

County of Albany

Harold L. Joyce
Albany County Office Building
112 State Street - Albany, NY 12207



Meeting Agenda

Thursday, May 26, 2022

5:30 PM

Held Remotely

Public Safety Committee

PREVIOUS BUSINESS:

1. APPROVING PREVIOUS MEETING MINUTES
2. PUBLIC HEARING ON PROPOSED LOCAL LAW NO. "B" FOR 2022: A LOCAL LAW OF THE COUNTY OF ALBANY AMENDING LOCAL LAW NO. 6 FOR 2017, TO EXEMPT THE COUNTY FROM WIRELESS COMMUNICATION SURCHARGES
3. PUBLIC HEARING ON PROPOSED LOCAL LAW NO. "C" FOR 2022 A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING THE SALE OF USED CATALYTIC CONVERTERS
4. LOCAL LAW NO. "B" FOR 2022: A LOCAL LAW OF THE COUNTY OF ALBANY AMENDING LOCAL LAW NO. 6 FOR 2017, TO EXEMPT THE COUNTY FROM WIRELESS COMMUNICATION SURCHARGES
5. LOCAL LAW NO. "C" FOR 2022: A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING THE SALE OF USED CATALYTIC CONVERTERS

CURRENT BUSINESS:

6. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES REGARDING THE FY2020 CRITICAL INFRASTRUCTURE GRANT PROGRAM
7. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES REGARDING THE FY2020 CYBER SECURITY GRANT PROGRAM
8. AMENDING THE 2022 SHERIFF'S OFFICE BUDGET: PERSONNEL CHANGES
9. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION AND AN AGREEMENT WITH THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES REGARDING THE 2022 STATEWIDE INTEROPERABLE COMMUNICATIONS GRANT - TARGETED PROGRAM

10. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION AND AN AGREEMENT WITH THE RESEARCH FOUNDATION FOR MENTAL HYGIENE FOR GRANT FUNDING

County of Albany

*Harold L. Joyce
Albany County Office Building
112 State Street - Albany, NY 12207*



Meeting Minutes

Thursday, April 28, 2022

5:30 PM

Held Remotely

Public Safety Committee

PREVIOUS BUSINESS:

Present: William M. Clay, Robert J. Beston, Zach Collins, Frank J. Commisso, Gary W. Domalewicz, Beroro T. Efekoro, Gilbert F. Ethier, Patrice Lockart and Sean E. Ward

1. APPROVING PREVIOUS MEETING MINUTES

A motion was made that the previous meeting minutes be approved. The motion carried by a unanimous vote.

2. PUBLIC HEARING ON PROPOSED LOCAL LAW NO. "B" FOR 2022: A LOCAL LAW OF THE COUNTY OF ALBANY AMENDING LOCAL LAW NO. 6 FOR 2017, TO EXEMPT THE COUNTY FROM WIRELESS COMMUNICATION SURCHARGES

This proposal was tabled at the request of the Sponsor.

3. LOCAL LAW NO. "B" FOR 2022: A LOCAL LAW OF THE COUNTY OF ALBANY AMENDING LOCAL LAW NO. 6 FOR 2017, TO EXEMPT THE COUNTY FROM WIRELESS COMMUNICATION SURCHARGES

This Local Law was tabled at the request of the Sponsor.

CURRENT BUSINESS:**4. PUBLIC HEARING ON PROPOSED LOCAL LAW NO. "C" FOR 2022 A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING THE SALE OF USED CATALYTIC CONVERTERS**

This proposal was tabled at the request of the Sponsor.

5. LOCAL LAW NO. "C" FOR 2022: A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING THE SALE OF USED CATALYTIC CONVERTERS

This Local Law was tabled at the request of the Sponsor.

6. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES REGARDING THE EXPLOSIVE DETECTION CANINE TEAM PROGRAM

A motion was made to move the proposal forward with a positive recommendation. The motion carried by a unanimous vote.

7. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES REGARDING THE TECHNICAL RESCUE AND URBAN SEARCH AND RESCUE GRANT PROGRAM

A motion was made to move the proposal forward with a positive recommendation. The motion carried by a unanimous vote.

8. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES REGARDING THE FY2020 HAZMAT GRANT

A motion was made to move the proposal forward with a positive recommendation. The motion carried by a unanimous vote.

9. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE UNITED STATES DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE ASSISTANCE REGARDING REIMBURSEMENT FOR THE INCARCERATION OF CRIMINAL ALIENS

A motion was made to move the proposal forward with a positive recommendation. The motion carried by a unanimous vote.

10. AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE NEW YORK STATE CANAL CORPORATION REGARDING REIMBURSEMENT FOR MARINE PATROL SERVICES

A motion was made to move the proposal forward with a positive recommendation. The motion carried by a unanimous vote.

11. ADOPTING THE REVISED ALBANY COUNTY FIRE AND MUTUAL AID PLAN

A motion was made to move the proposal forward with a positive recommendation. The motion carried by a unanimous vote.

12. AMENDING THE 2022 SHERIFF'S OFFICE BUDGET: PERSONNEL CHANGES

A motion was made to move the proposal forward with a positive recommendation. The motion carried by a unanimous vote.

LOCAL LAW “B” FOR 2022

A LOCAL LAW OF THE COUNTY OF ALBANY AMENDING LOCAL LAW NO. 6 FOR 2017, TO EXEMPT THE COUNTY FROM WIRELESS COMMUNICATION SURCHARGES

Introduced:

By Ms. McLean Lane:

BE IT ENACTED BY THE LEGISLATURE OF THE COUNTY OF ALBANY AS FOLLOWS:

SECTION 1. Legislative Intent

The purpose of this Local Law is to exempt Albany County from the payment of wireless communication surcharges on County owned or leased wireless telephones.

SECTION 2. Amendment

Section 2, of Local Law No. 6 for 2017, “A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REPEALING THE WIRELESS COMMUNICATION SURCHARGE AUTHORIZED BY ARTICLE 6 OF THE COUNTY LAW OF THE STATE OF NEW YORK SET FORTH IN ALBANY COUNTY LOCAL LAW 9 FOR 2009 AND IMPOSING THE WIRELESS COMMUNICATIONS SURCHARGES PURSUANT TO THE AUTHORITY OF TAX LAW §186-g,” is amended by the addition of a new subdivision (d) as follows:

(d) Limitations. No wireless communication surcharge set forth in this Local Law shall be imposed upon any wireless telephone owned or leased by Albany County.

SECTION 3. Severability

If any clause, sentence, paragraph, subdivision, or part of this Local Law or the application thereof to any person, firm, or corporation, or circumstance, shall be adjusted by any court of competent jurisdiction to be invalid or unconstitutional, such order or judgement shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, or part of this Local Law or in its application to the person, individual, firm, or corporation or circumstance, directly involved in the controversy in which such judgment or order shall be rendered.

SECTION 4. Effective Date

This law shall take effect immediately upon its filing with the Secretary of State.

RESOLUTION NO. 107

PUBLIC HEARING ON PROPOSED LOCAL LAW NO. “B” FOR 2022: A LOCAL LAW OF THE COUNTY OF ALBANY AMENDING LOCAL LAW NO. 6 FOR 2017, TO EXEMPT THE COUNTY FROM WIRELESS COMMUNICATION SURCHARGES

Introduced: 3/14/22

By Ms. McLean Lane:

RESOLVED, By the County Legislature of the County of Albany that a public hearing on proposed Local Law No. “B” for 2022, “A Local Law of the County of Albany Amending Local Law No. 6 for 2017, to Exempt the County from Wireless Communication Surcharges” to be held remotely by the Albany County Legislature at 7:15 p.m. on Tuesday, April 26, 2022, with participation information to be made available on the Albany County website, and the Clerk of the County Legislature is directed to cause notice of such hearing to be published containing the necessary information in accordance with the applicable provisions of law.

Referred to Law and Public Safety Committees – 3/14/22

LOCAL LAW NO. "C" FOR 2022

A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING THE SALE OF USED CATALYTIC CONVERTERS

Introduced: 04/11/22

By Messrs. Cleary and A. Joyce:

BE IT ENACTED by the Albany County Legislature as follows:

Section 1. Title

This local law shall be known as "Regulating the Sale of Used Catalytic Converters."

Section 2. Legislative Intent

The Legislature hereby finds and determines that there has been an increase in thefts of used catalytic converters from vehicles in the County for the purpose of reselling the converters as scrap metal.

