



Public Safety Committee

Wednesday, March 6, 2024 3:00PM
40 McMaster Street, Ballston Spa, NY

Chair: John Lant

Members: C. Eric Butler VC, Jesse Fish, Ian Murray, Scott Ostrander, Mo Wright, Cynthia Young

Agenda

- I. Welcome and Attendance
- II. Approval of the minutes of the February 7, 2024 meeting
- III. Authorizing the acceptance of a County Pretrial Services Grant from the New York State Division of Criminal Justice Services – Sue Costanzo, Probation
- IV. Authorizing an amendment to the agreement with Jacqueline Bashkoff PHD for the provision of expert psychological services - Andrew Blumenberg, Public Defender
- V. Michael Zurlo, Sheriff
 - a. Proclaiming April 14-20, 2024 as “Public Safety Telecommunications Week”
 - b. Authorizing an amended agreement with PrimeCare Medical of New York to include additional nursing coverage in the County Jail
- VI. Karen Heggen, District Attorney
 - a. Authorizing acceptance of a Criminal Justice Discovery Reform Grant from the New York State Division of Criminal Justice Services
 - b. Authorizing an agreement with Hugh G. Burke, Esq. for the provision of legal services pertaining to FOIL requests for the District Attorney's Office
- VII. Authorizing agreements with Motorola Solutions, Inc. – André Delvaux, Emergency Services
- VIII. Other Business
- IX. Adjournment



SARATOGA COUNTY AGENDA ITEM REQUEST

TO: Steve Bulger, County Administrator
Ridge Harris, Deputy County Administrator
George Conway, County Attorney
Therese Connolly, Clerk of the Board
Stephanie Hodgson, Director of Budget

CC: John Warnt, Director of Purchasing
Jason Kemper, Director of Planning and Economic Development
Bridget Rider, Deputy Clerk of the Board
Matt Rose, Management Analyst
Audra Hedden, County Administrator's Office
Samantha Kupferman, County Attorney's Office

DEPARTMENT: Probation Department

DATE: February 22, 2024

COMMITTEE: Public Safety

1. Is a Resolution Required:

Yes, Grant Acceptance

2. Proposed Resolution Title:

3. Specific Details on what the resolution will authorize:

Authorize the acceptance of the Saratoga County Pretrial Services Grant from the New York State Division of Criminal Justice Services in an amount up to \$415,738.00.

This column must be completed prior to submission of the request.

County Attorney's Office
Consulted Yes

4. Is a Budget Amendment needed: YES or NO
 If yes, budget lines and impact must be provided.
 Any budget amendments must have equal and offsetting entries.

County Administrator's Office
 Consulted Yes

Please see attachments for impacted budget lines.
 (Use ONLY when more than four lines are impacted.)

Revenue

Account Number	Account Name	Amount

Expense

Account Number	Account Name	Amount

Fund Balance (if applicable): (Increase = additional revenue, Decrease = additional expenses)

Amount:

5. Identify Budget Impact (**Required**):

No Budget Impact. Funds are included in the Department Budget

- a. G/L line impacted A.31-3880 Alt Incarc Pre Trial
- b. Budget year impacted 2023/2024
- c. Details

6. Are there Amendments to the Compensation Schedule?

YES or NO (If yes, provide details)

a. Is a new position being created? Y N

Effective date

Salary and grade

b. Is a new employee being hired? Y N

Effective date of employment

Salary and grade

Appointed position:

Term

c. Is this a reclassification? Y N

Is this position currently vacant? Y N

Is this position in the current year compensation plan? Y N

Human Resources Consulted

7. Does this item require the awarding of a contract: Y N

a. Type of Solicitation

b. Specification # (BID/RFP/RFQ/OTHER CONTRACT #)

c. If a sole source, appropriate documentation, including an updated letter, has been submitted and approved by Purchasing Department? Y N N/A

d. Vendor information (including contact name):

e. Is the vendor/contractor an LLC, PLLC, or partnership:

f. State of vendor/contractor organization:

g. Commencement date of contract term:

h. Termination of contract date:

i. Contract renewal date and term:

k. Is this a renewal agreement: Y N

l. Vendor/Contractor comment/remarks:

Purchasing Office Consulted

County Administrator's Office
Consulted

8. Is a grant being accepted: YES or NO

a. Source of grant funding:

State

b. Agency granting funds:

New York State Division of Criminal Justice Services

c. Amount of grant:

\$415,738.00

d. Purpose grant will be used for:

Pretrial Services

e. Equipment and/or services being purchased with the grant:

Laptops, Monitors, Leadwell Training

f. Time period grant covers:

New York State Fiscal Year 2023-2024

g. Amount of county matching funds:

None

h. Administrative fee to County:

None

9. Supporting Documentation:

Marked-up previous resolution

No Markup, per consultation with County Attorney

Information summary memo

Copy of proposal or estimate

Copy of grant award notification and information

Other _____

10. Remarks:

11/15/22



SARATOGA COUNTY BOARD OF SUPERVISORS

RESOLUTION 318 - 2022

Butler Fish Murray

Introduced by Public Safety: Supervisors Lant, ~~Barrett, Hammond, Lawler,~~
Ostrander, ~~K. Veitch~~ and Wright
Young

AUTHORIZING THE ACCEPTANCE OF A COUNTY PRETRIAL SERVICES GRANT FROM THE NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES

WHEREAS, pursuant to Resolution 110-2022, this Board authorized the approval of our current Alternatives to Incarceration (ATI) Performance-Based Service Plan through June 30, 2023, and the acceptance of funding from the NYS Division of Criminal Justice Services' Office of Probation and Correctional Alternatives; and

WHEREAS, the NYS Division of Criminal Justice Services has allocated additional funding for County Pretrial Services in the amount of ~~\$409,280~~ for the period of April 1, ~~2022~~ 2023 through March 31, ~~2023~~ and
2024 415,738

WHEREAS, acceptance of the County Pretrial Services grant from the State Division of Criminal Justice Services' Office of Probation and Correctional Alternatives requires this Board's approval; now, therefore, be it

RESOLVED, that the Chairman of the Board is authorized to execute all necessary documents and agreements with New York State Division of Criminal Justice Services' Office of Probation and Correctional Alternatives for the acceptance of the County Pretrial Services grant in the amount of ~~\$409,280~~ for the period April 1, ~~2022~~ through March 31, ~~2023~~; and it is further
415,738 2023 2024

RESOLVED, that the form and content of such documents shall be subject to the approval of the County Attorney; and it is further

RESOLVED, that this Resolution shall take effect immediately.

BUDGET IMPACT STATEMENT: No Budget Impact.

November 15, 2022 Regular Meeting
Motion to Adopt: Supervisor Hammond
Second: Supervisor Butler

AYES (194440): Joseph Grasso (4328), Philip C. Barrett (19014.5), Jonathon Schopf (19014.5), Eric Butler (6500), Diana Edwards (819), Jean Raymond (1333), Michael Smith (3525), Kevin Tollisen (25662), Mark Hammond (17130), Thomas Richardson (5163), Scott Ostrander (18800), Theodore Kusnierz (16202), Sandra Winney (2075), Tara N. Gaston (14245.5), Matthew E. Veitch (14245.5), Edward D. Kinowski (9022), John Lant (17361).

NOES (0):

ABSENT (41069): Eric Connolly (11831), Kevin Veitch (8004), Arthur M. Wright (1976), Willard H. Peck (5242), Thomas N. Wood, III (5808), John Lawler (8208)



KATHY HOCHUL
Governor

ROSSANA ROSADO
Commissioner

CILLIAN FLAVIN
Deputy Commissioner, Program
Development and Funding

Grant Award Notice

December 20, 2023

Hon. Theidore Kusnierz
Chairman, Board of Supervisors

The New York State Division of Criminal Justice Services (DCJS) is pleased to advise you that your county will receive funding to offset the costs associated with the provision of certified pretrial services, including but not limited to screening, assessment, supervision, and reporting as provided in the enacted (SFY 2023-24) New York State budget. The funding provided to the county herein must be used to support certified pretrial services. Pursuant to Criminal Procedure Law § 510.45, the Office of Court Administration certifies one or more pretrial services agencies in each county and maintains a listing of such agencies on their public website at: <https://ww2.nycourts.gov/court-research/ListOfAgencies.shtml>.

Project Name:	Saratoga County Pretrial Services	Award Amount:	\$ 415,738.00
----------------------	--	----------------------	----------------------

Additional Information:

Your 2023-24 award is consistent with the appropriation amount enacted for this purpose in the State budget and was determined based on an analysis of the five-year average of lower court arraignments in your county. Rather than issuing your grant award through a DCJS grant contract for this funding, the full award amount will be automatically disbursed to the county in one payment.

DCJS requests that your county’s certified pretrial services agency or agencies submit a Pretrial Services spending overview within 60 days of receiving the award. Attached to this letter is a form that DCJS requests agencies use in submitting the spending overview.

Should you have any programmatic questions, please contact Nicole Aldi, Program Manager, DCJS Office of Probation and Correctional Alternatives at (518) 485-8457 or nicole.aldi@dcjs.ny.gov. If you have any fiscal questions, please contact the DCJS Finance Office at (518) 457-6105 or dcjsGrantsUnitVoucherInquiry@dcjs.ny.gov.

Attachment: Pretrial Services Funding Overview

CC: Robert M. Maccarone, Deputy Commissioner and Director of Probation
Sue Costanzo, Probation Director



SARATOGA COUNTY AGENDA ITEM REQUEST

TO: Steve Bulger, County Administrator
Ridge Harris, Deputy County Administrator
George Conway, County Attorney
Therese Connolly, Clerk of the Board
Stephanie Hodgson, Director of Budget

CC: John Warnt, Director of Purchasing
Jason Kemper, Director of Planning and Economic Development
Bridget Rider, Deputy Clerk of the Board
Matt Rose, Management Analyst
Audra Hedden, County Administrator's Office
Samantha Kupferman, County Attorney's Office

DEPARTMENT: Public Defender

DATE: 2/26/24

COMMITTEE: Public Safety

1. Is a Resolution Required:

Yes, Contract Amendment

2. Proposed Resolution Title:

To amend Resolution 146-2015 and authorize an amended agreement with Dr. Jacqueline Bashkoff PH.D. for the provision of expert psychological services to assist the Public Defenders Office in Representation of our clients in Criminal and Family Courts.

3. Specific Details on what the resolution will authorize:

To amend Dr. Bashkoff's 2023 contract from \$20,000 to \$55,000 to automatically be renewed annually so amendments need not to be done in the future effective 2024.

This column must be completed prior to submission of the request.

County Attorney's Office
Consulted

4. Is a Budget Amendment needed: YES or NO
If yes, budget lines and impact must be provided.
Any budget amendments must have equal and offsetting entries.

County Administrator's Office
Consulted No

- Please see attachments for impacted budget lines.
(Use ONLY when more than four lines are impacted.)

Revenue

Account Number	Account Name	Amount
----------------	--------------	--------

Expense

Account Number	Account Name	Amount
----------------	--------------	--------

Fund Balance (if applicable): (Increase = additional revenue, Decrease = additional expenses)

Amount:

5. Identify Budget Impact (**Required**):

No Budget Impact. Funds are included in the Department Budget

- a. G/L line impacted A.26.000-8111
- b. Budget year impacted 2024
- c. Details

6. Are there Amendments to the Compensation Schedule?

YES or NO (If yes, provide details)

a. Is a new position being created? Y N

Effective date

Salary and grade

b. Is a new employee being hired? Y N

Effective date of employment

Salary and grade

Appointed position:

Term

c. Is this a reclassification? Y N

Is this position currently vacant? Y N

Is this position in the current year compensation plan? Y N

Human Resources Consulted

7. Does this item require the awarding of a contract: Y N

a. Type of Solicitation

b. Specification # (BID/RFP/RFQ/OTHER CONTRACT #)

c. If a sole source, appropriate documentation, including an updated letter, has been submitted and approved by Purchasing Department? Y N N/A

d. Vendor information (including contact name):

e. Is the vendor/contractor an LLC, PLLC, or partnership:

f. State of vendor/contractor organization:

g. Commencement date of contract term:

h. Termination of contract date:

i. Contract renewal date and term:

k. Is this a renewal agreement: Y N

l. Vendor/Contractor comment/remarks:

Purchasing Office Consulted

County Administrator's Office
Consulted

8. Is a grant being accepted: YES or NO

- a. Source of grant funding:
- b. Agency granting funds:
- c. Amount of grant:
- d. Purpose grant will be used for:
- e. Equipment and/or services being purchased with the grant:
- f. Time period grant covers:
- g. Amount of county matching funds:
- h. Administrative fee to County:

9. Supporting Documentation:

- Marked-up previous resolution
- No Markup, per consultation with County Attorney
- Information summary memo
- Copy of proposal or estimate
- Copy of grant award notification and information
- Other _____

10. Remarks:

We have had to amend Dr. Bashkoff's contract the last few years as she has gone over her contract amount, as the Judges in Family Court are ordering that the Public Defender's Office pay for indigent clients psychological services in custody hearings.



SARATOGA COUNTY BOARD OF SUPERVISORS

RESOLUTION 146 - 2015

Introduced by Supervisors ~~Barrett, Allen, Johnson, Lent, Peek, Wright and Ziegler~~ *Lent, Butler, Fish, Murray, Ostrander, Young*

AUTHORIZING AN AGREEMENT WITH JACQUELINE BASHKOFF, PH.D. FOR THE PROVISION OF EXPERT PSYCHOLOGICAL SERVICES TO ASSIST THE PUBLIC DEFENDER'S OFFICE IN THE REPRESENTATION OF THEIR CLIENTS

WHEREAS, Article 18B of the County Law requires counties to supply counsel, investigators, expert and other services to persons charged with a crime or involved in a Family Court proceeding unable to obtain these services; and

WHEREAS, from time to time our Public Defender's Office requires expert psychological services to assist in the representation of persons who are financially unable to obtain these services; and

WHEREAS, the County entered into an existing minor contract with Jacqueline Bashkoff, Ph.D. on October 16, 2013 for the provision of psychological services to assist in the representation of clients of the Public Defender's Office; and

WHEREAS, due to an increased need for Dr. Bashkoff's services in 2015, the cost of services rendered by Dr. Bashkoff this year is anticipated to exceed the minor contract limit of \$10,000 by an additional \$10,000; and

WHEREAS, the Public Defender has negotiated with Dr. Bashkoff a reduction in her hourly rates from \$175 per hour for out-of-court work to \$150 per hour, and from \$225 per hour for in-court services to \$150 per hour, effective July 1, 2015; and

WHEREAS, our Public Safety Committee has recommended that the County enter into an agreement with Jacqueline Bashkoff, Ph.D. for psychological services through December 31, 2015 at a cost not to exceed \$20,000, at the reduced hourly rate of \$150 for both in-court and out-of-court services effective as of July 1, 2015; now, therefore, be it

RESOLVED, that the Chair of the Board, or the Vice-Chair of the Board in the Chair's absence, are authorized to execute an agreement with Jacqueline Bashkoff, Ph.D. of Albany, New York, for the provision of expert psychological services to the Public Defender's Office to assist in the representation of their clients at a cost not to exceed \$20,000, for the term January 1, 2015 through December 31, 2015, subject to annual renewal, at the reduced hourly rate of \$150 for both in-court and out-of-court services effective as of July 1, 2015; and, be it further

RESOLVED, that the form and content of such agreement shall be subject to the approval of the County Attorney.

BUDGET IMPACT STATEMENT: No budget impact.



SARATOGA COUNTY AGENDA ITEM REQUEST

TO: Steve Bulger, County Administrator
Ridge Harris, Deputy County Administrator
George Conway, County Attorney
Therese Connolly, Clerk of the Board
Stephanie Hodgson, Director of Budget

CC: John Warnt, Director of Purchasing
Jason Kemper, Director of Planning and Economic Development
Bridget Rider, Deputy Clerk of the Board
Matt Rose, Management Analyst
Audra Hedden, County Administrator's Office
Samantha Kupferman, County Attorney's Office

DEPARTMENT: Sheriff's Office

DATE: 28 February 2024

COMMITTEE: Public Safety

1. Is a Resolution Required:

Yes, Proclamation/Honorary Resolution

2. Proposed Resolution Title:
Proclaiming April 14 - 20, 2024 as "Public Safety Telecommunicators Week"
3. Specific Details on what the resolution will authorize:
See attached previous resolution

This column must be completed prior to submission of the request.

County Attorney's Office
Consulted **No**

4. Is a Budget Amendment needed: YES or NO
If yes, budget lines and impact must be provided.
Any budget amendments must have equal and offsetting entries.

County Administrator's Office
Consulted **No**

- Please see attachments for impacted budget lines.
(Use ONLY when more than four lines are impacted.)

Revenue

Account Number	Account Name	Amount
----------------	--------------	--------

Expense

Account Number	Account Name	Amount
----------------	--------------	--------

Fund Balance (if applicable): (Increase = additional revenue, Decrease = additional expenses)

Amount:

5. Identify Budget Impact (**Required**):

No Budget Impact

- a. G/L line impacted
- b. Budget year impacted
- c. Details

6. Are there Amendments to the Compensation Schedule?

YES or NO (If yes, provide details)

a. Is a new position being created? Y N

Effective date

Salary and grade

b. Is a new employee being hired? Y N

Effective date of employment

Salary and grade

Appointed position:

Term

c. Is this a reclassification? Y N

Is this position currently vacant? Y N

Is this position in the current year compensation plan? Y N

Human Resources Consulted

N/A

7. Does this item require the awarding of a contract: Y N

a. Type of Solicitation

b. Specification # (BID/RFP/RFQ/OTHER CONTRACT #)

Purchasing Office Consulted

N/A

c. If a sole source, appropriate documentation, including an updated letter, has been submitted and approved by Purchasing Department? Y N N/A

d. Vendor information (including contact name):

e. Is the vendor/contractor an LLC, PLLC, or partnership:

f. State of vendor/contractor organization:

g. Commencement date of contract term:

h. Termination of contract date:

i. Contract renewal date and term:

k. Is this a renewal agreement: Y N

l. Vendor/Contractor comment/remarks:

8. Is a grant being accepted: YES or NO

County Administrator's Office
Consulted NO

- a. Source of grant funding:
- b. Agency granting funds:
- c. Amount of grant:
- d. Purpose grant will be used for:
- e. Equipment and/or services being purchased with the grant:
- f. Time period grant covers:
- g. Amount of county matching funds:
- h. Administrative fee to County:

9. Supporting Documentation:

- Marked-up previous resolution
- No Markup, per consultation with County Attorney
- Information summary memo
- Copy of proposal or estimate
- Copy of grant award notification and information
- Other _____

10. Remarks:



~~3/21/23~~

SARATOGA COUNTY BOARD OF SUPERVISORS

RESOLUTION ~~85-2023~~

Introduced by Public Safety: ~~Supervisors Lant, Butler, Grasso, Hammond, Raymond, Tollisen and K. Veitch~~

14-20, 2024
PROCLAIMING APRIL ~~9-15, 2023~~ AS
"PUBLIC SAFETY TELECOMMUNICATORS WEEK"

WHEREAS, emergencies can occur at any time that require police, fire or emergency medical services; and

WHEREAS, when an emergency occurs, the prompt response of police officers, firefighters and paramedics is critical to the protection of life and preservation of property; and

WHEREAS, the safety of our police officers, firefighters and paramedics is dependent upon the quality and accuracy of information obtained from citizens who contact the Saratoga County Sheriff's Office Communications Division; and

WHEREAS, public safety telecommunicators are the first and most critical contact our citizens have with emergency services; and

WHEREAS, public safety telecommunicators are the single vital link for our police officers, firefighters, and paramedics by monitoring their activities by radio, providing them information and ensuring their safety; and

WHEREAS, public safety telecommunicators of the Saratoga County Sheriff's Office have contributed substantially to the apprehension of criminals, suppression of fires and treatment of those in need of medical care; and,

WHEREAS, each telecommunicator of the Saratoga County Sheriff's Office has exhibited compassion, understanding and professionalism during the performance of their job during the ~~157,975~~ calls for service handled during ~~2022~~; now, therefore, be it

170,380 *2023*
RESOLVED, that the Saratoga County Board of Supervisors hereby proclaims the week of April ~~9-15, 2023~~ *14-20, 2024* as "Public Safety Telecommunicators Week" in Saratoga County, in honor of the men and women of the Saratoga County Sheriff's Office Communications Division, whose diligence and professionalism keep us safe.

