

Training is based upon several key criteria:

• Course design is driven by an analysis of student needs. It focuses on specific application rather than theory.

• Learning objectives are based upon what students need to accomplish on the job.

• Hands-on lab opportunities using specific job aids are incorporated to maximize learning and retention.

Our instructors bring invaluable experience and knowledge of customer communication solutions into their training approach. This gives them better insight and understanding into the practical aspects of your manager, technician and end user job functions. Each instructor has the proven ability to communicate with a novice as well as expert personnel.
3.3 PROPOSED COURSE

Motorola Solutions has identified the following course that is necessary to achieve your training goals.

Specifically, our proposed training plan addresses the following category:

- Vault System Administrators

3.3.1 Digital Evidence Management Software - Administrator Training Plan

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Target Audience</th>
<th>Sessions / Duration</th>
<th>Location</th>
<th>Date</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Central Vault Digital Evidence Management Solution (Instructor-led)</td>
<td>Command Central Vault System Administrators</td>
<td>1 / 2 days</td>
<td>Customer location</td>
<td>Prior to managing</td>
<td>Up to 12</td>
</tr>
</tbody>
</table>

Course Synopsis:
The CommandCentral Vault Field Workshop provides an in-depth learning experience for users of the CommandCentral Vault DEMS to enable them to make the most effective use of the solution. Key topics for this workshop include video management, redaction, data tagging, event correlation, and content security. Participants will learn topics through a combination of hands-on lab activities, demonstration, and discussion.

An additional section of this course adds additional content for system administrators responsible for the administration of a CommandCenter Vault solution. Key topics for this section include adding users and camera devices to vault, case type addition and modification, and other configuration tasks.