The Legislature further finds and determines that catalytic converter theft is a crime that is affecting an increasing number of families in the County. Accordingly, we must enact strategies and penalties to combat the problem.

The Legislature further finds and determines that requiring scrap metal recyclers doing business in Albany County to delay payment to sellers of used catalytic converters for at least fourteen (14) days after receipt of such devices will allow law enforcement additional time to investigate the theft of used catalytic converters and further discourage criminal conduct.

The Legislature also finds and determines that requiring scrap metal recyclers to maintain records of the purchase of used catalytic converters will assist law enforcement in the investigation of thefts of such devices.

Section 3. Purpose

The purpose of this Local Law to discourage the theft of catalytic converters from vehicles by requiring scrap metal recyclers doing business in Albany County to delay payments to sellers of used catalytic converters for at least fourteen (14) days after receipt and requiring scrap metal recyclers to maintain records of the purchase of such devices for three (3) years in order to aid law enforcement in the investigation of the theft of such devices.

Section 4. Definitions

As used in this local law, the following terms shall have the meanings indicated:

"Catalytic Converter" means a catalytic converter or other equipment or feature constituting an operational element of a motor vehicle's air pollution control system or mechanism required by federal or state law or by any rules or regulations promulgated pursuant thereto, as amended from time to time.

"Repair Shop" means a business enterprise that repairs vehicles and is certified by the New York State Department of Motor Vehicles,

"Scrap Metal Recycler" means a vehicle dismantler, salvage pool, mobile car crusher, itinerant vehicle collector or scrap processor doing business in Albany County; but shall not include a dealer registered pursuant to section four hundred fifteen of the New York Vehicle and Traffic Law, an insurance company, a governmental agency, a person in whose name a certificate of title, registration or other ownership document has been issued for the vehicle from which the Used Catalytic Converter was removed, or a Repair Shop.

"Used Catalytic Converter" means a Catalytic Converter that was previously installed in a vehicle and which has been removed from such vehicle in whole or in part.

Section 5. Prohibition.

No Scrap Metal Recycler shall purchase or take possession of, including for purposes of recycling or rebuilding, a Used Catalytic Converter from any person or entity other than a dealer registered pursuant to section four hundred fifteen of the Vehicle and Traffic Law, an insurance company, a governmental agency, a person in whose name a certificate of title or other ownership document has been issued for the vehicle from which the catalytic converter was removed, a Repair Shop, or a person registered or certified or issued an identification number for the vehicle under the Vehicle and Traffic Law.

Section 6. Maintenance of Records by Scrap Metal Recycler.

Each Scrap Metal Recycler who purchases or takes possession of, including for purposes of recycling or rebuilding, a Used Catalytic Converter shall record the purchase of the Used Catalytic Converter documenting the date of purchase, the name of seller, the seller's address or, in the case that the seller is an individual, the seller's residence address by street, number, city, village or town, the seller's driver's license number or information from a government issued photographic identification card, if any, or by such description as will reasonably locate the seller, or, if the seller is a Repair Shop, the Repair Shop's New York State Department of Motor Vehicles certification number. Such record shall be preserved by the Scrap Metal Recycler for

a period of three years from the date of receipt of the Used Catalytic Converter. Such records shall be available for inspection by any law enforcement authority with jurisdiction over the Scrap Metal Recycler.

Each Scrap Metal Recycler shall cause the record of purchase of the Used Catalytic Converter to be signed by the seller or his or her agent. It shall be unlawful for any seller or agent to refuse to furnish such information or to furnish incorrect or incomplete information. The Scrap Metal Recycler shall make and retain a copy of the government issued photographic identification card used to verify the identity of the person from whom the Used Catalytic Converter was purchased or obtained and shall retain the copy in a separate book, register or electronic archive for three (3) years from the date of purchase. Such records shall be available for inspection by any law enforcement agency having jurisdiction over the Scrap Metal Recycler.

Section 7. Payments.

Payments by any Scrap Metal Recycler to a business, agency or private citizen who turns in a catalytic converter for scrap will be issued through check, with a copy of the check being held by the Scrap Metal Recycler for three years from the date of disbursement. Such records shall be available for inspection by any law enforcement agency having jurisdiction over the Scrap Metal Recycler.

Section 8. Violations

(A) Any person that violates this Local Law shall:

- (1) be guilty of a class A misdemeanor, and
- (2) upon conviction thereof, shall be punished by a fine not to exceed \$300 for the first offense, \$500 for the second offense, and \$1,000 for each subsequent offense.

(B) This Local Law shall be enforced by any local law enforcement agency having jurisdiction over the Scrap Metal Recycler located within the County of Albany.

Section 9. Severability.

If any clause, sentence, paragraph, section or chapter of this local law shall be adjudged by any court of competent jurisdiction to be invalid, such determination shall not affect, impair or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, section or chapter thereof directly involved in the proceeding in which such adjudication shall have been rendered. This local law shall not supersede any applicable state or federal laws or regulations with regard to the subject matters set forth herein.

Section 10. Effective Date and Applicability

This local law shall be effective ninety (90) days subsequent to filing in the Office of the Secretary of State and shall apply to all transactions occurring on or after the effective date of this local law.

Referred to Law and Public Safety Committees – 4/11/22

RESOLUTION NO. 138

**PUBLIC HEARING ON PROPOSED LOCAL LAW NO. “C” FOR 2022 A
LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING
THE SALE OF USED CATALYTIC CONVERTERS**

Introduced: 4/11/22

By Mr. Cleary:

RESOLVED, By the County Legislature of the County of Albany that a public hearing on proposed Local Law No. “C” for 2022, “A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING THE SALE OF USED CATALYTIC CONVERTERS” to be held by the Albany County Legislature at 7:15 p.m. on Tuesday, May 24, 2022, with participation information to be made available on the Albany County website, and the Clerk of the County Legislature is directed to cause notice of such hearing to be published containing the necessary information in accordance with the applicable provisions of law.

Referred to Law and Public Safety Committees – 4/11/22

LOCAL LAW “B” FOR 2022

A LOCAL LAW OF THE COUNTY OF ALBANY AMENDING LOCAL LAW NO. 6 FOR 2017, TO EXEMPT THE COUNTY FROM WIRELESS COMMUNICATION SURCHARGES

Introduced: 3/14/22

By Ms. McLean Lane:

BE IT ENACTED BY THE LEGISLATURE OF THE COUNTY OF ALBANY AS FOLLOWS:

SECTION 1. Legislative Intent

The purpose of this Local Law is to exempt Albany County from the payment of wireless communication surcharges on County owned or leased wireless telephones.

SECTION 2. Amendment

Section 2, of Local Law No. 6 for 2017, “A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REPEALING THE WIRELESS COMMUNICATION SURCHARGE AUTHORIZED BY ARTICLE 6 OF THE COUNTY LAW OF THE STATE OF NEW YORK SET FORTH IN ALBANY COUNTY LOCAL LAW 9 FOR 2009 AND IMPOSING THE WIRELESS COMMUNICATIONS SURCHARGES PURSUANT TO THE AUTHORITY OF TAX LAW §186-g,” is amended by the addition of a new subdivision (d) as follows:

(d) Limitations. No wireless communication surcharge set forth in this Local Law shall be imposed upon any wireless telephone owned or leased by Albany County.

SECTION 3. Severability

If any clause, sentence, paragraph, subdivision, or part of this Local Law or the application thereof to any person, firm, or corporation, or circumstance, shall be adjusted by any court of competent jurisdiction to be invalid or unconstitutional, such order or judgement shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, or part of this Local Law or in its application to the person, individual, firm, or corporation or circumstance, directly involved in the controversy in which such judgment or order shall be rendered.

SECTION 4. Effective Date

This law shall take effect immediately upon its filing with the Secretary of State.

Referred to Law and Public Safety Committees – 3/14/22

LOCAL LAW NO. "C" FOR 2022

A LOCAL LAW OF THE COUNTY OF ALBANY, NEW YORK REGULATING THE SALE OF USED CATALYTIC CONVERTERS

Introduced: 04/11/22

By Messrs. Cleary and A. Joyce:

BE IT ENACTED by the Albany County Legislature as follows:

Section 1. Title

This local law shall be known as "Regulating the Sale of Used Catalytic Converters."

Section 2. Legislative Intent

The Legislature hereby finds and determines that there has been an increase in thefts of used catalytic converters from vehicles in the County for the purpose of reselling the converters as scrap metal.

The Legislature further finds and determines that catalytic converter theft is a crime that is affecting an increasing number of families in the County. Accordingly, we must enact strategies and penalties to combat the problem.