BUDGET IMPACT STATEMENT: No Budget Impact.



SARATOGA COUNTY AGENDA ITEM REQUEST

TO: Steve Bulger, County Administrator
Ridge Harris, Deputy County Administrator
George Conway, County Attorney
Therese Connolly, Clerk of the Board
Stephanie Hodgson, Director of Budget

CC: John Warnt, Director of Purchasing
Jason Kemper, Director of Planning and Economic Development
Bridget Rider, Deputy Clerk of the Board
Matt Rose, Management Analyst
Audra Hedden, County Administrator's Office
Samantha Kupferman, County Attorney's Office

DEPARTMENT: Sheriff's Office

DATE: 02/27/2024

COMMITTEE: Public Safety



This column must be completed prior to submission of the request.

County Attorney's Office
Consulted Yes

1. Is a Resolution Required:

Yes, Contract Approval

2. Proposed Resolution Title:

Authorize the Chairman on behalf of the Sheriff to amend the contract between the County and PrimeCare Medical of New York to include additional nursing coverage in the county jail.

3. Specific Details on what the resolution will authorize:

Authorize the Chairman on behalf of the Sheriff to amend the contract between the County and PrimeCare Medical of New York to include one additional nurse for the county jail. The County entered into a contract with PrimeCare on August 1, 2022 per Resolution 231-2022 for medical and dental services for the county jail. The County entered into an amended contract with PrimeCare on January 1, 2023 per Resolution 34-2023 for the addition of behavioral health services for the county jail. The County entered into an amended contract with PrimeCare on February 1, 2024 per Resolution 337-2023 to include nursing coverage in the county jail. PrimeCare provides nursing coverage in the jail 24 hours a day, 7 days a week at a cost not to exceed \$73,697.25 per month for first, second and third shift nursing coverage from February 1, 2024 until July 31, 2024 after which rates will be determined based upon the terms of the current contract. It also covers additional nursing coverage on a per diem basis. Term of the contract is August 1, 2022 to July 31, 2025. This amendment to the contract would include one additional full-time Registered Nurse at the county jail for an additional \$9,633.33 per month. When the nursing contract was approved the County employed two full-time Registered Nurses (county employees) at the jail. One of those nurses has now transferred to another county department resulting in a shortage of one nurse at the county jail.

4. Is a Budget Amendment needed: YES or NO
 If yes, budget lines and impact must be provided.
 Any budget amendments must have equal and offsetting entries.

County Administrator's Office
 Consulted Yes

- Please see attachments for impacted budget lines.
 (Use ONLY when more than four lines are impacted.)

Revenue

Account Number	Account Name	Amount

Expense

Account Number	Account Name	Amount

Fund Balance (if applicable): (Increase = additional revenue, Decrease = additional expenses)

Amount:

5. Identify Budget Impact (**Required**):

No Budget Impact. Funds are included in the Department Budget

- a. G/L line impacted A.30.301-8349
- b. Budget year impacted 2024
- c. Details

There will be some off setting costs. One county RN position will be de-funded. The contract RN staffing with Cross Country MSN will be cancelled once Primecare has provided full nursing staff in the jail. Contract RN staffing has been budgeted for \$105,000 for 2024 in GL line A.30.301-8344.I.

6. Are there Amendments to the Compensation Schedule?

YES or NO (If yes, provide details)

a. Is a new position being created? Y N

Effective date

Salary and grade

b. Is a new employee being hired? Y N

Effective date of employment

Salary and grade

Appointed position:

Term

c. Is this a reclassification? Y N

Is this position currently vacant? Y N

Is this position in the current year compensation plan? Y N

Human Resources Consulted

Yes

7. Does this item require the awarding of a contract: Y N

a. Type of Solicitation

b. Specification # (BID/RFP/RFQ/OTHER CONTRACT #)

Purchasing Office Consulted

No

c. If a sole source, appropriate documentation, including an updated letter, has been submitted and approved by Purchasing Department? Y N N/A

d. Vendor information (including contact name):

e. Is the vendor/contractor an LLC, PLLC, or partnership:

f. State of vendor/contractor organization:

g. Commencement date of contract term:

h. Termination of contract date:

i. Contract renewal date and term:

k. Is this a renewal agreement: Y N

l. Vendor/Contractor comment/remarks:

8. Is a grant being accepted: YES or NO

County Administrator's Office
Consulted **Yes**

- a. Source of grant funding:
- b. Agency granting funds:
- c. Amount of grant:
- d. Purpose grant will be used for:
- e. Equipment and/or services being purchased with the grant:
- f. Time period grant covers:
- g. Amount of county matching funds:
- h. Administrative fee to County:

9. Supporting Documentation:

- Marked-up previous resolution
- No Markup, per consultation with County Attorney
- Information summary memo
- Copy of proposal or estimate
- Copy of grant award notification and information
- Other _____

10. Remarks:

THIRD ADDENDUM TO HEALTH SERVICES AGREEMENT

THIS ADDENDUM (“Agreement”), by and among the **COUNTY OF SARATOGA**, a municipal corporation with principal offices at 40 McMaster Street Ballston Spa, NY 12020 (the “County”) and the **SARATOGA COUNTY SHERIFF’S OFFICE**, with its address at 6010 County Farm Road, Ballston Spa, NY 12020 (Collectively, “Business Associate”), **PRIMECARE MEDICAL OF NEW YORK, INC.**, a New York business corporation, with principal offices at 3940 Locust Lane, Harrisburg, PA 17109 (hereinafter referred to as “PrimeCare”), **PROFESSIONAL CARE MEDICAL PRACTICE, P.C.**, (the “Medical P.C.”), **PROFESSIONAL CARE DENTAL SERVICES, P.C.**, (the “Dental P.C”) and **PERSONALCARE REGISTERED PROFESSIONAL NURSING, P.C.** (The “Nursing P.C.”) (The Medical P.C., Dental P.C. and Nursing P.C. herein collectively referred to as “the P.C.s”) each of which P.C. has its principal office located at 3940 Locust Lane, Harrisburg Pennsylvania 17109.

WITNESSETH

WHEREAS, the County, PrimeCare and the P.C.s entered into a contract effective August 1, 2022 (hereinafter, “Underlying Agreement”) for PrimeCare to manage and the P.C.s to provide reasonably necessary medical and dental care for inmates under the care and custody of the Saratoga County Sheriff (the “Sheriff”) at the Saratoga County Correctional Facility (the “Facility”)(the “Underlying Agreement”); and

WHEREAS, by the First Addendum to the Health Services Agreement effective August 1, 2023, Mental Health and Psychiatric Services were added to the Underlying Agreement.

WHEREAS, by the Second Addendum to the Health Services Agreement effective January 1, 2024, twenty-four hour per day Nursing Services were added to the Underlying Agreement.

WHEREAS, the County now desires to add an additional Registered Nurse (1.00 FTE) on the daylight shift to provide necessary nursing services for the inmates at the Facility.

WHEREAS, Section 7.7 of the Underlying Agreement requires that any modifications to the agreement be in writing signed by the parties.

NOW, THEREFORE, in consideration of the mutual promises and covenants herein set forth, the parties agree as follows:

- 1.1. The Underlying Agreement is amended to include one additional full-time Registered Nurse (1.00 FTE) on the daylight shift, Monday through Friday.
- 1.2. Monthly compensation for the additional NY licensed Registered Nurse position due Personalcare Registered Professional Nursing P.C. shall be \$9,633.33, consistent with the terms set forth by the Second Addendum. Such compensation shall be pro-rated in the first month of this Addendum, based upon the day on which services are first provided.
- 1.3. The effective date of this Addendum shall be February 19, 2024.
- 1.4. All other terms and conditions of the Underlying Agreement remain unchanged and are in full force and effect for the remaining term of the Underlying Agreement.

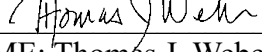
SIGNATURE PAGE TO FOLLOW

IN WITNESS WHEREOF, the parties have caused their duly authorized representatives to enter into this Agreement as of the dates set forth below, effective as of the commencement date set forth in Section 1.3 above.

Saratoga County Sheriff's Office

By: _____
NAME: Michael H. Zurlo
TITLE: Sheriff
DATE: _____

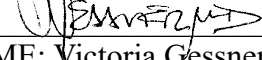
PrimeCare Medical Of New York, Inc.

By:  _____
NAME: Thomas J. Weber, Esq.
TITLE: Chief Executive Officer
DATE: 02/09/2024

County of Saratoga

By: _____
NAME: Phillip Barrett
TITLE: Chairman of the Board of Supervisors
DATE: _____
Per Resolution: _____

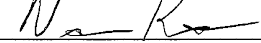
Professional Medical Practice P.C.

By:  _____
NAME: Victoria Gessner, M.D.
TITLE: President
DATE: 02/09/2024


Approved as to Form and Content:

County Attorney

Professional Dental Services P.C.

By:  _____
NAME: Nathan Kalteski, D.D.S.
TITLE: President
DATE: 02/09/2024

Personalcare Registered Professional Nursing, P.C.

By:  _____
NAME: Todd W. Haskins, R.N., BSN
TITLE: President
DATE: 02/09/2024



BOARD OF SUPERVISORS

12/19/2023

RESOLUTION ~~337-2023~~

Introduced by Public Safety: Supervisors Lant, Butler, Fish, Murray, Ostrander, Wright, and Young~~Grasso, Hammond, Raymond, Tollisen and K. Veiteh~~

AUTHORIZING AN AMENDED AGREEMENT WITH PRIMECARE MEDICAL OF NEW YORK, INC., PROFESSIONAL CARE MEDICAL PRACTICE, P.C., PROFESSIONAL CARE DENTAL SERVICES, P.C., AND PERSONALCARE REGISTERED PROFESSIONAL NURSING, P.C. FOR THE PROVISION OF NURSING SERVICES AT THE SARATOGA COUNTY CORRECTIONAL FACILITY

WHEREAS, pursuant to Resolution 231-2022, this Board authorized the execution of a three (3) year agreement with Prime Care Medical of New York, Inc., Professional Care Medical Practice, P.C., and Professional Care Dental Services, P.C., (Prime Care) to provide medical and dental services to inmates; and Resolution 34-2023, authorized an amended contract with Prime Care to provide Behavioral Health Services at the Saratoga County Jail; and Resolution 337-2023, authorizing an amended contract with PrimeCare to provide 24 Hour nursing services at the Saratoga County Jail; and these services are subject to an annual cost increase, based on the preceding 12-month U.S. Cost-of-Living index or 3%, whichever is higher; and the current contract will continue through July 31, 2025; and is subject to two (2) additional one-year renewal option periods, as mutually agreed upon by the parties in writing; and

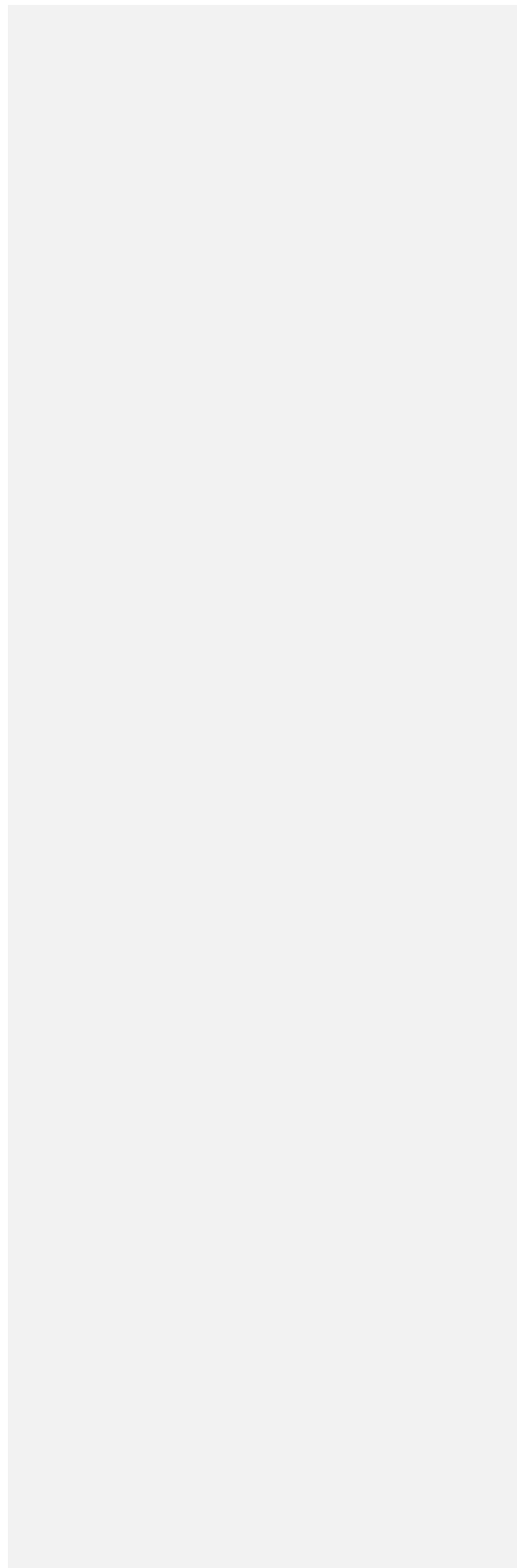
WHEREAS, our Public Safety Committee and the County Sheriff have recommended that the County enter into an amended agreement with Prime Care Medical of New York, and Personalcare Registered Professional Nursing, P.C. to provide for the addition of one full-time Registered Nurse for the Saratoga County Jail at an additional cost of \$9,633.33 per month 24-hour nursing services at the Saratoga County Jail at a monthly cost of \$73,697.25, with an additional cost of

\$45 per 8 hour shift plus the prevailing shift differential for Registered Nurses, and \$34 per 8 hour shift plus the prevailing shift differential for Licensed Practical Nurses, when County Nursing Staff utilize contractual time off; effective February 19~~1~~, 2024 through July 31, 2024, and the monthly cost, and the 8 hour shift plus prevailing shift differential, thereafter subject to an annual increase based on the preceding 12-month U.S. Cost-of-Living index or 3%, whichever is higher, for the duration of the current contract ending on July 31, 2025; and is subject to two (2) additional one-year renewal option periods, as mutually agreed upon by the parties in writing; now, therefore, be it

RESOLVED, that the Chair of the Board is authorized to execute an amended agreement with Prime Care Medical of New York, Inc., Professional Care Medical Practice, P.C., Professional Care Dental Services, P.C. and Personalcare Registered Professional Nursing, P.C. to provide for the addition of one full-time Registered Nurse for the Saratoga County Jail at an additional cost of \$9,633.33 per month 24-hour nursing services at the Saratoga County Jail at a monthly cost of \$73,697.25, with an additional cost of \$45 per 8 hour shift plus the prevailing

Formatted: Indent: First line: 0.5", Right: 0.08", Space Before: 0.05 pt

~~shift differential for Registered Nurses, and \$34 per 8 hour shift plus the prevailing shift differential for Licensed Practical Nurses, when County Nursing Staff utilize contractual time~~



~~off~~, effective February ~~19~~¹, 2024 through July 31, 2024, and the monthly cost, and the 8 hour shift plus prevailing shift differential, thereafter subject to an annual increase based on the preceding 12-month U.S. Cost-of-Living index or 3%, whichever is higher, for the duration of the current contract ending on July 31, 2025; and is subject to two (2) additional one-year renewal option periods, as mutually agreed upon by the parties in writing; and it is further

Formatted: Indent: First line: 0.5", Right: 0.1", Space Before: 0 pt

RESOLVED, that the form and content of such agreements shall be subject to the approval of the County Attorney; and it is further

RESOLVED, that this Resolution shall take effect immediately.

BUDGET IMPACT STATEMENT: No Budget Impact. Funds are included in the Department Budget.

December 19, 2023 Regular Meeting

Motion to Adopt: Supervisor Schopf

Second: Supervisor Hammond

AYES (216082): Eric Connolly (11831), Joseph Grasso (4328), Philip C. Barrett (19014.5), Jonathon Schopf (19014.5), Eric Butler (6500), Diana Edwards (819), Jean Raymond (1333), Michael Smith (3525), Kevin Veitch (8004), Arthur M. Wright (1976), Kevin Tollisen (25662), Mark Hammond (17130), Scott Ostrander (18800), Theodore Kusnierz (16202), Sandra Winney (2075), Ian Murray (5808), Tara N. Gaston (14245.5), Matthew E. Veitch (14245.5), John Lawler (8208), John Lant (17361)

NOES (0):

ABSENT (19427): Thomas Richardson (5163), Willard H. Peek (5242), Edward D. Kinowski (9022)



SARATOGA COUNTY AGENDA ITEM REQUEST

TO: Steve Bulger, County Administrator
Ridge Harris, Deputy County Administrator
George Conway, County Attorney
Therese Connolly, Clerk of the Board
Stephanie Hodgson, Director of Budget

CC: John Warnt, Director of Purchasing
Jason Kemper, Director of Planning and Economic Development
Bridget Rider, Deputy Clerk of the Board
Matt Rose, Management Analyst
Audra Hedden, County Administrator's Office
Samantha Kupferman, County Attorney's Office

DEPARTMENT: District Attorney

DATE: 2/27/24

COMMITTEE: Public Safety

1. Is a Resolution Required:

Yes, Grant Acceptance

2. Proposed Resolution Title:

Authorizing Acceptance of a Criminal Justice Discovery Reform Grant from the New York State Division of Criminal Justice Services

3. Specific Details on what the resolution will authorize:

Resolution accepting the 2023-2024 Criminal Justice Discovery Reform Grant from the New York State Division of Criminal Justice Services.