The Legislature further finds and determines that requiring scrap metal recyclers doing business in Albany County to delay payment to sellers of used catalytic converters for at least fourteen (14) days after receipt of such devices will allow law enforcement additional time to investigate the theft of used catalytic converters and further discourage criminal conduct.

The Legislature also finds and determines that requiring scrap metal recyclers to maintain records of the purchase of used catalytic converters will assist law enforcement in the investigation of thefts of such devices.

Section 3. Purpose

The purpose of this Local Law to discourage the theft of catalytic converters from vehicles by requiring scrap metal recyclers doing business in Albany County to delay payments to sellers of used catalytic converters for at least fourteen (14) days after receipt and requiring scrap metal recyclers to maintain records of the purchase of such devices for three (3) years in order to aid law enforcement in the investigation of the theft of such devices.

Section 4. Definitions

As used in this local law, the following terms shall have the meanings indicated:

"Catalytic Converter" means a catalytic converter or other equipment or feature constituting an operational element of a motor vehicle's air pollution control system or mechanism required by federal or state law or by any rules or regulations promulgated pursuant thereto, as amended from time to time.

"Repair Shop" means a business enterprise that repairs vehicles and is certified by the New York State Department of Motor Vehicles,

"Scrap Metal Recycler" means a vehicle dismantler, salvage pool, mobile car crusher, itinerant vehicle collector or scrap processor doing business in Albany County; but shall not include a dealer registered pursuant to section four hundred fifteen of the New York Vehicle and Traffic Law, an insurance company, a governmental agency, a person in whose name a certificate of title, registration or other ownership document has been issued for the vehicle from which the Used Catalytic Converter was removed, or a Repair Shop.

"Used Catalytic Converter" means a Catalytic Converter that was previously installed in a vehicle and which has been removed from such vehicle in whole or in part.

Section 5. Prohibition.

No Scrap Metal Recycler shall purchase or take possession of, including for purposes of recycling or rebuilding, a Used Catalytic Converter from any person or entity other than a dealer registered pursuant to section four hundred fifteen of the Vehicle and Traffic Law, an insurance company, a governmental agency, a person in whose name a certificate of title or other ownership document has been issued for the vehicle from which the catalytic converter was removed, a Repair Shop, or a person registered or certified or issued an identification number for the vehicle under the Vehicle and Traffic Law.

Section 6. Maintenance of Records by Scrap Metal Recycler.

Each Scrap Metal Recycler who purchases or takes possession of, including for purposes of recycling or rebuilding, a Used Catalytic Converter shall record the purchase of the Used Catalytic Converter documenting the date of purchase, the name of seller, the seller's address or, in the case that the seller is an individual, the seller's residence address by street, number, city, village or town, the seller's driver's license number or information from a government issued photographic identification card, if any, or by such description as will reasonably locate the seller, or, if the seller is a Repair Shop, the Repair Shop's New York State Department of Motor Vehicles certification number. Such record shall be preserved by the Scrap Metal Recycler for

a period of three years from the date of receipt of the Used Catalytic Converter. Such records shall be available for inspection by any law enforcement authority with jurisdiction over the Scrap Metal Recycler.

Each Scrap Metal Recycler shall cause the record of purchase of the Used Catalytic Converter to be signed by the seller or his or her agent. It shall be unlawful for any seller or agent to refuse to furnish such information or to furnish incorrect or incomplete information. The Scrap Metal Recycler shall make and retain a copy of the government issued photographic identification card used to verify the identity of the person from whom the Used Catalytic Converter was purchased or obtained and shall retain the copy in a separate book, register or electronic archive for three (3) years from the date of purchase. Such records shall be available for inspection by any law enforcement agency having jurisdiction over the Scrap Metal Recycler.

Section 7. Payments.

Payments by any Scrap Metal Recycler to a business, agency or private citizen who turns in a catalytic converter for scrap will be issued through check, with a copy of the check being held by the Scrap Metal Recycler for three years from the date of disbursement. Such records shall be available for inspection by any law enforcement agency having jurisdiction over the Scrap Metal Recycler.

Section 8. Violations

(A) Any person that violates this Local Law shall:

- (1) be guilty of a class A misdemeanor, and
- (2) upon conviction thereof, shall be punished by a fine not to exceed \$300 for the first offense, \$500 for the second offense, and \$1,000 for each subsequent offense.

(B) This Local Law shall be enforced by any local law enforcement agency having jurisdiction over the Scrap Metal Recycler located within the County of Albany.

Section 9. Severability.

If any clause, sentence, paragraph, section or chapter of this local law shall be adjudged by any court of competent jurisdiction to be invalid, such determination shall not affect, impair or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, section or chapter thereof directly involved in the proceeding in which such adjudication shall have been rendered. This local law shall not supersede any applicable state or federal laws or regulations with regard to the subject matters set forth herein.

Section 10. Effective Date and Applicability

This local law shall be effective ninety (90) days subsequent to filing in the Office of the Secretary of State and shall apply to all transactions occurring on or after the effective date of this local law.

Referred to Law and Public Safety Committees – 4/11/22



DANIEL P. MCCOY
COUNTY EXECUTIVE

DANIEL LYNCH
DEPUTY COUNTY EXECUTIVE

COUNTY OF ALBANY
DEPARTMENT OF MANAGEMENT AND BUDGET
DIVISION OF INFORMATION SERVICES
112 STATE STREET, ROOM 500
ALBANY, NEW YORK 12207
PHONE: (518) 447-7200 FAX: (518) 447-3000
www.albanycounty.com

M. DAVID REILLY
COMMISSIONER

PERRY J. BLANCHARD
CHIEF INFORMATION OFFICER

DATE: April 29, 2022
TO: Hon. Andrew Joyce, Chairman
Albany County Legislature
112 State Street, Room 710
Albany, New York 12207
RE: RLA – Authorization to apply for NYS Division of Homeland Security & Emergency Services’ (DHSES) FY22 Critical Infrastructure Grant

Dear Chairman Joyce,

The Division of Information Services is requesting permission to apply for the NYS Division of Homeland Security and Emergency Services’ FY2020 Critical Infrastructure Grant Program. Information Services is requesting to apply for grant funding to purchase networking equipment for the County Disaster Recovery Site that is nearing end of life and is in need of upgrade. NYS DHSES is accepting applications for projects up to \$50,000, and Albany County will be applying for \$38,848.20. There is no cost/County match associated with this grant application.

Should you have any questions, please don’t hesitate to contact me. Thank you for your consideration of this matter.

Sincerely,

Perry J Blanchard
Chief Information Officer
Division of Information Services

cc: Hon. Dennis A. Feeney, Majority Leader
Hon. Frank A. Mauriello, Minority Leader
Rebekah Kennedy, Majority Counsel
Arnis Zilgme, Minority Counsel



County of Albany

Harold L. Joyce
Albany County Office
Building
112 State Street - Albany,
NY 12207

Legislation Text

File #: TMP-3285, **Version:** 1

REQUEST FOR LEGISLATIVE ACTION

Description (e.g., Contract Authorization for Information Services):

Authorization for Division of Information Services to Apply for NYS Division of Homeland Security & Emergency Services' (DHSES) FY2020 Critical Infrastructure Grant Program

Date: 4/29/2022
Submitted By: Perry Blanchard
Department: Division of Information Services
Title: Chief Information Officer
Phone: 518-447-4962
Department Rep.
Attending Meeting: Perry Blanchard / Dave Reilly

Purpose of Request:

- Adopting of Local Law
- Amendment of Prior Legislation
- Approval/Adoption of Plan/Procedure
- Bond Approval
- Budget Amendment
- Contract Authorization
- Countywide Services
- Environmental Impact/SEQR
- Home Rule Request
- Property Conveyance
- Other: (state if not listed) Click or tap here to enter text.

CONCERNING BUDGET AMENDMENTS

Increase/decrease category (choose all that apply):

- Contractual
- Equipment
- Fringe
- Personnel

- Personnel Non-Individual
- Revenue

Increase Account/Line No.: Click or tap here to enter text.
Source of Funds: Click or tap here to enter text.
Title Change: Click or tap here to enter text.

CONCERNING CONTRACT AUTHORIZATIONS

Type of Contract:

- Change Order/Contract Amendment
- Purchase (Equipment/Supplies)
- Lease (Equipment/Supplies)
- Requirements
- Professional Services
- Education/Training
- Grant

New

Submission Date Deadline 5/5/2022

- Settlement of a Claim
- Release of Liability
- Other: (state if not listed) Click or tap here to enter text.

Contract Terms/Conditions:

Party (Name/address):

NYS Division of Homeland Security and Emergency Services
1220 Washington Avenue
State Office Campus, Building 7A
Albany, NY 12226

Additional Parties (Names/addresses):

Click or tap here to enter text.

Amount/Raise Schedule/Fee: \$38,848.20
Scope of Services: Grant application to purchase critical network switching for the Albany County Business Continuity / Disaster Recovery sites

Bond Res. No.: Click or tap here to enter text.
Date of Adoption: Click or tap here to enter text.

CONCERNING ALL REQUESTS

Mandated Program/Service: Yes No
If Mandated Cite Authority: Click or tap here to enter text.

Is there a Fiscal Impact: Yes No
Anticipated in Current Budget: Yes No

County Budget Accounts:

Revenue Account and Line: Click or tap here to enter text.
Revenue Amount: Click or tap here to enter text.

Appropriation Account and Line: Click or tap here to enter text.
Appropriation Amount: Click or tap here to enter text.

Source of Funding - (Percentages)

Federal:	0
State:	100
County:	0
Local:	0

Term

Term: (Start and end date) Start TBD - August 31, 2023
Length of Contract: TBD

Impact on Pending Litigation

If yes, explain: Yes No
Click or tap here to enter text.

Previous requests for Identical or Similar Action:

Resolution/Law Number: Click or tap here to enter text.
Date of Adoption: Click or tap here to enter text.

Justification: The Albany County Division of Information Services (DIS) is seeking legislative authorization to apply for the NYS Division of Homeland Security and Emergency Services' FY2020 Critical Infrastructure Grant Program. The DIS is looking to upgrade its server and storage capacity at its disaster recovery (DR) site. In the event of a disaster at the County's main data center due to a cyber-event or a natural disaster, the DR site would be activated to serve the needs of the employees and the county's constituents. The remaining items that need to be purchased are modern, higher capacity network switches to allow access to applications and data to the network. The grant application is due May 5, 2022. DIS is applying for \$38,848.20 (out of an allowable \$50,000) in funding to cover the costs associated with the switching upgrades at the Disaster Recovery site. There is no County match associated with this grant.



Bill To:
Albany County
Dept of General Services
112 State St Suite 1300
Albany, New York 12207-2023
United States

Ship To:
Albany County
Dept of General Services
112 State St Suite 1300
Albany, New York 12207-2023
United States

Quote Number: Q-37215
Quote Date: 04/27/2022
Expiration Date: 05/27/2022

Client: Albany County
Account Number: 0013803
Payment Terms: Net 30
Primary Contact: Perry Blanchard
Quote Name: County Switching

Quoted by: Scott Butler
P 908-566-0917 | **E** scott.butler@corebts.com
Account Manager: Bryon Perkins
P (518) 831-8940 | **E** bryon.perkins@corebts.com

Qty	Item Number	Description	Term (Months)	Billing Frequency	Price	Ext Price
5	C9300L-48P-4X-E	Catalyst 9300L 48p PoE, Network Essentials, 4x10G Uplink		Prepaid	\$3,500.99	\$17,504.95
5	CON-SNT-C93004X4	SNTC-8X5XNBD Catalyst 9300L 48p	60	Prepaid	\$2,899.05	\$14,495.25
5	C9300L-NW-E-48	C9300L Network Essentials, 48-port license		Prepaid	\$0.00	\$0.00
5	PWR-C1-BLANK	Config 1 Power Supply Blank		Prepaid	\$0.00	\$0.00
15	FAN-T2	Cisco Type 2 Fan Module		Prepaid	\$0.00	\$0.00
5	S9300LUK9-173	Catalyst 9300L XE 17.3 UNIVERSAL		Prepaid	\$0.00	\$0.00
5	PWR-C1-715WAC-P	715W AC 80+ platinum Config 1 Power Supply		Prepaid	\$0.00	\$0.00
5	C9300L-SPS-NONE	No Secondary Power Supply Selected		Prepaid	\$0.00	\$0.00
5	CAB-TA-NA	North America AC Type A Power Cable		Prepaid	\$0.00	\$0.00
5	C9300L-SSD-NONE	No SSD Card Selected		Prepaid	\$0.00	\$0.00
5	C9300L-DNA-E-48	C9300L Cisco DNA Essentials, 48-port license	36	Prepaid	\$0.00	\$0.00
5	C9300L-DNA-E-48-3Y	C9300L Cisco DNA Essentials, 48-port, 3 Year Term license	36	Prepaid	\$630.88	\$3,154.40
5	NETWORK-PNP-LIC	Network Plug-n-Play License for zero-touch device deployment		Prepaid	\$0.00	\$0.00
5	NETWORK-PNP-NONE	Network Plug-n-Play Opt Out SKU		Prepaid	\$0.00	\$0.00
5	C9300L-STACK-KIT	C9300L-STACK-KIT		Prepaid	\$714.72	\$3,573.60
10	C9300L-STACK	Catalyst 9300L Stack Module		Prepaid	\$0.00	\$0.00
5	STACK-T3-50CM	50CM Type 3 Stacking Cable for C9300L		Prepaid	\$0.00	\$0.00
3	SFP-10G-LRM-IO	SFP+ 1310nm LR MMF 220m 10G DDM Cisco SFP-10G-LRM Compatible		Prepaid	\$40.00	\$120.00
1	NY-CONTRACT-PM20800	NYS OGS Cisco Umbrella contract#PM20800		Prepaid	\$0.00	\$0.00
1	CORE-NOFGHT	No freight charge to client		Prepaid	\$0.00	\$0.00
					Subtotal:	\$38,848.20

First Invoice Amount: \$38,848.20
Quote Subtotal: \$38,848.20
Estimated Sales Tax: \$0.00
Quote Total: \$38,848.20

Notes:

Accepted by: _____ **Printed name:** _____ **Date:** _____

To ensure fastest processing, please send purchase order/signed quote to purchase.orders@corebts.com and CC the two individuals listed above or fax to (317) 573-1665. If changes are required, please request a revised quote. Thank you for your business!

By accepting this quote you agree to Core's Standard Terms and Conditions which can be found at <https://corebts.com/legal/T&C>.

This proposal is confidential, and shall not be used or disclosed, in whole or in part, for any purpose other than evaluation within the client organization. This quote shall expire on the "Expiration Date" above. Notwithstanding the foregoing, all product and pricing information is based on the latest information available and is subject to change without notice, including at any time prior to the expiration of the quote. All prices are in U.S. dollars. Prices and tax rates are valid in the U.S. only and are subject to change. Sales tax is based on the "ship to" address on your purchase order. Please indicate your taxability status on your purchase order. Product availability is subject to change and cannot be guaranteed. All shipments are FOB origin. Appropriate freight charges will be added at the time of invoice. Please note that this quote may include items which may be subject to vendor restocking fees if returned, or may not be returnable if not defective (all returns are subject to vendor RMA approval). Core passes through all vendor restocking terms and fees without modification, markup, or additional fees.

Cancellation of any licensing or services with a fixed term or indicated as non-cancellable shall incur a termination fee equal to 100% of the cost of the remainder of the term, payable to Core in full upon the effective termination date. If First Invoice Amount is less than the Quote Total this is due to the fact that some or all items have a billing frequency of more than one instance, please consult the billing frequency listed for each item. First Invoice Amount is estimated and may not include shipping/freight, estimated sales tax, and incidental charges.



Homeland Security and Emergency Services

FY2020 Critical Infrastructure Grant Program Request for Applications (RFA)

Application Deadline: May 5, 2022 by 5:00 pm

In order to ensure adequate time to respond, substantive written questions regarding this Request for Applications will be accepted until 12:00 noon on April 28, 2022.

Technical Assistance for E-Grants will not be available after 5:00 pm on May 5, 2022.