This column must be completed prior to submission of the request.

County Attorney's Office
Consulted **Yes**

4. Is a Budget Amendment needed: YES or NO
If yes, budget lines and impact must be provided.
Any budget amendments must have equal and offsetting entries.

County Administrator's Office
Consulted **Yes**

- Please see attachments for impacted budget lines.
(Use ONLY when more than four lines are impacted.)

Revenue

Account Number	Account Name	Amount
----------------	--------------	--------

Expense

Account Number	Account Name	Amount
----------------	--------------	--------

Fund Balance (if applicable): (Increase = additional revenue, Decrease = additional expenses)

Amount:

5. Identify Budget Impact (**Required**):

No Budget Impact. Funds are included in the Department Budget

- a. G/L line impacted **A.25.000.8160; Salaries and Fringe**
- b. Budget year impacted **2024**
- c. Details

6. Are there Amendments to the Compensation Schedule?

YES or NO (If yes, provide details)

a. Is a new position being created? Y N

Effective date

Salary and grade

b. Is a new employee being hired? Y N

Effective date of employment

Salary and grade

Appointed position:

Term

c. Is this a reclassification? Y N

Is this position currently vacant? Y N

Is this position in the current year compensation plan? Y N

Human Resources Consulted

No

7. Does this item require the awarding of a contract: Y N

a. Type of Solicitation

b. Specification # (BID/RFP/RFQ/OTHER CONTRACT #)

Purchasing Office Consulted

No

c. If a sole source, appropriate documentation, including an updated letter, has been submitted and approved by Purchasing Department? Y N N/A

d. Vendor information (including contact name):

e. Is the vendor/contractor an LLC, PLLC, or partnership:

f. State of vendor/contractor organization:

g. Commencement date of contract term:

h. Termination of contract date:

i. Contract renewal date and term:

k. Is this a renewal agreement: Y N

l. Vendor/Contractor comment/remarks:

Contract for maintenance of equipment/software for Office Data Systems, Inc. (iRecord); Year one of five-year contract (2024-2028) with Axon; Purchase Order for Cellebrite license.

8. Is a grant being accepted: YES or NO

County Administrator's Office
Consulted Yes

a. Source of grant funding:

State

b. Agency granting funds:

Division of Criminal Justice Services

c. Amount of grant:

\$839,465

d. Purpose grant will be used for:

To provide funding to support local district attorneys with expenses related to the implementation of discovery and pretrial reforms.

e. Equipment and/or services being purchased with the grant:

Maintenance of iRecord Digital Video/Audio Recording System; Axon Evidence.com licenses; Cellebrite license; Salary/fringe for certain DA Office positions.

f. Time period grant covers:

April 1, 2023 - March 31, 2024

g. Amount of county matching funds:

None

h. Administrative fee to County:

None

9. Supporting Documentation:

- Marked-up previous resolution
- No Markup, per consultation with County Attorney
- Information summary memo
- Copy of proposal or estimate
- Copy of grant award notification and information
- Other 2023-24 Discovery Reform Funding Plan

10. Remarks:



2/23/23

SARATOGA COUNTY BOARD OF SUPERVISORS

RESOLUTION 38 - 2023

Introduced by Public Safety: Supervisors Lant, Butler, Grasso, Hammond, Raymond, Tollisen and K. Veitch

AUTHORIZING ACCEPTANCE OF A CRIMINAL JUSTICE DISCOVERY REFORM GRANT FROM THE NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES

WHEREAS, a grant in the amount of ~~\$826,489~~ ^{\$839,465} is available from the New York State Division of Criminal Justice Services for the purpose of providing funding to support local district attorneys with expenses related to the implementation of discovery and pretrial reforms for the grant period April 1, ~~2022~~ ²⁰²³ through March 31, ~~2023~~ ²⁰²⁴; and

WHEREAS, the acceptance of this Criminal Justice Discovery Reform Grant requires our approval; now, therefore, be it

RESOLVED, that the Chair of the Board and/or the County Administrator execute all documents necessary to apply for and accept a New York State Division of Criminal Justice Services grant in the amount of ~~\$826,489~~ ^{\$839,465} to assist the District Attorney's Office with expenses related to the implementation of discovery and pretrial reforms for the grant period April 1, ~~2022~~ ²⁰²³ through March 31, ~~2023~~ ²⁰²⁴.

BUDGET IMPACT STATEMENT: No Budget Impact. Funds are included in the Department Budget.

February 23, 2023 Regular Meeting
Motion to Adopt: Supervisor Connolly
Second: Supervisor Edwards

AYES (168699): Eric Connolly (11831), Philip C. Barrett (19014.5), Diana Edwards (819), Jean Raymond (1333), Kevin Veitch (8004), Arthur M. Wright (1976), Kevin Tollisen (25662), Mark Hammond (17130), Scott Ostrander (18800), Theodore Kusnierz (16202), Sandra Winney (2075), Tara N. Gaston (14245.5), Matthew E. Veitch (14245.5), John Lant (17361)
NOES (0):



KATHY HOCHUL
Governor

ROSSANA ROSADO
Commissioner

DEAN DEFRUSCIO
Deputy Commissioner

Grant Award Notice

The Division of Criminal Justice Services (DCJS) is pleased to advise you that your county will receive funding under the State's Discovery Reform Grant Program for State Fiscal Year (SFY) 2023-24.

Table with 2 columns and 4 rows containing grant details: Grantee (Saratoga County), Date (September 28, 2023), Program Name (Criminal Justice Discovery Reform Grant), Award Amount (\$839,465), Name of Official (The Honorable Theodore Kusnierz), SFY 2023-24 dates, Email (tkusnierz@saratogacountyny.gov), and Contract # (C460158).

Criminal Justice Discovery Reform Grant - Additional Information:

DCJS is pleased to provide funding to your county to support local law enforcement agencies with expenses related to the implementation of discovery and pretrial reforms that took effect January 1, 2020. Your county's award amount has been determined based on the prorated share of 2018-2022 criminal court arraignments statewide.

This funding is contingent upon the submission by the county, and subsequent DCJS approval of, a Discovery Reform Funding Plan. Please see the attached 2023-24 Discovery Reform Application and the Discovery Reform Funding Plan for additional information. All funding provided is primarily intended to support costs incurred on or after the start of SFY 2023-24 (April 1, 2023); however, this funding may also be used to cover any costs incurred in SFY 2022-23 (April 1, 2022 to March 31, 2023).

In your county's application, the District Attorney's (DA) minimum amount must match the greatest amount that was allocated to the DA in your county's previously submitted budget to DCJS from either of the preceding years of discovery funding. If your county had not previously submitted a budget for this funding, the minimum should be calculated as 67% of the total county award amount.

The county's Discovery Reform Funding Plan should be submitted to DCJS using the DCJS Grants Management System (GMS). Additional information about GMS is provided in the attached application document. Questions about the submission of the plan should be emailed to DCJS at dcjsfunding@dcjs.ny.gov. Please include "Discovery Reform Question" in the subject line of your email.

Once plans are approved by DCJS, grantees will be notified and shall receive payment for their entire award. The county shall subsequently and promptly make this funding available to the recipient agencies (e.g., DA, probation department, sheriff's offices, local police department) within 60 days of receipt. Thank you for your continued partnership to help keep New Yorkers safe and ensure a justice system that works for all.

Attachment (2)

ATTACHMENT: 2023-24 Discovery Reform Funding Plan

Instructions: Indicate each Sub-Grantee using this attachment. If additional lines are needed, please submit additional attachments. Completed form(s) must be attached in GMS as part of the submitted Application. The total amount requested by the county cannot exceed the total county allocation provided on the award notice.

County:

Sub-Grantee	Sub-Grantee Name (if applicable):	Expense	Activities	Describe how this expenditure supports implementation of the discovery and/or bail reform efforts.
	TOTAL:			

NOTE: The total amount requested by the county cannot exceed the total county allocation provided on the award notice.



SARATOGA COUNTY AGENDA ITEM REQUEST

TO: Steve Bulger, County Administrator
Ridge Harris, Deputy County Administrator
George Conway, County Attorney
Therese Connolly, Clerk of the Board
Stephanie Hodgson, Director of Budget

CC: John Warnt, Director of Purchasing
Jason Kemper, Director of Planning and Economic Development
Bridget Rider, Deputy Clerk of the Board
Matt Rose, Management Analyst
Audra Hedden, County Administrator's Office
Samantha Kupferman, County Attorney's Office

DEPARTMENT: District Attorney

DATE: 03/01/24

COMMITTEE: Public Safety

1. Is a Resolution Required:

Yes, Contract Approval

2. Proposed Resolution Title:

Authorizing an agreement with Hugh G. Burke, Esq. to process and handle New York Freedom of Information Law (FOIL) requests for the District Attorney's Office.

3. Specific Details on what the resolution will authorize:

The resolution will authorize an agreement with Hugh G. Burke, Esq. to provide legal advice and representation with regard to the New York Freedom of Information Law (FOIL), including legal review and advice regarding the statute and preparation of materials in response to FOIL requests which involve the District Attorney. Mr. Burke currently has a minor contract with the District Attorney's Office but will exceed the \$15,000 limit quickly with the amount of work that needs to be done. Mr. Burke's services are required as we have open attorney positions in our office that we are having difficulty filling and no one else available to process the FOIL requests. He is earning \$158 per hour for the work he is providing and the major contract is not to exceed \$35,000.

This column must be completed prior to submission of the request.

County Attorney's Office
Consulted **Yes**

4. Is a Budget Amendment needed: YES or NO
 If yes, budget lines and impact must be provided.
 Any budget amendments must have equal and offsetting entries.

County Administrator's Office
 Consulted **Yes**

Please see attachments for impacted budget lines.
 (Use ONLY when more than four lines are impacted.)

Revenue

Account Number	Account Name	Amount

Expense

Account Number	Account Name	Amount

Fund Balance (if applicable): (Increase = additional revenue, Decrease = additional expenses)

Amount:

5. Identify Budget Impact (**Required**):

No Budget Impact. Funds are included in the Department Budget

- a. G/L line impacted A.25.000.8110 Attorney Fees; A.25.000.8119 Expenses Related to Legal Services
- b. Budget year impacted **2024**
- c. Details

Services will be provided at a rate of \$158/hour plus reasonable expenses, if any, not to exceed \$35,000. The hourly rate will be taken from account A.25.000.8110 Attorney Fees and any expenses will be taken from account A.25.000.8119 Expenses Related to Legal Services.

6. Are there Amendments to the Compensation Schedule?

YES or NO (If yes, provide details)

a. Is a new position being created? Y N

Effective date

Salary and grade

b. Is a new employee being hired? Y N

Effective date of employment

Salary and grade

Appointed position:

Term

c. Is this a reclassification? Y N

Is this position currently vacant? Y N

Is this position in the current year compensation plan? Y N

Human Resources Consulted

No

7. Does this item require the awarding of a contract: Y N

a. Type of Solicitation **Professional Service**

b. Specification # (BID/RFP/RFQ/OTHER CONTRACT #)

Purchasing Office Consulted

No

c. If a sole source, appropriate documentation, including an updated letter, has been submitted and approved by Purchasing Department? Y N N/A

d. Vendor information (including contact name):

Hugh G. Burke, Esq.
4 Bradbury Street
Clifton Park, NY 12065

e. Is the vendor/contractor an LLC, PLLC, or partnership:

f. State of vendor/contractor organization:

g. Commencement date of contract term:

h. Termination of contract date: **December 31, 2024**

i. Contract renewal date and term:

k. Is this a renewal agreement: Y N

l. Vendor/Contractor comment/remarks:

8. Is a grant being accepted: YES or NO

County Administrator's Office
Consulted **Yes**

- a. Source of grant funding:
- b. Agency granting funds:
- c. Amount of grant:
- d. Purpose grant will be used for:
- e. Equipment and/or services being purchased with the grant:
- f. Time period grant covers:
- g. Amount of county matching funds:
- h. Administrative fee to County:

9. Supporting Documentation:

- Marked-up previous resolution
- No Markup, per consultation with County Attorney
- Information summary memo
- Copy of proposal or estimate
- Copy of grant award notification and information
- Other _____

10. Remarks:

Hugh G. Burke Esq.
4 Bradbury St.
Clifton Park N.Y. 12065
(518) 469- 3165
burkejure@hotmail.com

Karen Heggen Esq.
District Attorney
Saratoga County District Attorney's Office
40 McMaster St.
Ballston Spa, N.Y. 12020

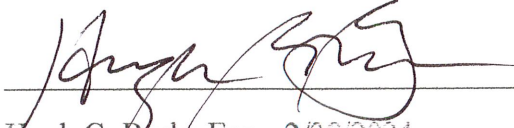
Dear Ms. Heggen,

Kindly accept this letter to outline the scope of services which I offer with regard to a proposed contract for services.

I propose to provide legal advice and representation with regard to N.Y. Public Officer's Law, Art. 6, sections 84-90, commonly known as the N.Y. Freedom of Information Law (FOIL), including legal review and advice regarding the statute and preparation of materials in response to FOIL requests which involve the District Attorney. Such services would supplement those services provided by the Saratoga County Attorney, but would not include such matters as are under the exclusive purview of the County Attorney; such as administrative appellate review or litigation.

Services would be provided at the hourly rate of \$158/hour plus reasonable expenses, if any, to be included in a contract to follow.

Thank you for your consideration.


Hugh G. Burke Esq., 2/28/2024



SARATOGA COUNTY AGENDA ITEM REQUEST

TO: Steve Bulger, County Administrator
Ridge Harris, Deputy County Administrator
George Conway, County Attorney
Therese Connolly, Clerk of the Board
Stephanie Hodgson, Director of Budget

CC: John Warnt, Director of Purchasing
Jason Kemper, Director of Planning and Economic Development
Bridget Rider, Deputy Clerk of the Board
Matt Rose, Management Analyst
Audra Hedden, County Administrator's Office
Samantha Kupferman, County Attorney's Office

DEPARTMENT: Office of Emergency Management

DATE: 02/29/2024

COMMITTEE: Public Safety



This column must be completed prior to submission of the request.

County Attorney's Office
Consulted Yes

1. Is a Resolution Required:

Yes, Contract Approval

2. Proposed Resolution Title:

Authorizing the Chairman to execute a contract for the purchase of the Motorola cybersecurity Astro 25 Managed Detection Response hardware and equipment, installation / activation services and initial 1 year subscription period for the Radio Network Infrastructure (RNI) followed by a two-year agreement with Motorola Solutions, Inc. for the Astro 25 MDR subscription on the County's Public Safety Radio Infrastructure

3. Specific Details on what the resolution will authorize:

This resolution will allow for the purchase of the Motorola cybersecurity Astro 25 Managed Detection Response hardware and equipment, installation / activation services and initial 1 year subscription period which will provide 24/7 security monitoring of the Radio Network Infrastructure through the ActiveEye platform. The Astro 25 MDR features ActiveEye Managed Detection and Response Elements, Service Modules (to include log collection / analytics, network detection, attack surface management) and security operations center monitoring which will commence on July 1, 2024 and continue through June 30, 2025. This agreement also includes an additional two-year subscription agreement with Motorola Solutions, Inc. which will commence on July 1, 2025 and continue through June 30, 2027. Form and content of agreement will be subject to the approval of County Attorney.

4. Is a Budget Amendment needed: YES or NO
If yes, budget lines and impact must be provided.
Any budget amendments must have equal and offsetting entries.

County Administrator's Office
Consulted No

- Please see attachments for impacted budget lines.
(Use ONLY when more than four lines are impacted.)

Revenue

Account Number	Account Name	Amount
----------------	--------------	--------

Expense

Account Number	Account Name	Amount
----------------	--------------	--------

Fund Balance (if applicable): (Increase = additional revenue, Decrease = additional expenses)

Amount:

5. Identify Budget Impact (**Required**):

No Budget Impact. Funds are included in the Department Budget

- a. G/L line impacted A.36.366-8520
- b. Budget year impacted 2024 - 2027
- c. Details

Initial purchase: A.36.366-8520 (SHSP 20 and SHSP 21)
Year 2 & Year 3 Subscription Period A.30.000-8520 (PSAP - Sheriff's Office grant)

6. Are there Amendments to the Compensation Schedule?

YES or NO (If yes, provide details)

a. Is a new position being created? Y N

Effective date

Salary and grade

b. Is a new employee being hired? Y N

Effective date of employment

Salary and grade

Appointed position:

Term

c. Is this a reclassification? Y N

Is this position currently vacant? Y N

Is this position in the current year compensation plan? Y N

Human Resources Consulted

No

7. Does this item require the awarding of a contract: Y N

a. Type of Solicitation **Sole Source**

b. Specification # (BID/RFP/RFQ/OTHER CONTRACT #)

Purchasing Office Consulted

Yes

c. If a sole source, appropriate documentation, including an updated letter, has been submitted and approved by Purchasing Department? Y N N/A

d. Vendor information (including contact name):

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781

e. Is the vendor/contractor an LLC, PLLC, or partnership:

f. State of vendor/contractor organization: IL

g. Commencement date of contract term: 07/01/2024

h. Termination of contract date: 06/30/2027

i. Contract renewal date and term:

k. Is this a renewal agreement: Y N

l. Vendor/Contractor comment/remarks:

Sole source purchase. Sole source letter is found on page 3 of proposal.

8. Is a grant being accepted: YES or NO

County Administrator's Office
Consulted **No**

- a. Source of grant funding:
- b. Agency granting funds:
- c. Amount of grant:
- d. Purpose grant will be used for:
- e. Equipment and/or services being purchased with the grant:
- f. Time period grant covers:
- g. Amount of county matching funds:
- h. Administrative fee to County:

9. Supporting Documentation:

- Marked-up previous resolution
- No Markup, per consultation with County Attorney
- Information summary memo
- Copy of proposal or estimate
- Copy of grant award notification and information
- Other Sole Source memo

10. Remarks:



MOTOROLA SOLUTIONS

**Firm Fixed Price Proposal
Saratoga County**

ASTRO 25 Managed Detection and Response

24-166173 / Cybersecurity Services
February 14, 2024

The design, technical, and price information furnished with this proposal is proprietary information of Motorola Solutions, Inc. (Motorola). Such information is submitted with the restriction that it is to be used only for the evaluation of the proposal, and is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the proposal, without the express written permission of Motorola Solutions, Inc.

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. © 2024 Motorola Solutions, Inc. All rights reserved.

PS-000166173

Table of Contents

Section 1

Executive Summary 1-2

Section 2

Solution Description..... 2-5

2.1 Solution Overview 2-5

2.2 Service Description 2-6

Section 3

Statement of Work 3-12

3.1 Overview 3-12

3.2 Description of Service 3-12

3.3 Security Operations Center Monitoring and Support 3-17

3.4 Limitations and Exclusion 3-22

Section 4

Proposal Pricing 4-24

4.1 Pricing Summary 4-24

4.2 Payment Schedule & Terms..... 4-24

4.3 Invoicing and Shipping Addresses 4-25

Section 5

Contractual Documentation..... 5-26

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

February 14, 2024

Andre M. Delvaux MPA, RN, NRP
Director of Emergency Management
6012 County Farm Road
Ballston Spa, NY 12020

RE: ASTRO® 25 Managed Detection and Response

Dear Mr. Delvaux,

Motorola Solutions, Inc. (Motorola) appreciates the opportunity to provide Saratoga County quality cybersecurity equipment and services. Motorola's project team has taken great care to propose a solution to address your needs and provide exceptional value. Motorola hereby certifies that the only cybersecurity platform certified and approved to work with Motorola ASTRO P25 systems is the ActiveEye solution. To ensure the integrity of the ASTRO P25 solution and continuity of operations, no other vendor is certified and approved to operate and deliver such solutions on Motorola systems.

Motorola's proposal is conditional upon Saratoga County acceptance of the terms and conditions included in this proposal, or a negotiated version thereof. Pricing will remain valid for 90 days from the date of this proposal.

Any questions Saratoga County has regarding this proposal can be directed to Nayeem Modan, Cybersecurity Account Manager at 917-620-5911 or by email at nayeem.modan@motorolasolutions.com.

Our goal is to provide Saratoga County with the best products and services available in the cybersecurity industry. We thank you for the opportunity to present our proposed solution, and we hope to strengthen our relationship by implementing this project.

Sincerely,



Mike Allen
Area Sales Manager, Cybersecurity – North America

MOTOROLA SOLUTIONS, INC.

Section 1

Executive Summary

Motorola is pleased to build upon our years of ongoing support to Saratoga County with a response that efficiently meets the needs for your ASTRO® 25 Managed Detection and Response (MDR) solution. We are a national and global leader in the cybersecurity community with our recent acquisitions of both Delta Risk and Lunarline in 2020. We have evolved into a holistic mission critical technology provider, placing Information Technology (IT), as well as cybersecurity, at the forefront of importance to protect our customers against threats to the confidentiality, integrity and availability of their operation.

ASTRO 25 Managed Detection and Response

Motorola's ASTRO 25 MDR provides radio network security element monitoring by experienced, specialized security technologists with extensive experience working with ASTRO 25 mission-critical networks. For highly complex or unusual security events, Motorola's technologists have direct access to Motorola engineers for rapid resolution.

Our solution provides 24x7x365 Security Operations Center Support. This is a component of our broader proprietary SOC 2 Type 2 certified Managed Security Platform targeted to Public Safety, Critical Infrastructure, and State/Local municipalities.

The ActiveEyeSM Platform

In 2020, Motorola acquired Delta Risk, a leading Managed Security Services Provider (MSSP). The acquisition now allows Motorola to extend the ActiveEyeSM platform to our customers and deliver a co-managed approach to 24/7 security monitoring operations across IT enterprise environments. The benefits of the ActiveEyeSM platform are demonstrated below:

- **Included Public Safety Threat Data Feed** — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.
- **Advanced Threat Detection & Response** — Consolidate SIEM data and direct threat inputs from endpoint security, network sensors, and cloud/SaaS applications. Pre-built custom playbooks to process alerts and reduce/eliminate manual analyst effort.
- **Single Dashboard for Threat Visibility** — Prioritize based on actual assets in the environment. Asset inventory created manually or automatically with Managed Vulnerability Assessment Service - external and authenticated scans of assets, providing a complete attack surface map.

Chief Information Security Officer (CISO) Benefits

Main dashboard displays and aggregates all of the important and relevant risk information from across the organization, helping decision makers to make better-informed decisions to balance cybersecurity efforts and operational efficiencies.

Main dashboard provides key performance metrics and indicators that can inform an admin at a glance to the activity that is occurring throughout their environment.

Create ad-hoc reports and notifications based on available data and ActiveEyeSM parameters.

Transparency into the service that Motorola is providing. The dashboard will provide the key indicators to the number of events that are handled on a daily, weekly, monthly basis and how those events are handled by the Motorola Security Operations Center (SOC).

Public Safety Threat Alliance

Cyber threats to public safety agencies are increasing in scope, scale, and complexity; however, most agencies lack the cybersecurity capabilities required to mitigate risk and ensure continuity of public safety operations. To address this critical need, Motorola has established a cyber threat information sharing and analysis organization (ISAO) for public safety called The Public Safety Threat Alliance (PSTA). The PSTA is recognized by the U.S. Cybersecurity and Infrastructure Security Association (CISA), and highlights Motorola's commitment to public safety agencies and the communities they serve.

The PSTA will leverage cybersecurity risk information from across Motorola's Cybersecurity Services. This, paired with information from members and trusted partners including CISA, other ISAOs, and nonprofits dedicated to sharing cyber threat intelligence, will help generate actionable intelligence to improve members' cybersecurity posture, defense, and resilience against evolving threats to their public safety missions. Membership in the PSTA is open to all public safety agencies. While initial efforts are focused on U.S. public safety, the Alliance will include global public safety agencies in the future.

Learn more about the Public Safety Threat Alliance at: <https://motorolasolutions.com/public-safety-threat-alliance>.

ABOUT MOTOROLA

Company Background and History

Motorola creates innovative, mission-critical communication solutions and services that help public safety and commercial customers build safer cities and thriving communities. You can find our products at work in a variety of industries including law enforcement, fire, emergency medical services, national government security, utilities, mining, energy, manufacturing, hospitality, retail, transportation and logistics, education, and public services. Our communication solutions span infrastructure, devices, services and software to help our public safety and commercial customers be more effective and efficient.

Company Overview

Since 1928, Motorola Solutions, Inc. (formerly Motorola, Inc.) has been committed to innovation in communications and electronics. Our company has achieved many milestones in its history. We pioneered mobile communications in the 1930s with car radios and public safety networks. We made the equipment that carried the first words from the moon in 1969. We commercialized the first handheld portable scanner in 1980. Today, as a global industry leader, excellence in innovation continues to shape the future of the Motorola brand.

We help people be their best in the moments that matter.

Motorola connects people through technology. Public safety and commercial customers around the world turn to Motorola innovations when they want highly connected teams that have the information they need throughout their workdays and in the moments that matter most to them.

Our customers rely on us for the expertise, services, and solutions we provide, trusting our years of invention and innovation experience. By partnering with customers and observing how our products can help in their specific industries, we are able to enhance our customers' experience every day.

Motorola's Corporate Headquarters is located at 500 West Monroe Street, Chicago, IL 60661. Telephone is +1 847.576.5000, and the website is www.motorolasolutions.com.

OUR VALUES

- WE ARE INNOVATIVE**
- WE ARE PASSIONATE**
- WE ARE DRIVEN**
- WE ARE ACCOUNTABLE**
- WE ARE PARTNERS**

Section 2

Solution Description

2.1 Solution Overview

Motorola Solutions, Inc. (Motorola) is pleased to present the proposed cybersecurity Managed Detection and Response (MDR) services for Saratoga County (hereinafter referred to as “Customer”).

Identifying and mitigating cyber threats requires a reliable solution that supplies the right data to cybersecurity experts. Motorola will provide access to our ActiveEyeSM Security Platform, along with 24x7 support from specialized security technologists, who will monitor your mission critical network against threat and intrusion.

The following ASTRO[®] 25 MDR features and services are included in our proposal:

- **ActiveEyeSM Managed Detection and Response Elements**
 - ActiveEyeSM Security Management Platform
 - ActiveEyeSM Remote Security Sensor (AERSS)
- **Service Modules**
 - Log Collection / Analytics
 - Network Detection
 - Attack Surface Management
- **Security Operations Center Monitoring and Support**

2.1.1 Site Information

The following site information is included in the scope of our proposal:

Table 2-1: Site Information

Site / Location	Quantity
Core Site	1
Network Management Clients	3
Dispatch Consoles	26
AIS	1

Services Included

The ActiveEyeSM service modules included in our proposal are selected in the **Subscribed** column below. The **Network Environment** column will designate the location of each module: ASTRO 25 Radio Network Infrastructure (RNI), Customer Enterprise Network (CEN), or the Control Room CEN.

Table 2-2: Service Modules

Service Module	Features Included	Network Environment	Subscribed
ActiveEye SM Remote Security Sensor (AERSS)	Number of sensors: 1 (1) Core Site	RNI	X
Log Collection / Analytics	Online Storage Period: 30 Day Storage Extended Log Storage Length: 12 Months	RNI	X
Network Detection	Up to 1 Gbps per sensor port	RNI	X
Attack Surface Management	Features in Section 3.2.3.3	RNI	X

Note: CENs are out of scope and are the responsibility of the customer.

The following table lists any ancillary components that may be required.

Table 2-3: Ancillary Components

Description	Quantity
Internetworking Firewall	1

2.2 Service Description

Managed Detection and Response is performed by Motorola’s Security Operations Center (SOC) using the ActiveEyeSM security platform. The SOC’s cybersecurity analysts monitor for alerts 24x7x365. If a threat is detected, analysts will investigate and initiate an appropriate Customer engagement. Customer engagements may include, but are not limited to: requesting additional information from the Customer, continuing to monitor the event for further development, or informing the Customer to enact the Customer’s documented Incident Response plan.

SOC analysts rely on monitoring elements to detect signs of a potential threat impacting the Customer’s ASTRO 25 network and applicable Customer Enterprise Network (CEN) systems. These elements are described below.

The MDR service includes the deployment and optimization of these elements into the Customer’s network. The Service also provides Cybersecurity awareness and best practices training to fortify the first line of defense, the organization’s people. A single subscription (1 seat) to Motorola Solutions online Learning Hub for Cybersecurity is included.

2.2.1 Managed Detection and Response Elements

This section and its subsections describe Managed Detection and Response elements, and their applicability for specific infrastructure.

2.2.1.1 ActiveEyeSM Security Platform

Motorola’s ActiveEyeSM security platform collects and analyzes security event streams from ActiveEyeSM Remote Security Sensors (AERSS) in the Customer’s ASTRO 25 network and applicable CEN systems, using security orchestration and advanced analytics to identify the most important security events from applicable systems. The ActiveEye platform is provided in the English language.

The platform automates manual investigation tasks, verifies activity with external threat intelligence sources, and learns what events will require rapid response action.

The Customer will receive access to the ActiveEyeSM platform as part of this service. ActiveEyeSM will serve as a single interface to display system security information. Using ActiveEyeSM, the Customer will be able to configure alerts and notifications, review security data, and perform security investigations.

Applies to included ASTRO 25 RNI.

2.2.1.2 ActiveEyeSM Managed Security Portal

The ActiveEyeSM Managed Security Portal will synchronize security efforts between the Customer and Motorola. From this central point, the Customer will be able to view threat insights, event investigations, security reports, threat advisories, and status of any security cases.

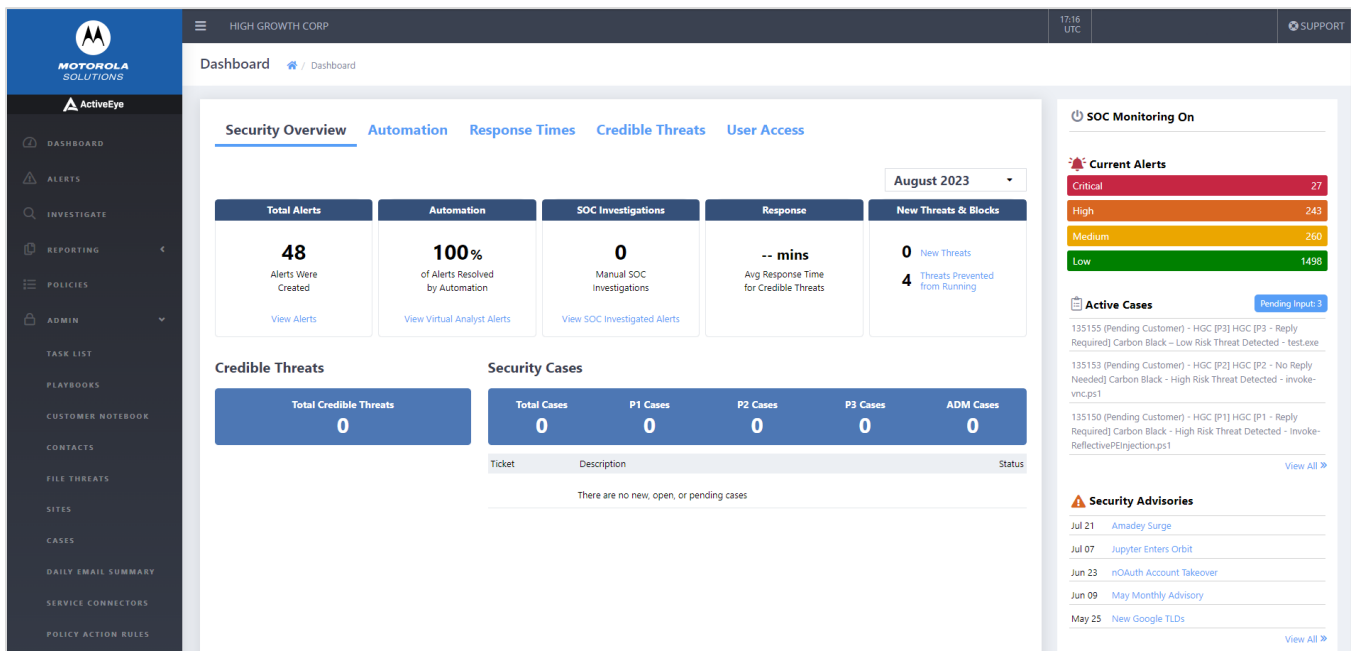


Figure 2-1: ActiveEyeSM Portal

Dashboard

Key information in the ActiveEyeSM Portal is summarized on the dashboard. This dashboard provides details about open alerts, an overview of alert categories, alert processing, key performance indicators (KPI), open security cases, and recent threat advisories. Also, users can access more in-depth information like security cases, alert details, alert trends, reports, and group communications.

Security Cases

When the Customer and Motorola identify a threat, the SOC will create a security case. Through the ActiveEyeSM Portal, the Customer can view details of current or past cases, create new cases, or respond to ongoing cases.

Alert Details and Trends

Alerts can be evidence of a past, active, or developing threat. ActiveEyeSM records relevant data for each alert, enabling users to quickly view its triggers, systems it impacts, and any actions taken to address the alert. ActiveEyeSM Portal also provides tools for reviewing groups of alerts based on key attributes or time periods. Attribute filters enable users to toggle which alert groups ActiveEyeSM Portal shows, helping to spot trends or threat activity. Users can also compare alert logs for specific time periods to determine if specific trends are associated with a threat or are false positives.

Investigations and Reporting

ActiveEyeSM Portal includes robust *ad hoc* reporting capabilities, which will provide important, additional information about active and historical threats. Users can share information outside of ActiveEyeSM Portal by downloading reports in .csv or .json format.

In addition to *ad hoc* reporting, ActiveEyeSM Portal can provide a daily email summary and monthly report. Daily email summaries can include alert counts, security cases opened or closed, saved queries that have new data, and detailed endpoint security statistics. If needed, ActiveEyeSM Portal can send one or more summary emails with different content for different groups. Monthly reports are available as a PDF download.

Security Advisories

Security Advisories are messages initiated from the SOC that share information on active threats with the Customer's security teams. These advisories guide security teams on how to best take action against a threat and tell them where they can find further information.

Information Sharing

The ActiveEyeSM Portal includes several functions for sharing information. Automatic security alerts notify pre-defined contacts of incidents, based on incident priority. Other information sharing functions include:

- **SOC Bulletins** - Instructions from the Customer, or the SOC, that SOC analysts reference when creating security cases. These can communicate short-term situations where a security case may not be needed, such as during testing or maintenance windows.
- **Customer Notebook** - The SOC will use the Customer Notebook to document the Customer's environment and any specific network implementation details that will help the SOC investigate security cases.
- **Contact Procedures** - Escalation procedures and instructions on who to contact if an incident occurs. Contact procedures include instructions and procedures for specific security incident levels. The SOC and the Customer will jointly manage contact procedures.

User Access

The ActiveEyeSM Portal provides the ability to add, update, and remove user access. Every ActiveEyeSM user can save queries, customize reports, and set up daily email summaries. Users may be given

administrative access, allowing them to perform administrative tasks, such as setting up new service connectors, resetting passwords, and setting up multi-factor authentication for other users.

2.2.1.3 ActiveEyeSM Remote Security Sensor

One or more AERSS will be deployed into the ASTRO 25 network and if applicable to CEN environments to deliver the service. These sensors monitor geo diverse sites for security events and pass security information to the ActiveEyeSM platform.

AERSS integrate the ActiveEyeSM platform with network elements, enabling it to collect logs from Syslog, as well as to analyze network traffic over port(s) and scan elements for vulnerabilities.

The following are the environmental requirements and specifications the Customer must provide to prepare for the AERSS deployment.

Specifications	Requirements
Rack Space	1U
Power Consumption (Max)	550 Watts (Redundant Power Supply)
Power Input	100-240V AC
Current	3.7 A – 7.4 A
Circuit Breaker	Qty. 2
Line Cord	NEMA 5-15P
Heat Dissipation (max)	2107 BTU/hr.
Internet Service Bandwidth	Bandwidth throughput 10Mbps per zone

Applies to included ASTRO 25 RNI.

2.2.1.4 Internetworking Firewall

Motorola introduces a formalized and centralized Internet connection to the ASTRO[®] 25 system using an Internetworking Firewall.

The Internetworking Firewall serves as a security barrier and demarcation point between a master site and the Internet (or a customer network leading to the Internet). The Internetworking Firewall supports traffic for various ASTRO[®] 25 features that require access to the Internet.

The Internetworking Firewall sits between the Demilitarized Zone (DMZ) and the Internet (or customer network leading to the Internet).

The following are the environmental requirements and specifications the Customer must provide to prepare for the Internetworking Firewall deployment.

Specifications	Requirement
Rack Space	1U
Power Consumption (Max)	28.6 W (Single Power Supply)
Power Input	100-240V AC

Specifications	Requirement
Current	.52 A
Circuits Breaker	Qty. 1
Heat Dissipation (Max)	97.6 BTU/hr.
Line Cord	NEMA 5-15P
Internet Service Bandwidth	Bandwidth throughput 10 MB High availability Internet Connection (99.99% (4-9s) or higher). Packet loss < 0.5%. Jitter <10 ms. Delay < 120 ms. RJ45 Port Speed - Auto Negotiate

2.2.2 Service Modules

ActiveEyeSM delivers service capability by integrating one or more service modules. These modules provide ActiveEyeSM analytics more information to correlate and a clearer vision of events on Saratoga County’s network. In addition, modules enable security teams and analysts to more easily access and compare data from these disparate systems. The following subsections describe each ActiveEyeSM service module in detail.