Table of Contents

I. Introduction	3
II. Eligibility	4
III. FY2020 Critical Infrastructure Grant Program Objectives	5
A. Identify a Government Owned Critical Infrastructure or Mass Gathering/Special Event Site	5
B. Complete a Risk Assessment and Evaluate the Capabilities of Local First Responders	5
C. Reduce Risk and Enhance Capabilities.....	5
IV. Authorized Program Expenditures	5
A. Permissible Costs.....	5
B. Costs Not Permissible	6
V. Application Format and Content.....	6
A. Format	6
B. Required Application Content.....	6
C. Required Budget Summary	7
D. Bonus Points Criteria	7
VI. Application Evaluation Criteria	8
A. Tier 1 Criteria	8
B. Tier 2 Criteria	8
VII. Checklist of Required Documents	10
VIII. Timeline.....	10
IX. Approval and Notification of Award.....	10
X. Administration of Grant Contracts	11
A. Issuing Agency.....	11
B. Filing an Application	11
C. Reservation of Rights.....	11
D. Term of the Contract	13
E. Payment and Reporting Requirements of Grant Awardees.....	13
F. Satisfactory Progress	19
G. General Specifications	20
H. Special Conditions	21
XI. Questions.....	22
Exhibit A: Allowable Costs Matrix	23
Exhibit B: Risk Instructions and Template Assessment and Capability Evaluation	25
Exhibit C: Examples of Government Owned Critical Infrastructure, Mass Gathering and Special Event Sites	28
Exhibit D: Best Practices for Preparing an Effective Grant Application	29

I. Introduction

The purpose of this Request for Applications (RFA) is to solicit applications for up to \$50,000 in federal FY2020 State Homeland Security Program (SHSP) funding made available by the NYS Division of Homeland Security and Emergency Service (DHSES) for critical infrastructure and/or mass gathering/special event site protection. There is a total of up to \$500,000 in funding that is made available under this grant program and funding will be awarded competitively based on the submission of completed and eligible applications.

The FY2020 Critical Infrastructure Grant Program (CIGP) advances a common understanding of risk management. Applicants select a critical infrastructure site¹ or mass gathering/special event site and complete a risk assessment. As a portion of that risk assessment, first responders assess their capability to prevent and protect against attacks on the site. Grant funding is then applied to mitigate vulnerabilities identified in the risk assessment or enhance first responder's capabilities.

The purpose and goals of the Critical Infrastructure Grant Program are:

- To ensure that New York State is providing tools and opportunities in support of the vision and major mission areas of the New York State Homeland Security Strategy. This grant program supports three of the five mission areas: prevention, protection, and mitigation.
- To ensure that major urban areas within New York State have access to a grant program to protect critical infrastructure.
- To ensure that grant dollars are being applied to identified vulnerabilities or gaps in protection efforts.
- To reduce the overall risk to critical infrastructure by:
 - Maintaining competitive funding to mitigate identified needs.
 - Fostering a forum for state partnering on local critical infrastructure security, safety, and planning.

The FY2020 CIGP is focused on government owned critical infrastructure sites and government owned mass gathering/special event sites. Please note, federal or state-owned sites are not eligible under this grant program. Examples of types of projects that are allowable are listed below for your reference:

- **Government Owned Critical Infrastructure:** Examples of government owned sites include, but are not limited to, government office buildings (city/town halls), emergency services (emergency operations centers, 911 centers, police or fire stations), water systems (water treatment facilities, water distribution, wastewater treatments) or government owned stadiums.

¹ Critical infrastructure, as defined by New York State, means "systems, assets, places or things, whether physical or virtual, so vital to the state that the disruption, incapacitation or destruction of such systems, assets, places or things could jeopardize the health, safety, welfare or security of the state, its residents or its economy."

- **Government Owned Mass Gathering/Special Event Site:** Government property, where events such as, but not limited to, major community festivals, races, concerts, or games are held. These events must be reoccurring (but not necessarily the same event) and located or held on government owned or leased property that has definable geographic boundaries. The event or location must pose special security concerns, such as population surges and other factors that require additional law enforcement or emergency resources.

II. Eligibility

Only specific counties and units of local government within targeted counties are eligible to apply for the FY2020 Critical Infrastructure Grant Program. Units of local governments include: counties, cities, towns, and/or villages. Privately owned and not-for-profit sites are **not** eligible to receive funding under the FY2020 CIGP.

Applicants must be located in New York City or one of the following targeted counties: Albany, Broome, Dutchess, Erie, Herkimer, Livingston, Madison, Monroe, Nassau, Niagara, Oneida, Onondaga, Ontario, Orange, Orleans, Oswego, Putnam, Rensselaer, Rockland, Saratoga, Schenectady, Schoharie, Suffolk, Tioga, Wayne, Westchester, and Yates. These targeted counties are a composition of the State's top seven Metropolitan Statistical Areas (MSAs).

The application must be coordinated with at least two (2) agencies with prevention and/or protection responsibilities at the selected site. These must be law enforcement, fire department, emergency management or public works agencies.

The applying unit of local government may submit **only one** application under the FY2020 CIGP. Multiple applications are unallowable, and only one application for either a government owned critical infrastructure or a government owned mass gathering/special event site (as described in the definitions in Section I. Introduction) will be accepted.

- **Nationwide Cyber Security Review (NCSR) Requirement:** All applicants that receive funding through the FY2020 CIGP will be required to participate in the Nationwide Cyber Security Review (NCSR) as a condition of receiving federal homeland security funding. Details concerning accessing and registering for the NCSR can be found at: <https://www.cisecurity.org/ms-isac/services/ncsr/>. It is advised that you coordinate closely with your Information Security Officer (ISO) to determine if your jurisdiction has already completed this requirement – please note that you are only required to submit once for your specific jurisdiction.

III. FY2020 Critical Infrastructure Grant Program Objectives

DHSES has identified the following objectives for the FY2020 Critical Infrastructure Grant Program:

A. Identify a Government Owned Critical Infrastructure or Mass Gathering/Special Event Site

DHSES recognizes that localities know their communities best. The CIGP was designed to allow for applicants to prioritize and select a **government owned critical infrastructure site** or **fixed government owned site with reoccurring events** for this targeted grant program.

The FY2020 CIGP is limited to government owned critical infrastructure and mass gathering/special event sites. Applicants are responsible for ensuring ownership or leased status of the selected sites.

B. Complete a Risk Assessment and Evaluate the Capabilities of Local First Responders

The CIGP supports the “assess risk” process of the risk management framework of the National Infrastructure Protection Plan (NIPP) by requiring partners to complete a risk assessment at the identified critical infrastructure site or mass gathering/special event site prior to submitting an application. Local first responders must also complete a capability assessment to identify equipment, training, and/or exercise needs to prevent and protect against attacks at the critical infrastructure site. Both the risk and capability assessments must be completed using the template in “Exhibit B.”

All jurisdictions have participated in the County Emergency Preparedness Assessment (CEPA) process and should have a good idea of the risks and capabilities within their jurisdiction and where gaps in capabilities may exist. Leveraging available data from the CEPA may be useful in this section.

C. Reduce Risk and Enhance Capabilities

Based upon the risk and capability assessments, develop a budget detailing how FY2020 CIGP funds will be used to mitigate risks identified through the risk assessment process and/or enhance capabilities identified through the risk management process.

IV. Authorized Program Expenditures

A. Permissible Costs

Grant funding under the FY2020 Critical Infrastructure Grant Program may be used for certain equipment, training, and exercise costs allowable under the State Homeland Security Program (SHSP). Due to the specialized nature of this grant program, applications must mitigate specific vulnerabilities at the selected government owned critical infrastructure or government owned mass gathering/special event sites and enhance first responder capabilities to prevent and protect the selected site. Applicants should refer to “Exhibit A - Allowable Costs Matrix,” for detailed information on allowable costs.

- **Grants Programs Directorate Information Bulletin (IB) 426:** This bulletin is in support of Executive Order 13809 and rescinds restrictions placed on certain

controlled equipment that was previously articulated in 407 and 407a issued by the Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA). In addition, IB#426 outlines specific policy and documentation requirements for some equipment which continue to require DHS/FEMA approval. If your agency requests equipment identified as requiring pre-approval and are disapproved, your grant award will decrease by the amount of the disapproved item(s). Please refer to “Exhibit A” for the specific category of equipment.

B. Costs Not Permissible

Organizational, management and administrative, construction, and personnel costs are not allowable under the FY2020 CIGP. Applicants should refer specifically to “Exhibit A” of this RFA to obtain clear guidance on allowable costs under this grant program.

V. Application Format and Content

A. Format: Grant applications **MUST** be submitted via the automated E-Grants System operated by DHSES. The system allows an agency to complete an application electronically and submit it over the Internet using a secure portal. If upon reading this RFA you are interested in completing a grant application, and you have not previously been registered to use the DHSES E-Grants system, your agency will need to register and be assigned a user name and password. The Registration Request Form and a detailed tutorial on how to use the E-Grants system is available at: <https://www.dhses.ny.gov/targeted-grants>.