2.2.2.1 Log Collection / Analytics

The AERSS deployed in the system collects logs and other security information from applicable servers, workstations, switches, routers, Network Detection, and firewalls. This information is forwarded to the ActiveEyeSM platform, which uses advanced analytics to identify signs of security incidents. If it identifies signs of a security incident, ActiveEyeSM notifies the SOC for further analysis.

Collected events will be stored in the ActiveEyeSM Security Management Platform to enable historical searching or threat hunting as needed. Some high volume, repetitive logs may be aggregated as noted in the documentation. The default storage time period is one year, but no longer than 90 days, following expiration or termination of the Agreement. A longer time period can be provided if subscribed, see Table 2-2: Service Modules for subscription details.

2.2.2.2 Network Detection

The AERSS supports Network Detection, constantly monitoring traffic passing across, into, or out of infrastructure. Network Detection analyzes traffic for signs of malicious activity in real time, and performs packet level and flow level analysis to enable communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including traffic using encrypted connections. Network Detection forwards detected suspicious activity to the SOC for further analysis.

2.2.2.3 Attack Surface Management

Attack Surface Management is provided for the ASTRO® internet-facing, external network interfaces. The scan is enabled from an internet cloud hosted service outside the ASTRO® network. Discovery and vulnerability scans will be run quarterly or on a less frequent schedule defined with the Customer.

2.2.3 Security Operations Center Services

Motorola delivers SOC Monitoring using one or more SOC facilities. The SOC includes any centralized hardware and software used to deliver this Service and its service modules. The SOC and its centralized hardware and software are housed within an SSAE-18 compliant data center.

Motorola's SOC is staffed with security experts who will use ActiveEyeSM Security Management Platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate and triage detected threats, and to recommend responses to the Customer.

Section 3

Statement of Work

3.1 Overview

Motorola's ASTRO® 25 MDR provides monitoring of radio network security information by specialized cybersecurity analysts with extensive experience working with ASTRO® 25 mission-critical networks.

The following sections describe the deliverables of the service, its technologies, and service obligations.

In order to receive the services as defined within this SOW, the Customer is required to keep the system within a standard support period as described in Motorola's Software Support Policy (SwSP). Contact your local Customer Support Manager for details.

3.2 Description of Service

3.2.1 Deployment Timeline and Milestones

The following phase descriptions lay out the necessary deployment activities and milestones required to achieve service readiness:

Phase 1: Service Onboarding

After contract signature, Motorola will schedule a service kick-off meeting with the Customer and provide information-gathering documents. This kick-off meeting is conducted remotely at the earliest, mutually available opportunity within 30 days of contract signing. Customer is to identify and ensure participation of key team members in kickoff and project initiation activities.

The Customer will be provisioned onto the ActiveEyeSM MDR portal and be able to configure key contacts for interaction with the Security Operations team. The portal will enable service notifications, access to vulnerability scans and cybersecurity advisories. The first vulnerability scan will be conducted and reported within the first 30-day period. The Customer will receive instructions for accessing the Security Operations Center and Incident Response (IR) teams within the first 30 days. Once access is provisioned, the customer will receive any assistance required from the IR team. Access will also be provided to the Cybersecurity Learning portal.

Phase 2: Infrastructure Readiness

Motorola will provide detailed requirements regarding Customer infrastructure preparation actions after kick-off meeting. It is the Customer's responsibility to accomplish all agreed upon infrastructure preparations. It is Motorola's responsibility to separately complete any obligated and/or agreed infrastructure readiness tasks.

Phase 3: System Buildout and Deployment

Motorola will build and provision tools in accordance with the requirements of this proposal and consistent with information gathered in earlier phases. Motorola will also provide detailed requirements regarding Customer deployment actions. The Customer must deploy tools, as applicable, in their environment, in accordance with provided requirements.

Phase 4: Monitoring “Turn Up”

Motorola will verify all in-scope assets are forwarding logs or events. Motorola will notify Customer of any exceptions. Motorola will begin monitoring any properly connected in-scope sources after the initial tuning period.

Phase 5: Tuning/Report Setup

Motorola will conduct initial tuning of the events and alarms in the service and conduct an additional ActiveEyeSM Portal training session.

Service Commencement

The Service will commence with the Service Onboarding phase or within 30 days of contract signature, whichever event occurs soonest for existing customers.

In the case of a new ASTRO system, the Service will commence in parallel to the commencement date of the core ASTRO Service package “Turn Up” date. Motorola and the Customer will collaborate to complete the additional deployment tasks.

3.2.2 General Responsibilities

3.2.2.1 Motorola Responsibilities

- Provide, maintain, and when necessary, repair under warranty hardware and software required to monitor the ASTRO 25 network and applicable CEN systems Inclusive of the AERSS and all software operating on it.
 - If the Centralized Event Logging feature is not installed on the Customer’s ASTRO 25 RNI, Motorola will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola service authentication credentials.
- Monitor the Customer’s ASTRO 25 network and applicable CEN systems 24/7/365 for malicious or unusual activity.
- Respond to security incidents in the Customer’s system in accordance with Section 3.3.6: Incident Priority Level Definitions and Response Times. This may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further development or informing the Customer to enact the Customer’s documented Incident Response plan.

- Assist the Customer with identifying devices that support logging within the ASTRO 25 network and applicable CEN systems have been configured to forward Syslog events to the AERSS.
- Provide the Customer with access to the ActiveEyeSM platform enabling Customer access to security event and incident details.

3.2.2.2 Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before service commences. Internet service bandwidth requirements are as follows:
 - Bandwidth throughput of 10MB
 - High availability Internet Connection (99.99% (4-9s) or higher)
 - Packet loss < 0.5%
 - Jitter <10 ms
 - Delay < 120 ms
 - RJ45 Port Speed - Auto Negotiate
- Maintain an active subscription for:
 - Security Update Service (SUS) (or Remote Security Update Service), ensuring patches and antivirus definitions are applied according to the release cadence of the service.
 - ASTRO Dispatch Service and ASTRO Infrastructure Response.
- The ASTRO 25 Managed Detection and Response service requires an ASTRO 25 WAVE SUS subscription.
- Allow Motorola continuous remote access to monitor the ASTRO 25 network and applicable CEN systems. This includes keeping the connection active, providing passwords, and working with Motorola to understand and maintain administration privileges.
- Provide continuous utility service(s) to any equipment installed or utilized at the Customer's premises to support service delivery and remote monitoring.
- Provide Motorola with contact information necessary to complete the Customer Support Plan (CSP). Notify the Customer's Customer Support Manager (CSM) within two weeks of any contact information changes.
- Notify Motorola if any components are added to or removed from the environment as it may be necessary to update or incorporate in Managed Detection and Response. Changes to monitored components may result in changes to the pricing of the Managed Detection and Response service.
- As necessary, upgrade the ASTRO 25 system, on-site systems, and third party software or tools to supported releases.
- Allow Motorola's dispatched field service technicians physical access to monitoring hardware when required.
- Cooperate with Motorola and perform all acts that are required to enable Motorola to provide the services described in this SOW.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEyeSM sensor for applicable CEN systems.

- Respond to Cybersecurity Incident Cases created by the Motorola SOC.

3.2.3 Service Modules

The following subsections describe the delivery of the service modules selected in Table 2-2: Service Modules.

3.2.3.1 Log Analytics

The AERSS deployed in the system collects logs and other security information from applicable servers, workstations, switches, routers, Network Detection, and firewalls. This information is forwarded to the ActiveEyeSM platform, which uses advanced analytics to identify signs of security incidents. If it identifies signs of a security incident, ActiveEyeSM notifies the SOC for further analysis.

Motorola Responsibilities

- Consult with and advise the Customer on performing necessary system configurations to direct log sources to the appropriate Remote Security Sensor.
- The SOC will consult with the Customer to identify appropriate log sources for the level of threat detection desired in each environment.

Customer Responsibilities

- If applicable, configure customer-managed networking infrastructure to allow AERSS to Communicate with ActiveEyeSM as defined.
- If applicable, configure any Customer managed devices in the CEN to forward data to ActiveEyeSM.

Applies to included ASTRO 25 RNI.

3.2.3.2 Network Detection

The AERSS deploys a Network Intrusion Detection System (NIDS), constantly monitoring traffic passing across, into, or out of infrastructure. Network Detection analyzes traffic for signs of malicious activity in real time, and performs packet level and flow level analysis to enable communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including traffic using encrypted connections. Network Detection forwards detected suspicious activity to the SOC for further analysis.

Motorola Responsibilities

- Work with the Customer to integrate AERSS.
- Optimize the policies and configuration to tune out noise and highlight potential threats.
- The SOC consults with the Customer to identify the appropriate deployment of Network Detection Service Components. The SOC will monitor and update the security policy of each sensor to tune out unnecessary alerting and flow monitoring so that the system is optimized to detect true malicious activity.

Customer Responsibilities

- If necessary, configure Customer's networking infrastructure to allow AERSS to communicate with ActiveEyeSM as defined.

- For Customer's owned CEN infrastructure, configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEyeSM sensor.
- Initiate recommended response actions when active attacks are detected.

Applies to included ASTRO 25 RNI.

3.2.3.3 Attack Surface Management

Attack Surface Management is provided for the ASTRO® internet-facing, external network interfaces. The scan is enabled from an internet cloud hosted service outside the ASTRO® network. Discovery and vulnerability scans will be run quarterly or on a less frequent schedule defined with the Customer.

The initial scan results will be discussed with the Customer during service onboarding. Subsequent scans will be reviewed by a cybersecurity analyst. If any new findings of interest are surfaced, a ticket will be created to communicate these findings with the customer defined contacts.

Motorola Responsibilities

- Configure scans to match the Customer's preferences for external scope.
- Verify vulnerability scans are operating correctly.
- Make generated results available in the Customer's ActiveEyeSM portal.
- Create ticket notifications for significant, new findings of interest.

Customer Responsibilities

- During Service Onboarding kickoff, provide Motorola with the IP addresses and/or domain names to be included in the external vulnerability scans.
- In accepting this Statement of Work, the Customer authorizes Motorola to engage in external vulnerability scans of internet-facing, external assets disclosed by the Customer.
- Update Motorola with any changes to the IP addresses and/or domain names of the internet-facing, external assets subject to the external vulnerability scans.
- If the information required to enable vulnerability scanning of the internet-facing, external assets is not provided initially or is not current at any time during the term, Motorola will suspend scans until it is reasonably satisfied that it has been provided with the most current information.
- Review all quarterly vulnerability reports, and tickets of new findings.
- Perform any remediation actions required to address identified vulnerabilities.

Applies to Internet facing assets only.

3.2.4 Cybersecurity Awareness and Best Practices Training

A key component of any cybersecurity program is ensuring people involved in managing and using IT systems understand specific cybersecurity practices to both prevent actions that involuntarily create cybersecurity risk and respond quickly if a compromise is suspected. The Managed Detection and Response service provides access to an online subscription based Learning Hub, containing courses and content focused on the Cybersecurity needs of our customers. There are a number of

Cybersecurity Modules offered through the hub via a variety of teaching methods and courses, providing timely, relevant and custom-fit cybersecurity training.

A single subscription to the Learning Hub is provided during Service Onboarding. The number of subscriptions and duration can be scaled to meet customer needs.

3.3 Security Operations Center Monitoring and Support

3.3.1 Scope

Motorola delivers SOC Monitoring using one or more SOC facilities. The SOC includes any centralized hardware and software used to deliver this Service and its service modules. The SOC and its centralized hardware and software are housed within an SSAE-18 compliant data center.

Motorola's SOC is staffed with security experts who will use ActiveEyeSM Security Management Platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate and triage detected threats, and to recommend responses to the Customer. Customer support is provided in the English language.

Motorola will start monitoring the ASTRO® 25 MDR service in accordance with Motorola processes and procedures after deployment, as described in Section 3.2.1: Deployment Timeline and Milestones.

The SOC receives system-generated alerts 24x7, and provides the Customer with a toll-free telephone number and email address for support requests, available 24x7. Support requests are stored in a ticketing system for accountability and reporting. The SOC will respond to detected events in accordance with Section 3.3.6: Incident Priority Level Definitions and Response Times.

3.3.2 Ongoing Security Operations Center Service Responsibilities

Motorola Responsibilities

If a probable security incident is detected, provide phone and email support to:

- Engage the Customer's defined Incident Response Process.
- Gather relevant information and attempt to determine the extent of compromise using existing monitoring capabilities in place as part of the ASTRO 25 MDR service.
- Analysis and support to help the Customer determine if the Customer's corrective actions are effective.
- Continuous monitoring, in parallel with analysis, to support incident response.

Customer Responsibilities

- Provide Motorola with accurate and up-to-date information, including the name, email, landline telephone numbers, and mobile telephone numbers for all designated, authorized Customer escalation Points of Contact (PoC).
- Provide a timely response to SOC security incident tickets or investigation questions.
- Notify Motorola at least 24 hours in advance of any scheduled maintenance, network administration activity, or system administration activity that would affect Motorola's ability to perform the Managed SOC Service, as described in this SOW.

3.3.3 Technical Support

ActiveEyeSM Security Management Technical Support provides the Customer with a toll-free telephone number and email address for ActiveEyeSM Security Management support requests, available Monday through Friday from 8am to 7pm CST.

Motorola Responsibilities

- Notify Customer of any scheduled maintenance or planned outages.
- Provide technical support, security control, and service improvements related to ActiveEyeSM.

Customer Responsibilities

- Provide sufficient information to allow Motorola technical support agents to diagnose and resolve the issue.

Limitations and Exclusions

Technical support is limited to the implementation and use of the ActiveEyeSM Security Management platform and does not include use or implementation of third-party components.

3.3.4 Incident Response

An Indicator of Compromise (IoC) is an observable event that Motorola Security Analysts have determined will jeopardize the confidentiality, integrity, or availability of the system. Examples of IoC include ransomware or malicious use of PowerShell.

When an IoC is observed, the Motorola Security Operations team will engage with the customer to investigate the issue, determine the extent of the compromise and contain the activity to the extent possible with the Motorola security controls deployed within the environment. This expert guidance is available upon contract signature and extends through MDR infrastructure deployment phases and the term of the contract.

When an IoC is observed by the Security Analyst, Motorola and Customer will be responsible for the tasks defined in the following subsections.

Motorola Responsibilities

- Upon the identification of an IoC, notify the Customer's documented contact and initiate the escalation plan.
- Take documented, Customer approved actions in an attempt to contain an IoC to the extent enabled via Motorola managed technology. Communicate to the Customer any additional potential containment actions and incident response resources that can be taken across the Customer's managed IT infrastructure.
- Perform investigation using the ActiveEyeSM Managed Detection and Response integrated and enabled data sources in an initial attempt to determine the extent of an IoC.
- Document and share IoC and artifacts discovered during investigation. Motorola services exclude performing on-site data collection or official forensic capture activities on physical devices.

Customer Responsibilities

- Maintain one named PoC to coordinate regular team discussions and organize data collection and capture across the Customer and Motorola teams.
- If determined to be required by Customer, contract an Incident Response service provider to perform procedures beyond the scope of this Agreement such as forensic data capture, additional malware removal, system recovery, ransomware payment negotiation, law enforcement engagement, insurance provider communications, identify patient zero, etc.

3.3.5 Event Response and Notification

Motorola will analyze events created and/or aggregated by the Service, assess their type, and notify the Customer in accordance with the following table.

Table 3-1: Event Handling

Event Type	Details	Notification Requirement
False Positive or Benign	Any event(s) determined by Motorola Solutions to not likely have a negative security impact on the organization.	None
Event of Interest (EOI)	Any event(s) determined by Motorola Solutions to likely have a negative security impact on the organization.	Escalate to Customer in accordance with routine notification procedure. Escalate in accordance with urgent notification procedure when required by agreed-upon thresholds and SOC analysis. Notification procedures are included in Table 3-2: Notification Procedures.

Notification

Motorola will establish notification procedures with the Customer, generally categorized in accordance with the following table.

Table 3-2: Notification Procedures

Notification Procedure	Details
Routine Notification Procedure	The means, addresses, format, and desired content (within the capabilities of the installed technology) for Events of Interest. These can be formatted for automated processing, e.g., by ticketing systems.
Urgent Notification Procedure	Additional, optional means and addresses for notifications of Events of Interest that require urgent notification. These usually include telephone notifications.

Motorola will notify the Customer according to the escalation and contact procedures defined by the Customer and Motorola during the implementation process.

Tuning

Motorola will assess certain events to be environmental noise, potentially addressable configuration issues in the environment, or false positives. Motorola may recommend these be addressed by the Customer to preserve system and network resources.

Motorola will provide the Customer with the ability to temporarily suppress alerts reaching ActiveEyeSM, enabling a co-managed approach to tuning and suppressing events or alarms. The SOC may permanently suppress particular alerts and alarms if not necessary for actionable threat detection.

Tuning Period Exception

The tuning period is considered to be the first 30 days after each service module has been confirmed deployed and configured and starts receiving data. During the tuning period, Motorola may make recommendations to the Customer to adjust the configurations of their installed software so Services can be effectively delivered. Service Availability will not be applicable during the tuning period and responses or notifications may not be delivered. However, Motorola will provide responses and notifications during this period.

Motorola may continue to recommend necessary tuning changes after this period, with no impact on Service Availability.

3.3.6 Incident Priority Level Definitions and Response Times

Priority for an alert-generated incident or EOI is determined by the ActiveEyeSM Platform analytics that process multiple incoming alert feeds, automation playbooks, and cybersecurity analyst knowledge.

Table 3-3: Priority Level Definitions and Response Times

Incident Priority	Incident Definition	Notification Time
Critical P1	Security incidents that have caused, or are suspected to have caused significant damage to the functionality of Customer’s ASTRO 25 system or information stored within it. Effort to recover from the incident may be significant. Examples: <ul style="list-style-type: none"> • Malware that is not quarantined by anti-virus. • Evidence that a monitored component has communicated with suspected malicious actors. 	Response provided 24 hours, 7 days a week, including US public holidays.
High P2	Security incidents that have localized impact, and may become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant. Examples: <ul style="list-style-type: none"> • Malware that is quarantined by antivirus. • Multiple behaviors observed in the system that are consistent with known attacker techniques. 	Response provided 24 hours, 7 days a week, including US public holidays.

Incident Priority	Incident Definition	Notification Time
Medium P3	Security incidents that potentially indicate an attacker is performing reconnaissance or initial attempts at accessing the system. Effort to recover from the incident may be low to moderate. Examples include: <ul style="list-style-type: none"> • Suspected unauthorized attempts to log into user accounts. • Suspected unauthorized changes to system configurations, such as firewalls or user accounts. • Observed failures of security components. • Informational events. • User account creation or deletion. • Privilege change for existing accounts. 	Response provided on standard business days, Monday through Friday 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.
Low P4	These are typically service requests from the Customer.	Response provided on standard business days, Monday through Friday from 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.