B. Required Application Content: The following questions must be addressed in your FY2020 Critical Infrastructure Grant Program application. You must answer these specific grant questions in the “Questions” tab in E-Grants:

1. Site Identification: Applicants must provide the site name of the government owned critical infrastructure site or government owned mass gathering/special event site.
2. Site Selection Questions (for the government owned critical infrastructure site or government owned mass gathering/special event site):
 - Applicants must provide a description of the government owned critical infrastructure site or government owned mass gathering/special event site selected and the critical role it has within the community;
 - Describe the relationship between the selected government owned infrastructure site or government owned mass gathering/special event site and the local first responder community. Be sure to include the criteria used for the selection of the partnering agencies.
 - Explain **in detail** how this site was selected and prioritized over other sites. **In doing so, explain why the site was selected and discuss the other sites that were considered.**

3. **Partnering Agencies:** The application must be coordinated with at least two (2) agencies with prevention and/or protection responsibilities at the selected site. These must be law enforcement, fire department, emergency management, or public works agencies. **Applicants must describe in detail the coordination efforts between agencies and how these efforts are undertaken, such as, but not limited to, event plan development, and if applicable, describing joint training and/or exercises done at the potential site.**
4. **Overall Application Questions:** Applicants must summarize how the application meets the overall goals and objectives of the FY2020 CIGP, as well as establish the **need** for this grant funding.
5. If the application is successful, it must show how the projects implemented will be maintained and sustained at the critical infrastructure location;
6. Given the time constraints for spending down grants funds, please explain how the project will be implemented by **August 31, 2023**.
7. Risk Assessment and Capability Evaluation: Refer to “Exhibit B” for instructions on completing the Risk Assessment and Capability Evaluation. Attach the completed excel document to your project in E-Grants.

C. Required Budget Summary: Under the Budget tab in E-Grants applicants are asked to enter in the following:

1. **Budget Item Description:** Applicants must provide a description of the item to be implanted at the government owned critical infrastructure site or government owned mass gathering/special event site.
2. **Justification:** Explain **in detail**, justification of the budgetary item and the capability enhancement the budgeted item can provide at the selected site.

D. Bonus Points Criteria: Due to the highly competitive nature of this program and to maximize the impacts of funding across the state, Bonus Points will be awarded to applicants who are applying for government owned mass gathering/special event sites and/or have not been previously funded under the Critical Infrastructure Grant Program. All government owned mass gathering/special event site applications will be awarded two (2) Bonus Points while all previously unfunded applicants will be awarded three (3) Bonus Points. These Bonus Points will be added to their overall application scores.

Any jurisdiction awarded funding must comply with the National Environmental Policy Act (NEPA). If you need additional information regarding Environmental and Historic Preservation (EHP) compliance, please visit our website at <https://www.dhSES.ny.gov/grant-programs>. Additionally, the Authorized Equipment List (AEL) has been updated to include a notification in the individual equipment under the FEMA Grants Programs column if an EHP review is necessary, which can be found at: <https://www.fema.gov/authorized-equipment-list>.

VI. Application Evaluation Criteria

The following multi-tiered criteria will be used by DHSES to evaluate each application and to determine grant awards. DHSES will select a multi-agency review panel to evaluate applications. All grant awards are approved by the Commissioner of DHSES.

A. Tier 1 Criteria

Tier 1 criteria are rated either “yes” or “no” and serve as a baseline review by DHSES to determine if applicants are eligible and have appropriately submitted all the required application materials prior to review by the multi-agency review committee. If any of the answers are “no,” the application will be immediately disqualified without further review and consideration for an award.

1. Was the application submitted on time?
2. Was the application submitted via E-Grants?
3. Was the application complete including the required exhibits? (the **required** Risk Assessment and Capability Evaluation must be attached in E-Grants by the submission due date)
4. Did the application meet the eligibility requirements?
 - a. From a targeted county/NYC.
 - b. From a unit of local government.
 - c. Was coordinated with two or more agencies.
 - d. Selected a government owned critical infrastructure site or a mass gathering/special event site (**Multiple submissions regardless of the project funding type, will result in both applications being disqualified without further review**).

B. Tier 2 Criteria

Applications meeting the Tier 1 review set forth above will be reviewed and evaluated competitively using the criteria specified below. Scores per criterion will be totaled to establish a ranked list of eligible applications for consideration of awards. At the sole discretion of DHSES, applicants may be disqualified due to untimely submission of any requested supporting documentation.

Tier 2 Evaluation Criteria	Point Score Range
Overall Application	0-10 points
Identification of (Government Owned) Critical Infrastructure or Mass Gathering/Special Event Site	0-10 points
Risk Assessment and Capability Evaluation	0-50 points
Budget	0-20 points
Risk Score ¹	0-10 points
Subtotal	100 Points Maximum
Bonus Points: Mass Gathering/Special Event Site Applications	2 points
Bonus Points: Previously Unfunded Applicants	3 points
Grant Management Performance History ²	0-10 point (Subtracted off the top of final average score)
Total	105 Points Maximum

Applications receiving the highest average score based upon panel review will be selected for recommendation to the Commissioner of DHSES for award. The total scores will be averaged and ranked in order from highest to lowest. The State reserves the right, for the purpose of ensuring the completeness and comparability of proposals, to analyze submissions and make adjustments or normalize submissions in the proposals, including applicants' technical assumptions, and underlying calculations and assumptions used to support the computation of costs, or to apply such other methods, as it deems necessary to make comparisons. In the event of a tie score where one or more applicants may not be fully funded, the applicant with the highest score in the "Overall Application" section will be ranked higher. Proposed budgets will be reviewed, and items deemed inappropriate, unallowable, or inconsistent with project or program activities will be eliminated. Grants in the amount of the budgets, as adjusted, will be made to the highest-ranking applicants until funds are insufficient to fund the next ranking application in full. The State reserves the right, at its discretion, to make amendments and/or alter funding levels of one or more applicants based on any new information discovered that would have originally affected the scoring or to not award funding to any application with a final average score of 60 or less.

¹ DHSES is committed to distributing homeland security funding based upon risk. The Division of Homeland Security and Emergency Services will award each applicant up to 10 points in competitive scoring. Core variables which will be considered in the risk score include, county threat score (0-3 points); population and population density (0-4 points); critical infrastructure (0-1); and mass gatherings (0-2).

² Per the Code for Federal Regulations (CFR) 2 CFR Part 200, DHSES is required to assess the risk posed by applicants of federal funding passed through DHSES. For previously funded applicants, DHSES will assess how well they have historically managed federal grant funds. This will include reporting compliance, successful award spend-down, and program objective compliance. Once a prospective applicant's final overall average score is determined by the review panel, DHSES may subtract up to 10 points based on its "Grant Management Performance History" criteria.

VII. Checklist of Required Documents

- Applications must be submitted to DHSES via E-Grants with the required attachments uploaded.
- Completed Risk Assessment and Capability Evaluation (“Exhibit B”) must be submitted as an **attachment** to your project in E-Grants.

VIII. Timeline

DHSES must receive completed grant applications by **5:00 p.m. on May 5, 2022**. Applications received after the due date and time will not be considered. Applications must be submitted via DHSES E-Grants System. Please note that E-Grants Technical Assistance will only be available during business hours on the date the application is due. Furthermore, all written questions must be submitted to DHSES by **12:00 noon on April 28, 2022** to ensure that a timely response is provided to the applicant.

Grant applicants can expect to be notified of award decisions sometime in June / July 2022.

IX. Approval and Notification of Award

The Commissioner of DHSES will provide oversight of the grant review process. The Commissioner will announce the final grant award decisions based on the review panel’s rating of applications and recommendations. DHSES will notify all applicants in writing as to final grant award determinations. Nothing herein requires or prohibits DHSES to approve grant funding for any one applicant, certain applicants, all applicants or no applicants. Any disbursement of an award is contingent upon entering into a contract with DHSES, as explained in further detail below.

Pursuant to Section 163(9)(c) of the State Finance Law, any unsuccessful Bidder may submit a written request for a debriefing regarding the reasons that the Bid submitted by the Bidder was not selected for award. Requests for a debriefing must be made within 15 calendar days of notification by DHSES that the Bid submitted by the Bidder was not selected for award. An unsuccessful Bidder’s written request for a debriefing shall be submitted to DHSES Director of Grants Program Administration. The debriefing shall be scheduled within 10 business days of receipt of the written request by DHSES or as soon as practicable under the circumstances.

Due to the competitive nature of this grant application proposed changes to the scope of the program may not be approved post-award.

X. Administration of Grant Contracts

DHSES will negotiate and develop a grant contract with the applicant based on the contents of the submitted application and intent of the grant program as outlined in this RFA. The grant contract is subject to approval by the NYS Office of the Attorney General and the Office of the State Comptroller before grant funding may actually be disbursed to reimburse project expenses.

The period of performance for contracts supported by the FY2020 Critical Infrastructure Grant Program funds will be determined once awards have been approved but cannot extend beyond **August 31, 2023**. Although the contract format may vary, the contract will include such standard terms and conditions included in DHSES grant contracts available for review on the DHSES website: <https://www.dhSES.ny.gov/grant-reporting-forms>.

Applicants agree to adhere to all applicable state and federal regulations.

A. Issuing Agency

This RFA is issued by DHSES, which is responsible for the requirements specified herein and for the evaluation of all applications.

B. Filing an Application

Grant applications must be submitted via the automated DHSES E-Grants System. The system allows an agency to complete an application electronically and submit it over the Internet using a secure portal. If, upon reading this RFA, you are interested in completing a grant application and you have not previously been registered to use the DHSES E-Grants system, your agency will need to register and be assigned a username and password. The Registration Request Form can be found at the following Internet address: <https://www.dhSES.ny.gov/e-grants>.

A detailed tutorial on how to use the E-Grants system can also be found at the following Internet address: <https://www.dhSES.ny.gov/targeted-grants>. It will guide you in a step-by-step process through the E-Grants application submission.

C. Reservation of Rights

The issuance of this RFA and the submission of a response or the acceptance of such response by DHSES does not obligate DHSES in any manner. DHSES reserves the right to:

1. Reject any and all applications received in response to this RFA;
2. Withdraw the RFA at any time at DHSES' sole discretion;
3. Make an award under the RFA in whole or in part;
4. Disqualify any applicant whose conduct and/or application fails to conform to the requirements of the RFA;
5. Seek clarifications and revisions of the applications;

6. Use application information obtained through site visits, management interviews and the State's investigation of an applicant's qualifications, experience, ability or financial standing, and any material or information submitted by the applicant in response to DHSES' request for clarifying information in the course of evaluation and/or selection under the RFA;
7. Prior to the application opening, amend the RFA specifications to correct errors or oversights, or to supply additional information, as it becomes available;
8. Prior to the application opening, direct applicants to submit application modifications addressing subsequent RFA amendments;
9. Change any of the scheduled dates;
10. Eliminate any non-mandatory, non-material specifications that cannot be complied with by all the prospective applicants;
11. Waive any requirements that are not material;
12. Negotiate with successful applicants within the scope of the RFA in the best interests of the State;
13. Conduct contract negotiations with the next responsible applicant, should DHSES be unsuccessful in negotiating with the selected applicant;
14. Utilize any and all ideas submitted in the applications received;
15. Unless otherwise specified in the RFA, every offer is firm and not revocable for a period of 60 days from the application opening; and,
16. Communicate with any applicant at any time during the application process to clarify responses and /or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of an applicant's proposal and/or to determine an applicant's compliance with the requirements of this RFA.
17. Award grants based on geographic or regional considerations to serve the best interests of the State.
18. Terminate, renew, amend or renegotiate contracts with applicants at the discretion of DHSES.
19. Periodically monitor the applicant's performance in all areas mentioned above, in addition to the activities in the contract.
20. Revoke funds awarded to an applicant, or enforce any available sanction against any applicant, who materially alters the activities or is in material noncompliance under the grant award, or who does not implement an approved project within 60 days of the final contract approval.
21. Consider all applications and documentation submitted as State agency records subject to the New York State Freedom of Information Law (Public Officers Law, Article 6). Any portion of the application that an applicant believes constitutes proprietary or critical infrastructure information entitled to confidential handling, as an exception to the Freedom of Information Law, must be clearly and specifically designated in the application.
22. Applicants funded through this program agree to provide DHSES, upon request at any time during the life of the grant contract, such cooperation and information deemed necessary by DHSES to ascertain: (1) the nature and extent of any threats or hazards that may pose a risk to the applicant; and (2) the status of any corresponding applicant or applicant plans, capabilities, or other resources for

preventing, protecting against, mitigating, responding to, and recovering from such threats or hazards.

23. Require applicants to attend and participate in any DHSES-sponsored conferences, training, workshops or meetings (excluding those identified by DHSES as voluntary) that may be conducted, by and at the request of DHSES, during the life of the grant contract.
24. In its sole discretion, reserves the sole discretion to increase or decrease the total funding available for this program at any time, resulting in more or fewer applications funded under this RFA.

DHSES may exercise the foregoing rights at any time without notice and without liability to any responding applicant or any other party for its expenses incurred in preparation of responses hereto or otherwise. All costs associated with responding to this RFA will be at the sole cost and expense of the applicant.

D. Term of the Contract

Any resulting contract or agreement for more than \$50,000 from this RFA will be effective only upon approval by both the NYS Office of the Attorney General and State Comptroller. Any resulting contract for \$50,000 and under from this RFA will be effective upon signature of both parties. For grants valued at \$10,000 or less, a Purchase Order invoking a "Letter of Agreement" between DHSES and the successful applicant will be issued.

E. Payment and Reporting Requirements of Grant Awardees

1. Standard Cost Reimbursement Contract

Each successful applicant must enter into a standard cost reimbursement contract with DHSES. Such contract will include this Request for Applications, the successful applicant's proposal, any attachments or exhibits and the standard clauses required by the NYS Attorney General for all State contracts (available upon request). The contract will be subject to approval by the Attorney General and State Comptroller. Although the contract format may vary, the contract will include such clauses, information, and rights and responsibilities as can be found on the DHSES website, including:

- APPENDIX A-1 - Agency Specific Clauses or a Letter of Agreement (Depending upon Funding Amount)
- APPENDIX B - Budget
- APPENDIX C - Payment and Reporting Schedule
- APPENDIX D - Workplan/Special Conditions

For purposes of this RFA, these terms and conditions are incorporated by reference and the applicant must agree to the inclusion of all of these terms and conditions in any resulting grant contracts as part of the application submission. Copies of the standard

terms and conditions included in DHSES grant contracts are available for review on the DHSES website at <https://www.dhSES.ny.gov/grant-reporting-forms>. Payments will be made subject to proper documentation and compliance with reimbursement procedures and all other contractual requirements.

2. Compliance with State and Federal Laws and Regulations, Including Procurement and Audit Requirements

2 CFR Part 200

Applicants (also referred to herein as “Subrecipients”) are responsible to become familiar with and comply with all state and federal laws and regulations applicable to these funds. Applicants are required to consult with the DHSES standard contract language (referenced above) for more information on specific requirements. Additionally, applicants must comply with all the requirements in 2 CFR Part 200 (Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards). Applicants are required to understand and adhere to all federal requirements. You may access 2 CFR Part 200 at: <https://www.ecfr.gov/cgi-bin/text-idx?SID=1c9afe07b881b32365c2f4ce1db64860&mc=true&node=pt2.1.200&rgn=div5>

Procurements

Additionally, applicants must follow and comply with all procurement procedures under General Municipal Law 5A and 2 CFR Part 200, Subpart D (see 2 CFR §§200.317-.327), and/or any other state or federal regulations applicable to these funds and will be subject to monitoring by DHSES to ensure compliance.

Single Audit

Applicants that expend \$750,000 or more from all Federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the requirements of U.S. Government Accountability Office’s (GAO) Government Auditing Standards, located at <http://www.gao.gov>, and the requirements of Subpart F of 2 CFR Part 200 located at: <http://www.ecfr.gov/cgi-bin/text-idx?node=sp2.1.200.f>.

Environmental and Historic Preservation (EHP) Compliance

As a federal agency, DHS/FEMA is required to consider the effects of its actions on the environment and/or historic properties to ensure that all activities and programs funded by DHS/FEMA, including grant-funded projects, comply with Federal EHP regulations, laws and Executive Orders, as applicable. Sub-recipients proposing projects that have the potential to impact the environment, including but not limited to the modification or renovation of existing buildings, structures and facilities, or new construction including replacement of facilities, must participate in the DHS/FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with supporting documentation so that DHS/FEMA may determine whether the proposed project has the potential to impact environmental resources and/or historic properties. In some cases, DHS/FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. The EHP review process must be completed before funds

are released to carry out the proposed project; otherwise DHS/FEMA may not be able to fund the project due to noncompliance with EHP laws, executive order, regulations, and policies.