3.3.6.1 Response Time Goals

Priority	Response Time
Critical P1	An SOC Cybersecurity Analyst will make contact with the customer technical representative within one (1) hour of the request for support being logged in the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.
High P2	An SOC Cybersecurity Analyst will make contact with the customer technical representative within four (4) hours of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.
Medium P3	An SOC Cybersecurity Support Engineer will make contact with the customer technical representative within the next business day of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action.
Low P4	An SOC Cybersecurity Support Engineer will make contact with the Customer technical representative within seven business days of the logged request for support at the issue management system.

3.3.6.2 ActiveEyeSM Platform Availability

The platform utilizes a multi-zone architecture which can recover from failures in different data collection, enhancement, analysis, and visualization tiers. Motorola will make commercially reasonable efforts to provide monthly availability of 99.9% for the ActiveEyeSM Platform services. Service availability is subject to limited scheduled downtime for servicing and upgrades, as well as unscheduled

and unanticipated downtime resulting from circumstances or events outside of Motorola's reasonable control, such as disruptions of, or damage, to the Customer's or a third-party's information or communications systems or equipment, telecommunication circuit availability/performance between Customer sites, any on-premises core and/or between on-premises equipment and the ActiveEyeSM Platform.

3.3.6.3 ActiveEyeSM Remote Security Sensor

One or more AERSS may be deployed as part of the MDR solution. The AERSS is configured with multiple local redundancy features such as hot-swap hard disk drives in a redundant drive array configuration and dual redundant power supplies.

The AERSS and all components of ActiveEyeSM are monitored by a dedicated Site Reliability Engineering team. In cases of hardware failure of the AERSS, Motorola will provide, subject to active service subscriptions in the Customer contract, onsite services to repair the AERSS and restore service. AERSS operation and outage troubleshooting requires network connection to the ActiveEyeSM Platform which may be impacted by customer configuration changes, telecommunications connectivity, and/or customer network issues/outages.

3.4 Limitations and Exclusion

Motorola's ASTRO MDR service does not include services to perform physical containment and/or remediation of confirmed security incidents, remote or onsite. The Customer may choose to purchase additional Incident Response professional services to assist in the creation of and/or completion of a Customer's Incident Response Plan.

Motorola's scope of services does not include responsibilities relating to active protection of customer data, including its transmission to Motorola, recovery of data available through the products or services, or remediation or responsibilities relating to the loss of data, ransomware, or hacking.

3.4.1 Service Limitations

Cybersecurity services are inherently limited and will not guarantee that the Customer's system will be error-free or immune to security breaches as a result of any or all of the services described in this SOW. Motorola does not warrant or guarantee that this service will identify all cybersecurity incidents that occur in the Customer's system. Services and deliverables are limited by, among other things, the evolving and often malicious nature of cyber threats, conduct/attacks, as well as the complexity/disparity and evolving nature of Customer computer system environments, including supply chains, integrated software, services, and devices. To the extent we do offer recommendations in connection with the services, unless otherwise stated in the Statement of Work, our recommendations are necessarily subjective, may or may not be correct, and may be based on our assumptions relating to the relative risks, priorities, costs and benefits that we assume apply to you.

3.4.2 Processing of Customer Data in the United States and/or other Locations

Customer understands and agrees that data obtained, accessed, or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola in the

U.S. and/or other Motorola operations globally. Customer consents to and authorizes all such processing and agrees to provide, obtain, or post any necessary approvals, consents, or notices that may be necessary to comply with applicable law.

3.4.3 Customer and Third-Party Information

Customer understands and agrees that Motorola may obtain, use and/or create and use, anonymized, aggregated and/or generalized Customer Data, such as data relating to actual and potential security threats and vulnerabilities, for its lawful business purposes, including improving its services and sharing and leveraging such information for the benefit of Customer, other customers, and other interested parties. For avoidance of doubt, so long as not specifically identifying the Customer, Customer Data shall not include, and Motorola shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, third party threat vectors and IP addresses (i.e., so long as not defined as personal information under applicable law), file hash information, domain names, malware signatures and information, information obtained from third party sources, indicators of compromise, and tactics, techniques, and procedures used, learned or developed in the course of providing Services, which data shall be deemed Service Use Data (i.e., Motorola data).

3.4.4 Third-Party Software and Service Providers, including Resale

Motorola may use, engage, license, resell, interface with or otherwise utilize the products or services of third-party processors or sub-processors and other third-party software, hardware, or services providers (such as, for example, third-party endpoint detection and response providers). Such processors and sub-processors may engage additional sub-processors to process personal data and other Customer Data. Customer understands and agrees that the use of such third-party products and services, including as it relates to any processing or sub-processing of data, is subject to each respective third-party's own terms, licenses, End User License Agreements (EULA), privacy statements, data processing agreements and/or other applicable terms. Such third-party providers and terms may include the following, if applicable, or as otherwise made available publicly, through performance, or upon request:

Motorola disclaims any and all responsibility for any and all loss or costs of any kind associated with security events. Motorola disclaims any responsibility for customer use or implementation of any recommendations provided in connection with the services. Implementation of recommendations does not ensure or guarantee the security of the systems and operations evaluated.

Section 4

Proposal Pricing

4.1 Pricing Summary

Motorola pricing is based on the services and solution presented in Section 2. The addition or deletion of any component(s) may subject the total solution price to modifications.

Description	
ASTRO® 25 Managed Detection and Response	\$45,600.00
Hardware and Equipment	\$8,400.00
Installation and Activation Services	\$30,123.00
Subtotal	\$84,123.00
Customer Loyalty Discount	(\$4,206.15)
Year 1 Total	\$79,916.85

Initial Subscription Period after Year 1:

Description			
Year	Price	Customer Loyalty Discount	Total
Initial Subscription Period - Year 2	\$47,424.00	(\$2,371.20)	\$45,052.80
Initial Subscription Period - Year 3	\$49,320.96	(\$2,466.05)	\$46,854.91

4.2 Payment Schedule & Terms

Period of Performance

The initial MDR subscription period of the contract will extend three (3) years from the Commencement Date of Service, defined as the date data is available for analysis, or not later than thirty (30) days after Motorola provides the Customer with necessary hardware or software.

Term

The Term of the contract begins on the Commencement Date of Service and remains in effect until the expiration of the initial period so specified.

Billing

Upon acceptance of this proposal by the Customer, Motorola will invoice the Customer for all service fees in advance for the full Year 1 amount according to the Pricing table in Section 4.1.

Thereafter, Motorola will invoice the Customer annually, in advance for (a) the Services to be performed (as applicable); and (b) any other charges incurred as agreed upon between the parties during the term of the subscription.

Customer will make payments to Motorola within thirty (30) days after receipt of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a United States financial institution.

INFLATION ADJUSTMENT. For multi-year agreements, at the end of the first year of the Agreement and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, all Items, Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right to increase all future maintenance prices by the CPI increase amount exceeding 3%. All items, not seasonally adjusted shall be used as the measure of CPI for this price adjustment. Measurement will take place once the annual average for the new year has been posted by the Bureau of Labor Statistics. For purposes of illustration, if in year 5 the CPI reported an increase of 8%, Motorola may increase the Year 6 price by 5% (8%-3% base).

Tax

Unless otherwise noted, this proposal excludes sales tax or other applicable taxes (such as Goods and Services Tax, Value Added Tax and other taxes of a similar nature). Any tax the customer is subject to will be added to invoices.

4.3 Invoicing and Shipping Addresses

Invoices will be sent to Customer at the following address:	
Name:	
Address:	
Phone:	
Email:	

Address of Ultimate Destination for Equipment to be Delivered to Customer:	
Name:	
Address:	

Equipment Shipped to Customer at the following address:	
Name:	
Address:	
Phone:	

Section 5

Contractual Documentation

The agreements and licenses available at the links listed below are incorporated into and made a part of this proposal, which, together with any statements of work or other exhibits or schedules attached to this proposal, collectively form the agreement between Motorola Solutions and Saratoga County for the Services described in this proposal (the "Agreement"). By signing below, Saratoga County accepts and agrees to the terms of the Agreement. The Agreement is effective between Motorola Solutions and Saratoga County as of the date of the last signature below.

MOTOROLA

CUSTOMER

BY: _____

BY: _____

NAME: _____

NAME: _____

TITLE: _____

TITLE: _____

DATE: _____

DATE: _____

Document	Links
Addendum to a Primary Agreement	https://www.motorolasolutions.com/content/dam/msi/docs/msi-standards/terms-conditions/US_addendum_to_a_primary_agreement.pdf
Data Processing Addendum – U.S.	https://www.motorolasolutions.com/content/dam/msi/docs/msi-standards/terms-conditions/data_processing_addendum_US.pdf

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

February 21, 2024

To: Motorola Solutions, Inc. ("Motorola")
500 W. Monroe St.
Chicago, IL 60661

Re: Saratoga County ASTRO 25 Managed Detection and Response 24-166173 / Cybersecurity Services

Proposal / Quote Ref: Saratoga County ASTRO 25 Managed Detection and Response 24-166173 / Cybersecurity Services

Saratoga County does not have a formal purchase order system. This Notice to Proceed (NTP) serves as authorization for Motorola Solutions to place an order and invoice for the cybersecurity equipment and services as referenced on Saratoga County ASTRO 25 Managed Detection and Response 24-166173 / Cybersecurity Services for the purchase price of:

Description and Year	Price
ASTRO® 25 Managed Detection and Response – Year 1*	\$79,916.85
ASTRO® 25 Managed Detection and Response – Year 2	\$45,052.80
ASTRO® 25 Managed Detection and Response – Year 3	\$46,854.91
Total:	\$171,824.56

*Year 1 includes set up and installation fees.

Saratoga County agrees to pay Motorola Solutions "Net 30 days from receiving an invoice" for the equipment and services.

Title and Risk of Loss to Equipment shall pass to Customer upon shipment from Motorola. Unless otherwise agreed by the parties in writing, shipment will be made in a manner determined by Motorola. This NTP will take precedence with respect to conflicting or ambiguous terms.

Customer affirms that execution of this Agreement is the only Notice to Proceed that Motorola will receive for the term of this Agreement. Customer will not issue a purchase order or other funding documentation in order to pay Motorola per this Agreement. Customer affirms funding has been encumbered for this order in accordance with applicable law and will pay all proper invoices as received from Motorola solely against this Agreement.

Define Other Payment Milestones (if any):

Unless otherwise agreed upon in writing, invoices will be billed based on equipment shipped, services rendered, and standard payment terms and milestones. Once billed, invoices shall be sent and emailed to the Customer at the following address:

Invoices should reference: _____

The Equipment will be shipped to the Customer at the following address:

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

The ultimate destination address (if different from the ship to above) where the Equipment will be delivered to Customer is:

Customer may change shipment information by giving written or electronic notice to Motorola.

If you have any questions regarding this order, please feel free to contact Nayeem Modan, 917-620-5911, nayeem.modan@motorolasolutions.com

MOTOROLA SOLUTIONS

SARATOGA COUNTY

BY: _____

BY: _____

NAME: _____

NAME: _____

TITLE: _____

TITLE: _____

DATE: _____

DATE: _____

Cyber Addendum

Motorola Solutions Inc. ("**Motorola**") and the customer named in the Agreement to which this Cyber Addendum (the "**Addendum**") is attached ("**Customer**") hereby agree as follows:

Section 1. APPLICABILITY

1.1 This Addendum sets out terms applicable to Customer's purchase of cyber security services that are in addition to, and that may in some respects amend or supersede, terms in the Agreement pertaining to (i) Remote Security Update Service, Security Update Service, and Managed Detection & Response subscription services, among other subscription services ("**Subscription Services**"),(ii) professional services ("**Professional Services**"), and/or (iii) retainer services (i.e., professional services when expressly purchased as a block of pre-paid hours for use, subject to expiration, within a specified period across certain offered service categories ("**Retainer Services**") (all collectively herein, "**Services**").

Section 2. ADDITIONAL DEFINITIONS AND INTERPRETATION

2.1. "**Customer Contact Data**" has the meaning given to it in the DPA.

2.2 "**Customer Data**" has the meaning given to it in the DPA.

2.3 "**Data Processing Addendum**" or "**DPA**" means the Motorola Data Processing Addendum I applicable to processing of Customer Data for US customers, as updated, supplemented, or superseded from time to time. The DPA is attached to this Addendum and is incorporated into and made a part of this Addendum and the Agreement for all purposes pertaining to the contents of the DPA. Where terms or provisions in this Addendum or the Agreement conflict with terms or provisions of the DPA, the terms or provisions of the DPA will control with respect to the contents of the DPA

2.4 "**Feedback**" means comments or information, in oral or written form, given to Motorola by Customer or Authorized Users, including their end users, in connection with or relating to the Services. Any Feedback provided by Customer is entirely voluntary. Motorola may use, reproduce, license, and otherwise distribute and exploit the Feedback without any obligation or payment to Customer or Authorized Users. Customer represents and warrants that it has obtained all necessary rights and consents to grant Motorola the foregoing rights.

2.5 "**Motorola Data**" has the meaning given to it in the DPA.

2.6 "**Process**" or "**Processing**" has the meaning given to it in the DPA.

2.7 "**Service Use Data**" has the meaning given to it in the DPA.

2.8 "**Statement(s) of Work**" or "**SOW(s)**" as used in this Addendum means a statement of work, ordering document, accepted proposal, or other agreed upon engagement document issued under or subject to this Addendum. Mutually agreed upon SOWs may be attached hereto as Exhibit(s) , and/or are respectively incorporated by reference, each of which will be governed by the terms and conditions of this Addendum. Statements of Work may set out certain "**Deliverables,**" which include all written information (such as reports, specifications, designs, plans, drawings, or other technical or business information) that Motorola prepares for Customer in the performance of the Services and is obligated to provide to Customer under a SOW and this Addendum. The Deliverables, if any, are more fully described in the Statements of Work.

2.9 "**Third-Party Data**" has the meaning given to it in the DPA.

Section 3. LICENSE, DATA AND SERVICE CONDITIONS

3.1 Delivery of Cyber Services

3.1.1 All Professional Services will be performed in accordance with the performance schedule included in a SOW. Delivery of hours purchased as Retainer Services is at the onset of the applicable retainer period. Hours purchased as Retainer Services expire and are forfeited if not used within the Retainer period, subject to terms of use, expiration and extension, if any, as set out in the applicable SOW or ordering document. Professional Services described in a SOW will be deemed complete upon Motorola's performance of such Services or, if applicable, upon

exhaustion or expiration of the Retainer Services hours, whichever occurs first.

3.1.2 **Subscription Services.** Delivery of Subscription Services will occur upon Customer's receipt of credentials required for access to the Subscription Services or upon Motorola otherwise providing access to the Subscription Services platform.

3.1.3 To the extent Customer purchases equipment from Motorola ("**Supplied Equipment**"), title and risk of loss to the Supplied Equipment will pass to Customer upon installation (if applicable) or shipment by Motorola. Customer will take all necessary actions, reimburse freight or delivery charges, provide or obtain access and other rights needed and take other requested actions necessary for Motorola to efficiently perform its contractual duties. To the extent Supplied Equipment is purchased on an installment basis, any early termination of the installment period will cause the outstanding balance to become immediately due.

3.2 Motorola may use or provide Customer with access to software, tools, enhancements, updates, data, derivative works, and other materials which Motorola has developed or licensed from third parties (collectively, "**Motorola Materials**"). The Services, Motorola Data, Third-Party Data, and related documentation, are considered Motorola Materials. Notwithstanding the use of such materials in Services or Deliverables, the Motorola Materials are the property of Motorola or its licensors, and Motorola or its licensors retain all right, title and interest in and to the Deliverables and the Motorola Materials. Motorola grants Customer and Authorized Users a limited, non-transferable, non-sublicensable, and non-exclusive license to use the Services and associated Deliverables solely for Customer's internal business purposes.

3.2.1 Motorola may use, engage, resell, or otherwise interface with third-party software, hardware or services providers (such as, for example, third-party end point detection and response providers) and other sub-processors, who in turn may engage additional sub-processors to process personal data and other Customer Data. Customer agrees that such third-party software or services providers, sub-processors or their respective sub-processors may process and use personal and other Customer Data in accordance with and subject to their own respective licenses or terms and in accordance with applicable law. Customer authorizes and will provide and obtain all required notices and consents, if any, and comply with other applicable legal requirements, if any, with respect to such collection and use of personal data and other Customer Data by Motorola, and its subcontractors, sub-processors and/or third-party software, hardware or services providers.

3.2.2 In addition to terms set forth in this Addendum, certain components of the Subscription Services and the Motorola Materials may be governed by one or more third-party End User License Agreements ("**EULA**"), which include terms governing third-party software licensed to Motorola ("**Licensed Software**"), such as open source software, included in the Subscription Services and/or the Motorola Materials. Customer will comply, and ensure its Authorized Users comply, with such additional license agreements. EULAs for the Licensed Software are linked through the proposal to which this Addendum is attached.

3.3 To the extent Customer is permitted to access, use, or integrate Customer or third-party software, services, content, or data that is not provided by Motorola (collectively, "**Non-Motorola Content**") with or through the Services, or will use equipment or software not provided by Motorola, which may be required for use of the Services ("**Customer-Provided Equipment**"), Customer will obtain and continuously maintain all rights and licenses necessary for Motorola to efficiently perform all contemplated Services under this Addendum and will assume responsibility for operation and integration of such content and equipment.

3.4 **Ownership of Customer Data.** Customer retains all right, title and interest, including intellectual property rights, if any, in and to Customer Data. Motorola acquires no rights to Customer Data except those rights granted under this Addendum including the right to Process and use the Customer Data as set forth in the DPA. The Parties agree that with regard to the Processing of personal information that may be part of Customer Data, Customer is the controller and Motorola is the processor, and Motorola may engage sub-processors pursuant to the provisions of the DPA.

3.5 **Motorola Use of Customer Data.** Notwithstanding any provision to the contrary in this Addendum or any related agreement, and except as may be provided to the contrary in the DPA, and in addition to other uses and rights set out herein, Customer understands and agrees that Motorola may obtain, use and/or create and use, anonymized, aggregated and/or generalized Customer Data, such as data relating to actual and potential security threats and vulnerabilities, for its lawful business purposes, including improving its services and sharing and leveraging such information for the benefit of Customer, other customers, and other interested parties.

3.6 **Authorized Users.** Customer will ensure its employees and Authorized Users comply with the terms of this

Addendum and will be liable for all acts and omissions of its employees and Authorized Users. Customer is responsible for the secure management of Authorized Users' names, passwords and login credentials for access to products and Services. "**Authorized Users**" are Customer's employees, full-time contractors engaged for the purpose of supporting the products and Services that are not competitors of Motorola or its affiliates, and the entities (if any) specified in a SOW or otherwise approved by Motorola in writing (email from an authorized Motorola signatory accepted), which may include affiliates or other Customer agencies.

3.7 Beta or Proof of Concept Services. If Motorola makes any beta version of its Services ("**Beta Service**") available to Customer, or provides Customer a trial period or proof of concept period (or other demonstration) of the Services at reduced or no charge ("**Proof of Concept**" or "**POC Service**"), Customer may choose to use such Beta or POC Service at its own discretion, provided, however, that Customer will use the Beta or POC Service solely for purposes of Customer's evaluation of such Beta or POC Service, and for no other purpose. Customer acknowledges and agrees that all Beta or POC Services are offered "as-is" and without any representations or warranties or other commitments or protections from Motorola. Motorola will determine the duration of the evaluation period for any Beta or POC Service, in its sole discretion, and Motorola may discontinue any Beta or POC Service at any time. Customer acknowledges that Beta Services, by their nature, have not been fully tested and may contain defects or deficiencies. Notwithstanding any other provision of this Agreement, to the extent a future paid Service has been agreed upon subject to and contingent on the Customer's evaluation of a Proof of Concept Service, Customer may cancel such future paid Service as specified in the SOW or, if not specified, within a reasonable time before the paid Service is initiated.

Section 4. WARRANTY

4.1 CUSTOMER ACKNOWLEDGES, UNDERSTANDS AND AGREES THAT MOTOROLA DOES NOT GUARANTEE OR WARRANT THAT IT WILL DISCOVER ALL OF CUSTOMER'S SECURITY EVENTS (SUCH EVENTS INCLUDING THE UNAUTHORIZED ACCESS, ACQUISITION, USE, DISCLOSURE, MODIFICATION OR DESTRUCTION OF CUSTOMER DATA), THREATS, OR SYSTEM VULNERABILITIES. MOTOROLA DISCLAIMS ANY AND ALL RESPONSIBILITY FOR ANY AND ALL LOSS OR COSTS OF ANY KIND ASSOCIATED WITH SECURITY EVENTS, THREATS OR VULNERABILITIES WHETHER OR NOT DISCOVERED BY MOTOROLA. MOTOROLA DISCLAIMS ANY RESPONSIBILITY FOR CUSTOMER'S USE OR IMPLEMENTATION OF ANY RECOMMENDATIONS PROVIDED IN CONNECTION WITH THE SERVICES. IMPLEMENTATION OF RECOMMENDATIONS DOES NOT ENSURE OR GUARANTEE THE SECURITY OF THE SYSTEMS AND OPERATIONS EVALUATED. CUSTOMER SHALL BE RESPONSIBLE TO TAKE SUCH ACTIONS NECESSARY TO MITIGATE RISKS TO ITS OPERATIONS AND PROTECT AND PRESERVE ITS COMPUTER SYSTEMS AND DATA, INCLUDING CREATION OF OPERATIONAL WORKAROUNDS, BACKUPS AND REDUNDANCIES.

4.2. Customer acknowledges, understands and agrees that the Services and products or equipment provided by or used by Motorola to facilitate performance of the Services may impact or disrupt information systems. Except in instances of gross negligence in performing the Services, Motorola disclaims responsibility for costs incurred by Customer in connection with any such disruptions of and/or damage to Customer's or a third party's information systems, equipment, voice transmissions, data and Customer Data, including, but not limited to, inadequacies in or failure of Customer's network, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision or delivery of the Services.

4.3. Motorola warrants that Supplied Equipment, under normal use and service, will be free from material defects in materials and workmanship for one (1) year from the date of shipment, subject to Customer providing written notice to Motorola within that period. AS IT RELATES TO THE SUPPLIED EQUIPMENT, MOTOROLA DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

4.4 Motorola warrants that the Services will be performed in a professional and workmanlike manner and will conform in all material respects to the SOW(s). This warranty will be for a period of ninety (90) days following completion of the Services. If Motorola breaches this warranty, Customer's sole and exclusive remedy is to require Motorola to re-perform the non-conforming Services or to refund, on a pro-rata basis, the fees paid for the non-conforming Services. OTHER THAN THOSE WARRANTIES SET FORTH IN THIS SECTION 4, MOTOROLA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED. Customer acknowledges that the Deliverables for the Subscription Services may contain recommendations, suggestions or advice from Motorola to Customer (collectively, "recommendations"). Motorola makes no warranties concerning those recommendations, and Customer alone accepts responsibility for choosing whether and how to implement the recommendations and the results to be realized from implementing them.

4.5. Pass-Through Warranties. Notwithstanding any provision of this Addendum or any related agreement to the contrary, Motorola will have no liability for third-party software, hardware or services resold or otherwise provided by Motorola; provided, however, that to the extent offered by third-party software, hardware or services providers and to the extent permitted by law, Motorola will pass through to Customer express warranties provided by such third parties.

Section 5 LIMITATION OF LIABILITY

5.1. DISCLAIMER OF CONSEQUENTIAL DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, MOTOROLA, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE “**MOTOROLA PARTIES**”) WILL NOT BE LIABLE IN CONNECTION WITH SERVICES PROVIDED UNDER THIS ADDENDUM (WHETHER UNDER MOTOROLA’S INDEMNITY OBLIGATIONS, A CAUSE OF ACTION FOR BREACH OF CONTRACT, UNDER TORT THEORY, OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF MOTOROLA HAS BEEN ADVISED BY CUSTOMER OR ANY THIRD PARTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES AND WHETHER OR NOT SUCH DAMAGES OR LOSSES ARE FORESEEABLE.

5.2. DIRECT DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF THE MOTOROLA PARTIES, WHETHER BASED ON A CLAIM IN CONTRACT OR IN TORT, LAW OR EQUITY, RELATING TO OR ARISING OUT OF THIS ADDENDUM OR ANY RELATED OR UNDERLYING AGREEMENT, WILL NOT EXCEED THE FEES SET FORTH IN THE APPLICABLE SOW OR PRICING FOR THE SERVICES UNDER WHICH THE CLAIM AROSE. NOTWITHSTANDING THE FOREGOING, FOR ANY SUBSCRIPTION SERVICES, PROFESSIONAL SERVICES, OR FOR ANY RECURRING SERVICES, THE MOTOROLA PARTIES’ TOTAL LIABILITY FOR ALL CLAIMS RELATED TO SUCH PRODUCT OR SERVICES IN THE AGGREGATE WILL NOT EXCEED THE TOTAL FEES PAID FOR THE SERVICES TO WHICH THE CLAIM IS RELATED DURING THE CONSECUTIVE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FROM WHICH THE FIRST CLAIM AROSE. FOR AVOIDANCE OF DOUBT, THE LIMITATIONS IN THIS SECTION 5.2 APPLY IN THE AGGREGATE TO INDEMNIFICATION OBLIGATIONS ARISING OUT OF THIS ADDENDUM OR ANY RELATED AGREEMENTS.

5.3. ADDITIONAL EXCLUSIONS. NOTWITHSTANDING ANY OTHER PROVISION OF THIS ADDENDUM, THE PRIMARY AGREEMENT OR ANY RELATED AGREEMENT, MOTOROLA WILL HAVE NO LIABILITY FOR DAMAGES ARISING OUT OF (A) CUSTOMER DATA, INCLUDING ITS TRANSMISSION TO MOTOROLA, OR ANY OTHER DATA AVAILABLE THROUGH THE PRODUCTS OR SERVICES; (B) CUSTOMER-PROVIDED EQUIPMENT, NON-MOTOROLA CONTENT, THE SITES, OR THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, SERVICES, DATA, OR OTHER THIRD- PARTY MATERIALS, OR THE COMBINATION OF PRODUCTS AND SERVICES WITH ANY OF THE FOREGOING; (C) LOSS OF DATA OR HACKING, RANSOMWARE, OR OTHER THIRD-PARTY ATTACKS OR DEMANDS; (D) MODIFICATION OF PRODUCTS OR SERVICES BY ANY PERSON OTHER THAN MOTOROLA; (E) RECOMMENDATIONS PROVIDED IN CONNECTION WITH OR BY THE PRODUCTS AND SERVICES; (F) DATA RECOVERY SERVICES OR DATABASE MODIFICATIONS; OR (G) CUSTOMER’S OR ANY AUTHORIZED USER’S BREACH OF THIS ADDENDUM, THE PRIMARY AGREEMENT OR ANY RELATED AGREEMENT OR MISUSE OF THE PRODUCTS AND SERVICES; (H) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (I) DISRUPTION OF OR DAMAGE TO CUSTOMER’S OR THIRD PARTIES’ SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (J) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE SERVICES, OR INTERPRETATION, USE, OR MISUSE THEREOF; (K) TRACKING AND LOCATION-BASED SERVICES; OR (L) BETA SERVICES.

5.4. Voluntary Remedies. Motorola is not obligated to remedy, repair, replace, or refund the purchase price for the disclaimed issues in **Section 5.3 – Additional Exclusions**, but if Motorola agrees to provide Services to help resolve such issues, Customer will reimburse Motorola for its reasonable time and expenses, including by paying Motorola any fees set forth in this Addendum or separate order for such Services, if applicable.

5.5. Representations and Standards. Except as expressly set out in this Addendum or the applicable Motorola proposal or statement of work relating to the cyber products or services, or applicable portion thereof, Motorola makes no representations as to the compliance of Motorola cyber products and services with any specific standards, specifications or terms. For avoidance of doubt, notwithstanding any related or underlying agreement or terms, conformance with any specific standards, specifications, or requirements, if any, as it relates to cyber products and services is only as expressly set out in the applicable Motorola SOW or proposal describing such cyber products or services or the applicable (i.e., cyber) portion thereof. Customer represents that it is authorized to engage Motorola to

perform Services that may involve assessment, evaluation or monitoring of Motorola's or its affiliate's services, systems or products.

5.6. Wind Down of Services. In addition to any other termination rights, Motorola may terminate the Services, any SOW or subscription term, in whole or in part, in the event Motorola plans to cease offering the applicable Services to customers.

5.7. Third-Party Beneficiaries. This Addendum is entered into solely between, and may be enforced only by, the Parties. Each Party intends that the Addendum will not benefit, or create any right or cause of action in or on behalf of, any entity other than the Parties. Notwithstanding the foregoing, a licensor or supplier of third-party software, products or services included in the Services will be a direct and intended third-party beneficiary of this Addendum.

Data Processing Addendum _US

This Data Processing Addendum, including its Schedules and Annexes (“DPA”), forms part of the Master Customer Agreement (“MCA” or “Agreement”) to reflect the parties’ agreement with regard to the Processing of Customer Data, which may include Personal Data. In the event of a conflict between this DPA, the MCA or any Schedule, Annex or other addenda to the MCA, this DPA must prevail.

When Customer renews or purchases new Products or Services, the then-current DPA must apply and must not change during the applicable Term. When Motorola provides new features or supplements the Product or Service, Motorola may provide additional terms or make updates to this DPA that must apply to Customer’s use of those new features or supplements.

1. Definitions.

All capitalized terms not defined herein must have the meaning set forth in the Agreement.

“**Customer Data**” means data including images, text, videos, and audio, that are provided to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users, through the use of the Products and Services. Customer Data does not include Customer Contact Data, Service Use Data, other than that portion comprised of Personal Information, or Third Party Data.

“**Customer Contact Data**” means data Motorola collects from Customer, its Authorized Users, and their end users for business contact purposes, including without limitation marketing, advertising, licensing, and sales purposes.

“**Data Protection Laws**” means all data protection laws and regulations applicable to a Party with respect to the Processing of Personal Data under the Agreement.

“**Data Subjects**” means the identified or identifiable person to whom Personal Data relates.

“**Metadata**” means data that describes other data.

“**Motorola Data**” means data owned by Motorola and made available to Customer in connection with the Products and Services.

“**Personal Data**” or “**Personal Information**” means any information relating to an identified or identifiable natural person transmitted to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users as part of Customer Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Process**” or “**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Security Incident**” means an incident leading to the accidental or unlawful destruction, loss, alteration or disclosure of, or access to Customer Data, which may include Personal Data, while processed by Motorola.

“**Service Use Data**” means data generated about the use of the Products and Services through Customer’s use or Motorola’s support of the Products and Services, which may include Metadata, Personal Data, product performance and error information, activity logs, and date and time of use.

“**Sub-processor**” means other processors engaged by Motorola to Process Customer Data which may include Personal Data.

“**Third Party Data**” means information obtained by Motorola from publicly available sources or its third party content providers and made available to Customer through the Products or Services.

2. Processing of Customer Data

2.1. Roles of the Parties. The Parties agree that with regard to the Processing of Personal Data hereunder, Customer is the Controller and Motorola is the Processor who may engage Sub-processors pursuant to the requirements of **Section 6** entitled “Sub-processors” below.

2.2. Motorola’s Processing of Customer Data. Motorola and Customer agree that Motorola may only use and Process Customer Data, including the Personal Information embedded in Service Use Data, in accordance with applicable law and Customer’s documented instructions for the following purposes: (i) to perform Services and provide Products under the Agreement; (ii) analyze Customer Data to operate, maintain, manage, and improve Motorola products and services; and (iii) create new products and services. Customer agrees that its Agreement (including this DPA), along with the Product and Service Documentation and Customer’s use and configuration of features in the Products and Services, are Customer’s complete and final documented instructions to Motorola for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer’s Agreement. Customer represents and warrants to Motorola that Customer’s instructions, including appointment of Motorola as a Processor or sub-processor, have been authorized by the relevant controller. Customer Data may be processed by Motorola at any of its global locations and/or disclosed to Subprocessors. It is Customer’s responsibility to notify Authorized Users of Motorola’s collection and use of Customer Data, and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use. Customer represents and warrants to Motorola that it has complied with the terms of this provision.

2.3. Details of Processing. The subject-matter of Processing of Personal Data by Motorola hereunder, the duration of the Processing, the categories of Data Subjects and types of Personal Data are set forth on **Annex I** to this DPA.

2.4. Disclosure of Processed Data. Motorola must not disclose to or share any Customer Data with any third party except to Motorola’s sub-processors, suppliers and channel partners as necessary to provide the products and services unless permitted under this Agreement, authorized by Customer or required by law. In the event a government or supervisory authority demands access to Customer Data, to the extent allowable by law, Motorola must provide Customer with notice of receipt of the demand to provide sufficient time for Customer to seek appropriate relief in the relevant jurisdiction. In all circumstances, Motorola retains the right to comply with applicable law. Motorola must ensure that its personnel are subject to a duty of confidentiality, and will contractually obligate its sub-processors to a duty of confidentiality, with respect to the handling of Customer Data and any Personal Data contained in Service Use Data.

2.5. Customer’s Obligations. Customer is solely responsible for its compliance with all Data Protection Laws and establishing and maintaining its own policies and procedures to ensure such compliance. Customer must not use the Products and Services in a manner that would violate applicable Data Protection Laws. Customer must have sole responsibility for (i) the lawfulness of any transfer of Personal Data to Motorola, (ii) the accuracy, quality, and legality of Personal Data provided to Motorola; (iii) the means by which Customer acquired Personal Data, and (iv) the provision of any required notices to, and obtaining any necessary acknowledgements, authorizations or consents from Data Subjects. Customer takes full responsibility to keep the amount of Personal Data provided to Motorola to the minimum necessary for Motorola to perform in accordance with the Agreement. Customer must be solely responsible for its compliance with applicable Data Protection Laws.

2.6. Customer Indemnity. Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to Customer’s failure to comply with its obligations under this Agreement and/or applicable Data Protection Laws. Motorola will give Customer

prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

3. Service Use Data. Except to the extent that it is Personal Information, Customer understands and agrees that Motorola may collect and use Service Use Data for its own purposes, provided that such purposes are compliant with applicable Data Protection Laws. Service Use Data may be processed by Motorola at any of its global locations and/or disclosed to Subprocessors.

4. Third-Party Data and Motorola Data. Motorola Data and Third Party Data may be available to Customer through the Products and Services. Customer and its Authorized Users may use the Motorola Data and Third Party Data as permitted by Motorola and the applicable third-party data provider, as described in the Agreement or applicable Addendum. Unless expressly permitted in the Agreement or applicable Addendum, Customer must not, and must ensure its Authorized Users must not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer's internal business purposes or disclose the data to third parties;

(b) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (c) use such data in violation of applicable laws ; (d) use such data for activities or purposes where reliance upon the data could lead to death, injury, or property damage; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Additional restrictions may be set forth in the Agreement or applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data must immediately terminate upon termination or expiration of the applicable Addendum, Ordering Document, or the MCA. Further, Motorola or the applicable Third Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Data or Third-Party Data if Motorola or such Third Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or by Motorola's agreement with the applicable Third Party Data provider. Upon termination of Customer's rights to use of any Motorola Data or Third-Party Data, Customer and all Authorized Users must immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola has no liability for Third-Party Data or Motorola Data available through the Products and Services. Motorola and its Third Party Data providers reserve all rights in and to Motorola Data and Third- Party Data not expressly granted in an Addendum or Ordering Document.

5. Motorola as a Controller or Joint Controller. In all instances where Motorola acts as a Controller it must comply with the applicable provisions of the Motorola Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement as each may be updated from time to time. Motorola holds all Customer Contact Data as a Controller and must Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In instances where Motorola is acting as a Joint Controller with Customer, the Parties must enter into a separate addendum to the Agreement to allocate the respective roles as joint controllers.

6. Sub-processors.

6.1. Use of Sub-processors. Customer agrees that Motorola may engage Sub-processors who in turn may engage Sub-processors to Process Personal Data in accordance with the DPA. A current list of Sub-processors is set forth at **Annex III**. When engaging Sub-processors, Motorola must enter into agreements with the Sub-processors to bind them to obligations which are substantially similar or more stringent than those set out in this DPA.

6.2. Changes to Sub-processing. The Customer hereby consents to Motorola engaging Sub-processors to process Customer Data provided that: (i) Motorola must use its reasonable endeavours to provide at least 10 days' prior notice of the addition or removal of any Sub-processor, which may be given by posting details of such addition or removal at a URL provided to Customer in **Annex III**; (ii) Motorola imposes data protection terms on any Sub-processor it appoints that protect the Customer Data to the same standard provided for by this Addendum; and (iii) Motorola remains fully liable for any breach of this clause that is caused by an act, error or omission of its Sub-processor(s). The Customer may object to Motorola's

appointment or replacement of a Sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Motorola will either appoint or replace the Sub-processor or, if in Motorola's discretion this is not feasible, the Customer may terminate this Agreement and receive a pro-rata refund of any prepaid service or support fees as full satisfaction of any claim arising out of such termination.

6.3. Data Subject Requests. Motorola must, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject, including without limitation requests for access to, correction, amendment, transport or deletion of such Data Subject's Personal Data and, to the extent applicable, Motorola must provide Customer with commercially reasonable cooperation and assistance in relation to any complaint, notice, or communication from a Data Subject. Customer must respond to and resolve promptly all requests from Data Subjects which Motorola provides to Customer. Customer must be responsible for any reasonable costs arising from Motorola's provision of such assistance under this Section.

7. Data Transfers

Motorola agrees that it must not make transfers of Personal Data under this Agreement from one jurisdiction to another unless such transfers are performed in compliance with this Addendum and applicable Data Protection Laws. Motorola agrees to enter into appropriate agreements with its affiliates and Sub-processors, which will permit Motorola to transfer Personal Data to its affiliates and Sub-processors. Motorola agrees to amend as necessary its agreement with Customer to permit transfer of Personal Data from Motorola to Customer. Motorola also agrees to assist the Customer in entering into agreements with its affiliates and Sub-processors if required by applicable Data Protection Laws for necessary transfers.

8. Security. Motorola must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects. The appropriate technical and organizational measures implemented by Motorola are set forth in **Annex III**. In assessing the appropriate level of security, Motorola must weigh the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

9. Security Incident Notification. If Motorola becomes aware of a Security Incident, then Motorola must (i) notify Customer of the Security Incident without undue delay, (ii) investigate the Security Incident and apprise Customer of the details of the Security Incident and (iii) take commercially reasonable steps to stop any ongoing loss of Personal Data due to the Security Incident if in the control of Motorola. Notification of a Security Incident must not be construed as an acknowledgement or admission by Motorola of any fault or liability in connection with the Security Incident. Motorola must make reasonable efforts to assist Customer in fulfilling Customer's obligations under Data Protection Laws to notify the relevant supervisory authority and Data Subjects about such incident.

10. Data Retention and Deletion.

Except for anonymized Customer Data, as described above, or as otherwise provided under the Agreement, Motorola must delete all Customer Data no later than ninety (90) days following termination or expiration of the MCA or the applicable Addendum or Ordering Document unless otherwise required to comply with applicable law.

11. Audit Rights

11.1 Periodic Audit. Motorola will allow Customer to perform an audit of reasonable scope and duration of Motorola operations relevant to the Products and Services purchased under the Agreement, at Customer's sole expense, for verification of compliance with the technical and organizational measures set forth in **Annex II** if (i) Motorola notifies Customer of a Security Incident that results in actual compromise to the Products and/or Services purchased; or (ii) if Customer reasonably believes Motorola is not in compliance with its security commitments under this DPA, or (iii) if such audit is legally required by the Data Protection

Laws. Any audit must be conducted in accordance with the procedures set forth in **Section 11.3** of this DPA and may not be conducted more than one time per year. If any such audit requires access to confidential information of Motorola's other customers, suppliers or agents, such portion of the audit may only be conducted by Customer's nationally recognized independent third party auditors in accordance with the procedures set forth in **Section 11.3** of this DPA. Unless mandated by GDPR or otherwise mandated by law or court order, no audits are allowed within a data center for security and compliance reasons. Motorola must, in no circumstances, provide Customer with the ability to audit any portion of its software, products, and services which would be reasonably expected to compromise the confidentiality of any third party's information or Personal Data.

11.2 Satisfaction of Audit Request. Upon receipt of a written request to audit, and subject to Customer's agreement, Motorola may satisfy such audit request by providing Customer with a confidential copy of a Motorola's applicable most recent third party security review performed by a nationally recognized independent third party auditor, such as a SOC2 Type II report or ISO 27001 certification, in order that Customer may reasonably verify Motorola's compliance with national standards.

11.3 Audit Process. Customer must provide at least sixty days (60) days prior written notice to Motorola of a request to conduct the audit described in **Section 11.1**. All audits must be conducted during normal business hours, at applicable locations or remotely, as designated by Motorola. Audit locations, if not remote will generally be those location(s) where Customer Data is accessed, or Processed. The audit must not unreasonably interfere with Motorola's day to day operations. An audit must be conducted at Customer's sole cost and expense and subject to the terms of the confidentiality obligations set forth in the Agreement. Before the commencement of any such audit, Motorola and Customer must mutually agree upon the time, and duration of the audit. Motorola must provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not copy, Motorola security information or materials provided such auditor has executed an appropriate non-disclosure agreement. Motorola's policy is to share methodology and executive summary information, not raw data or private information. Customer must, at no charge, provide to Motorola a full copy of all findings of the audit.

12. Regulation Specific Terms

12.1. HIPAA Business Associate. If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of the MCA includes execution of the Motorola HIPAA Business Associate Agreement Addendum ("BAA"). Customer may opt out of the BAA by sending the following information to Motorola in a written notice under the terms of the Customer's Agreement: "Customer and Motorola agree that no Business Associate Agreement is required. Motorola is not a Business Associate of Customer's, and Customer agrees that it will not share or provide access to Protected Health Information to Motorola or Motorola's subprocessors."

12.2. FERPA. If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Motorola acknowledges that for the purposes of the DPA, Motorola is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Motorola agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Customer understands that Motorola may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer must be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Motorola to students (or, with respect to a student under 18 years of age and not in attendance at a post-secondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Motorola's possession as may be required under applicable law.

12.3. CJIS. Motorola agrees to support the Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy and must comply with the terms of the CJIS Security Addendum for the Term of this Agreement and such CJIS Security Addendum is incorporated herein by reference. Customer hereby consents to allow Motorola "screened" personnel as

defined by the CJIS Security Policy to serve as an authorized “escort” within the meaning of CJIS Security Policy for escorting unscreened Motorola personnel that require access to unencrypted Criminal Justice Information for purposes of Tier 3 support (e.g. troubleshooting or development resources). In the event Customer requires access to Service Use Data for its compliance with the CJIS Security Policy, Motorola must make such access available following Customer’s request. Notwithstanding the foregoing, in the event the MCA or applicable Ordering Document terminates, Motorola must carry out deletion of Customer Data in compliance with Section 10 herein and may likewise delete Service Use Data within the time frame specified therein. To the extent Customer objects to deletion of its Customer Data or Service Use Data and seeks retention for a longer period, it must provide written notice to Motorola prior to expiration of the 30 day period for data retention to arrange return of the Customer Data and retention of the Service Use Data for a specified longer period of time.

12.4. CCPA / CPRA. If Motorola is Processing Personal Data within the scope of the California Consumer Protection Act (“CCPA”) and/or the California Privacy Rights Act (“CPRA”) (collectively referred to as the “California Privacy Acts”), Customer acknowledges that Motorola is a “Service Provider” within the meaning of California Privacy Acts. Motorola must process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the California Privacy Acts, including under any “sale” exemption. In no event will Motorola sell any such data, nor will M. If a California Privacy Act applies, Personal Data must also include any data identified with the California Privacy Act or Act’s definition of personal data. Motorola shall provide Customer with notice should it determine that it can no longer meet its obligations under the California Privacy Acts, and the parties agree that, if appropriate and reasonable, Customer may take steps necessary to stop and remediate unauthorized use of the impacted Personal Data.

12.5 CPA, CTDPA, VCDPA. If Motorola is Processing Personal Data within the scope of the Colorado Privacy Rights Act (“CPA”), the Connecticut Data Privacy Act (“CTDPA”), or the Virginia Consumer Data Protection Act (“VCDPA”) Motorola will comply with its obligations under the applicable legislation, and shall make available to Customer all information in its possession necessary to demonstrate compliance with obligations in accordance with such legislation. **Motorola Contact.** If Customer believes that Motorola is not adhering to its privacy or security obligations hereunder, Customer must contact the Motorola Data Protection Officer at Motorola Solutions, Inc., 500 W. Monroe, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1.

Name: Customer

Role (controller/processor): Controller 2.

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Motorola Solutions, Inc.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Motorola acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the Customer Data:

- Employees, contractors, and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of personal data transferred

Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the Customer Data:

- Basic personal data (for example place of birth, street name, and house number (address), Agreemental code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video, and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP- addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location, and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);

- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified under applicable law or regulation.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data may be transferred on a continuous basis during the term of the MCA or other agreement to which this DPA applies.

Nature of the processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MCA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

Purpose(s) of the data transfer and further processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MCA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data retention is governed by Section 10 of this Data Processing Addendum

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Transfers to sub-processors will only be for carrying out the performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MCA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities. In accordance with the DPA, the data exporter agrees the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such sub-processors must be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymisation and encryption of personal data

Where technically feasible and when not impacting services provided:

- We minimize the data we collect to information we believe is necessary to communicate, provide, and support products and services and information necessary to comply with legal obligations.
- We encrypt in transit and at rest.
- We pseudonymize and limit administrative accounts that have access to reverse pseudonymisation.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

In order to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, Motorola Solutions Information Protection policy mandates the institutionalization of information protection throughout solution development and operational lifecycles. Motorola Solutions maintains dedicated security teams for its internal information security and its products and services. Its security practices and policies are integral to its business and mandatory for all Motorola Solutions employees and contractors. The Motorola Chief Information Security Officer maintains responsibility and executive oversight for such policies, including formal governance, revision management, personnel education and compliance. Motorola Solutions generally aligns to the NIST Cybersecurity Framework as well as ISO 27001.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Security Incident Procedures Motorola Solutions maintains a global incident response plan to address any physical or technical incident in an expeditious manner. Motorola maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. For each security breach that is a Security Incident, notification will be made in accordance with the Security Incident Notification section of this DPA.

Business Continuity and Disaster Preparedness Motorola maintains business continuity and disaster preparedness plans for critical functions and systems within Motorola's control that support the Products and Services purchased under the Agreement in order to avoid services disruptions and minimize recovery risks.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Motorola periodically evaluates its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Customer Data, including personal information. Motorola documents the results of these evaluations and any remediation activities taken in response to such evaluations. Motorola periodically has third party assessments performed against applicable industry standards, such as ISO 27001, 27017, 27018 and 27701.

Measures for user identification and authorisation

Identification and Authentication. Motorola uses industry standard practices to identify and authenticate users who attempt to access Motorola information systems. Where authentication mechanisms are based on passwords, Motorola requires that the passwords are at least eight characters long and are changed regularly. Motorola uses industry standard password protection practices, including practices designed to

maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Access Policy and Administration. Motorola maintains a record of security privileges of individuals having access to Customer Data, including personal information. Motorola maintains appropriate processes for requesting, approving and administering accounts and access privileges in connection with the Processing of Customer Data. Only authorized personnel may grant, alter or cancel authorized access to data and resources. Where an individual has access to systems containing Customer Data, the individuals are assigned separate, unique identifiers. Motorola deactivates authentication credentials on a periodic basis.

Measures for the protection of data during transmission

Data is generally encrypted during transmission within the Motorola managed environments. Encryption in transit is also generally required of any sub-processors. Further, protection of data in transit is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for the protection of data during storage

Data is generally encrypted during storage within the Motorola managed environments. Encryption in storage is also generally required of any sub-processors. Further, protection of data in storage is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for ensuring physical security of locations at which personal data are processed

Motorola maintains appropriate physical and environment security controls to prevent unauthorized access to Customer Data, including personal information. This includes appropriate physical entry controls to Motorola facilities such as card-controlled entry points, and a staffed reception desk to protect against unauthorized entry. Access to controlled areas within a facility will be limited by job role and subject to authorized approval. Use of an access badge to enter a controlled area will be logged and such logs will be retained in accordance with Motorola policy. Motorola revokes personnel access to Motorola facilities and controlled areas upon separation of employment in accordance with Motorola policies. Motorola policies impose industry standard workstation, device and media controls designed to further protect Customer Data, including personal information.

Measures for ensuring personnel security

Access to Customer Data. Motorola maintains processes for authorizing and supervising its employees, and contractors with respect to monitoring access to Customer Data. Motorola requires its employees, contractors and agents who have, or may be expected to have, access to Customer Data to comply with the provisions of the Agreement, including this Annex and any other applicable agreements binding upon Motorola.

Security and Privacy Awareness. Motorola must ensure that its employees and contractors remain aware of industry standard security and privacy practices, and their responsibilities for protecting Customer Data and Personal Data. This must include, but not be limited to, protection against malicious software, password protection, and management, and use of workstations and computer system accounts. Motorola requires periodic Information security training, privacy training, and business ethics training for all employees and contract resources

Sanction Policy. Motorola maintains a sanction policy to address violations of Motorola's internal security requirements as well as those imposed by law, regulation, or contract.

Background Checks. Motorola follows its standard mandatory employment verification requirements for all new hires. In accordance with Motorola internal policy, these requirements must be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation and any additional checks as deemed necessary by Motorola.

Measures for ensuring events logging

Protection, and Response. Motorola assesses organization's effectiveness annually via external assessors who report and share the assessment findings with Motorola Audit Services who tracks any identified remediations. For more information, please see the Motorola Trust Center at https://www.motorolasolutions.com/en_us/about/trust-center/security.html

Measures for certification/assurance of processes and products

Motorola performs internal Secure Application Review and Secure Design Review security audits and Production Readiness Review security readiness reviews prior to service release. Where appropriate, privacy assessments are performed for Motorola's products and services. A risk register is created as a result of internal audits with assignments tasked to appropriate personnel. Security audits are performed annually with additional audits as needed. Additional privacy assessments, including updated data maps, occur when material changes are made to the products or services. Further, Motorola Solution has achieved AICPA SOC2 Type 2 reporting and ISO/IEC 27001:2013 certification for many of its development and support operations.

Measures for ensuring data minimisation

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires data minimisation. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as data minimisation.

Measures for ensuring data quality

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires ensuring the quality and accuracy of data. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as ensuring data quality.

Measures for ensuring limited data retention

Motorola Solutions maintains a data retention policy that provides a retention schedule outlining storage periods for personal data. The schedule is based on business needs and provides sufficient information to identify all records and to implement disposal decisions in line with the schedule. The policy is periodically reviewed and updated.

Measures for ensuring accountability

To ensure compliance with the principle of accountability, Motorola Solutions maintains a Privacy Program which generally aligns its activities to both the Nymity Privacy Management and Accountability Framework and NIST Privacy Framework. The Privacy Program is audited annually by Motorola Solutions Audit Services.

Measures for allowing data portability and ensuring erasure

When subject to a data subject request to move, copy or transfer their personal data, Motorola Solutions will provide personal data to the Controller in a structured, commonly used and machine readable format. Where possible and if the Controller requests it, Motorola Solutions can directly transmit the personal information to

another organization.

For transfers to (sub-) processors

If, in the course of providing products and services under the MCA, Motorola Solutions transfers information containing personal data to third parties, said third parties will be subjected to a security assessment and bound by obligations substantially similar, but at least as stringent, as those included in this DPA.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorization of sub-processors. The controller has authorized the use of one or more of the following sub-processors:

1. Microsoft
2. Amazon
3. PagerDuty Inc
4. SalesForce
5. Twilio
6. Neustar
7. Google
8. VMWare
9. CrowdStrike
10. Palo Alto
11. AT&T
12. Okta
13. Cisco
14. Sophos
15. Tenable
16. Corelight



SARATOGA COUNTY
OFFICE OF EMERGENCY MANAGEMENT

6012 County Farm Road, Ballston Spa, New York 12020

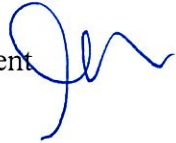
518-885-2232

emergencyservices@saratogacountyny.gov

518-885-2278 (Fax)

MEMO

To: John Warnt, Director of Purchasing

From: Andre Delvaux, Director of Emergency Management 

Date: February 12, 2024

Subject: Sole Source-Motorola Astro 25 Managed Detection and Response / ActiveEye Platform

The Motorola Astro 25 MDR provides radio network security element monitoring on a 24x7x365 basis through their ActiveEye platform. The unique benefit of this product is to identify and mitigate cyber threats that could threaten our mission-critical Motorola radio communications network / equipment.

There is no other vendor that is certified or approved to operate and deliver Motorola radio communications network / equipment cyber monitoring, nor is there another product that provides a substantially equivalent or similar benefit on our specific Motorola system.

Therefore, in consideration of these benefits, the provided quote, and customer discounts the purchase is viewed as reasonable and of great benefit in protecting the County of Saratoga's Motorola radio communications network / equipment against cyberintrusion.

Since this Motorola Astro 25 MDR Cybersecurity Service is specific to protecting their proprietary Motorola equipment, there is no possibility of competition from a competing dealer or distributor.

6/20/2023



SARATOGA COUNTY BOARD OF SUPERVISORS

RESOLUTION 165 - 2023 ²⁰²⁴

Introduced by Public Safety: Supervisors Lant, Butler, ~~Grasso, Hammond,~~ ^{Fish Murray}
~~Raymond, Tollisen and K. Veitch~~
~~Ostrander Wright Young~~

AUTHORIZING A ~~FOUR YEAR~~ ^{Three} MAINTENANCE SERVICE AGREEMENT WITH MOTOROLA SOLUTIONS, INC. FOR MAINTENANCE OF THE COUNTY'S PUBLIC SAFETY RADIO INFRASTRUCTURE

The purpose of the Motorola cybersecurity Astro 25 managed detection response hardware & equipment, installation/activation services & initial 1 year subscription period for the radio network infrastructure (MRI) followed by a two-year agreement with Motorola Solutions, Inc. for the Astro 25 MDR Subscription on the County's public Safety Radio Infrastructure.

WHEREAS, Motorola Solutions, Inc. has submitted a quote for the renewal of its maintenance service agreement for the continued maintenance of the County's 800 MHz radio system, covering non-warranty radio system infrastructure, cyber intrusion and further upgrades to the County's 800 MHz Emergency Radio System with upgrade to include hardware, software and implementation services for a term of four years commencing on July 1, 2023 and continuing through June 30, 2027 at a total cost of \$3,833,160.77; and

WHEREAS, our Public Safety Committee and the Director of the Office of Emergency Management have recommended that the County's maintenance agreement with Motorola Solutions, Inc. be renewed for an additional term of four years commencing on July 1, 2023, and continuing through June 30, 2027 at a cost of \$3,833,160.77; now, therefore, be it

RESOLVED, that the Chair of the Board is authorized to execute a renewal agreement with Motorola Solutions, Inc. of Chicago, Illinois, for the provision of maintenance services for the County's 800 MHz Public Safety Radio infrastructure covering all non-warranty radio system infrastructure, cyber intrusion, and further upgrades to the County's 800 MHz Emergency Radio System with upgrade to include hardware, software and implementation services, for a term of four years commencing on July 1, 2023 and continuing through June 30, 2027 at a cost not to exceed \$3,833,160.77; and it is further

RESOLVED, that the form and content of such agreement shall be subject to the approval of the County Attorney.

BUDGET IMPACT STATEMENT: No Budget Impact. Funds are included in the Department Budget.

June 20, 2023 Regular Meeting
Motion to Adopt: Supervisor Hammond
Second: Supervisor Barrett
AYES (210214): Eric Connolly (11831), Joseph Grasso (4328), Philip C. Barrett (19014.5), Jonathon Schopf (19014.5), Eric Butler (6500), Diana Edwards (819), Jean Raymond (1333), Michael Smith (3525), Kevin Veitch (8004), Arthur M. Wright (1976), Kevin Tollisen (25662), Mark Hammond (17130), Thomas Richardson (5163), Scott Ostrander (18800), Theodore Kusnierz (16202), Sandra Winney (2075), Matthew E. Veitch (14245.5), Edward D. Kinowski (9022), John Lawler (8208), John Lant (17361)

NOES (0):

ABSENT (~~25296~~): Willard H. Peck (5242), ~~Thomas N. Wood, III (5808)~~, ~~Tara N. Gaston (14245.5)~~