Conflict of Interest

Pursuant to 2 CFR §200.112, in order to eliminate and reduce the impact of conflicts of interest in the sub-award process, applicants must follow their own policies and procedures regarding the elimination or reduction of conflicts of interest when making sub-awards. Applicants are also required to follow any applicable state, local, or Tribal statutes or regulations governing conflicts of interest in the making of sub-awards.

The applicant must disclose to the respective Contract Representative, in writing, any real or potential conflict of interest as defined by the Federal, state, local, or Tribal statutes or regulations or their own existing policies, which may arise during the administration of the Federal award within five days of learning of the conflict of interest. Similarly, applicants must disclose any real or potential conflict of interest to the pass-through entity (State) as required by the applicant's conflict of interest policies, or any applicable state, local, or Tribal statutes or regulations.

Conflicts of interest may arise during the process of DHS/FEMA making a federal award in situations where an employee, officer, or agent, any members of his or her immediate family, his or her partner has a close personal relationship, a business relationship, or a professional relationship, with an applicant, sub-applicant, recipient, subrecipient, or DHS/FEMA employees.

Additionally, applicants must disclose, in writing to the Federal Awarding Agency or to the pass-through entity (State) all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures can result in any of the remedies described in § 200.339. Remedies for noncompliance, including suspension or debarment. (See also 2 CFR part 180 and 31 U.S.C. 3321).

Contracting with Small and Minority Firms, Women's Business Enterprise and Labor Surplus Area Firms

Pursuant to New York State Executive Law Article 15-A, the New York State Division of Homeland Security and Emergency Services recognizes its obligation under the law to promote opportunities for maximum feasible participation of certified minority-and women-owned business enterprises and the employment of minority group members and women in the performance of New York State Division of Homeland Security and Emergency Services contracts. Minority and women-owned business enterprises can be readily identified on the directory of certified businesses at:
<https://ny.newnycontracts.com/>.

All qualified applicants shall be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

Consistent with 2 CFR §200.321, non-Federal contracting entities must take all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible.

Affirmative steps must include:

1. Placing qualified small and minority businesses and women's business enterprises on solicitation lists;
2. Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
3. Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
4. Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises;
5. Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce; and
6. Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs (1) through (5) of this section.

For purposes of this solicitation, applicants and subcontractors are hereby notified the State of New York has set an overall goal of **30% for MWBE participation** or more, **15% for Minority-Owned Business Enterprises ("MBE")** participation and **15% for Women-Owned Business Enterprises ("WBE")** participation, based on the current availability of qualified MBEs and WBEs for your project needs.

An applicant on any contract resulting from this procurement ("Contract") must incorporate the affirmative steps above into its grant management policies and procedures.

Further, pursuant to Article 15 of the Executive Law (the "Human Rights Law"), all other State and Federal statutory and constitutional non-discrimination provisions, the applicant and subrecipients will not discriminate against any employee or applicant for employment because of race, creed (religion), color, sex, national origin, sexual orientation, military status, age, disability, predisposing genetic characteristic, marital status or domestic violence victim status, and shall also follow the requirements of Human Rights Law with regard to non-discrimination on the basis of prior criminal conviction and prior arrest.

Sexual Harassment Prevention

By submitting this application, Applicants are certifying that Applicant has a policy addressing sexual harassment prevention and that applicant provides sexual harassment training to all its employees on an annual basis that meets the Department of Labor's model policy and training standards. If Applicant cannot make the certification, the Applicant may provide an explanatory statement with its bids detailing the reasons why the certification cannot be made.

Use of Service-Disabled Veteran-Owned Business Enterprises in Contract Performance

Article 17-B of the Executive Law enacted in 2014 acknowledges that Service-Disabled Veteran-Owned Businesses (SDVOBs) strongly contribute to the economics of the State and the nation. As defenders of our nation and in recognition of their economic activity in doing business in New York State, bidders/proposers for this contract for commodities, services or technology are strongly encouraged and expected to consider SDVOBs in the fulfillment of the requirements of the contract. Such partnering may be as subcontractors, suppliers, protégés or other supporting roles. SDVOBs can be readily identified on the directory of certified businesses at <https://online.ogs.ny.gov/SDVOB/search>

Bidders/proposers need to be aware that all authorized users of this contract will be strongly encouraged to the maximum extent practical and consistent with legal requirements of applicable federal laws and regulations including 2 CFR Part 200, State Finance Law, General Municipal Law and the Executive Law to use responsible and responsive SDVOBs in purchasing and utilizing commodities, services and technology that are of equal quality and functionality to those that may be obtained from non-SDVOBs. Furthermore, bidders/proposers are reminded that they must continue to utilize small, minority and women-owned businesses consistent with current State Law. Utilizing SDVOBs in State contracts will help create more private sector jobs, rebuild New York State's infrastructure, and maximize economic activity to the mutual benefit of the contractor and its SDVOB partners. SDVOBs will promote the contractor's optimal performance under the contract, thereby fully benefiting the public sector programs that are supported by associated public procurements.

Public procurements can drive and improve the State's economic engine through promotion of the use of SDVOBs by its contractors. The State, therefore, expects bidders and proposers to provide maximum assistance to SDVOBs in their contract performance. The potential participation by all kinds of SDVOBs will deliver great value to the State and its taxpayers.

For purposes of this solicitation, applicants and subrecipients are hereby notified the State of New York has set an overall goal of 6% for SDVOB participation or more.

Contractor will report on actual participation by each SDVOB during the term of the contract to the contracting agency/authority according to policies and procedures set by the contracting agency/authority.

Worker's Compensation and Disability Benefits Insurance Coverage

By submitting this application, Applicants are certifying that Applicant has workers' compensation and disability coverage. Provided, however, that if Applicant cannot make the certification, the Applicant may provide an exemption statement with its bids detailing the reasons why the certification cannot be made.

3. Iran Divestment Act

As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, a new provision has been added to the State Finance Law (SFL), § 165-a, effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of “persons” who are engaged in “investment activities in Iran” (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b), the initial list is expected to be issued no later than 120 days after the Act’s effective date, at which time it will be posted on the OGS website.

By submitting a proposal in response to this RFA, or by assuming the responsibility of a Contract awarded hereunder, the applicant (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, applicants are advised that once the list is posted on the OGS website, any applicant seeking to renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should DHSES receive information that a person is in violation of the above-referenced certification, DHSES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then DHSES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Contractor in default. DHSES reserves the right to reject any bid or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the prohibited entities list after contract award.

4. Vendor Responsibility

State Finance Law §163(9)(f) requires a State Agency to make a determination that an applicant is responsible prior to awarding that applicant a State contract which may be based on numerous factors, including, but not limited to the applicants: (1) financial and organizational capacity; (2) legal authority to do business in this State; (3) integrity of the owners, officers, principals, members, and contract managers; and (4) past performance of the applicant on prior government contracts. Thereafter, applicants shall at all times during the Contract term remain responsible. The applicant agrees, if requested by the Commissioner of DHSES, or his or her designee, to present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity. DHSES requires that vendors file the required Vendor Responsibility Questionnaire online via the New York State VendRep System. To enroll in and use the New York State VendRep System, see the VendRep System, see the VendRep System Instructions available at:

http://www.osc.state.ny.us/vendrep/info_vrsystem.htm or go directly to the VendRep system online at <https://onlineservices.osc.state.ny.us/Enrollment/login?0>. Vendors must provide their New York State Vendor Identification Number when enrolling. To request assignment of a Vendor ID or for VendRep System assistance, contact the Office of the State Comptroller's Help Desk at 866-370-4672 or 518-408-4672 or by email at ITServiceDesk@osc.state.ny.us. Vendors opting to complete and submit a paper questionnaire can obtain the appropriate questionnaire from the VendRep website http://www.osc.state.ny.us/vendrep/forms_vendor.htm or may contact the Office of the State Comptroller's Help Desk for a copy of the paper form. Applicants will also be required to complete and submit a Vendor Responsibility Questionnaire prior to contracting.

a) Suspension of Work for Non-Responsibility:

The Commissioner of DHSES or his or her designee, in his or her sole discretion, reserves the right to suspend any or all activities under the Contract, at any time, when he or she discovers information that calls into question the responsibility of the applicant. In the event of such suspension, the applicant will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the Commissioner of DHSES or his or her designee issues a written notice authorizing the resumption of performance under the Contract.

b) Termination for Non-Responsibility:

Upon written notice to the applicant, and a reasonable opportunity to be heard by appropriate DHSES officials or staff, the Contract may be terminated by the Commissioner of DHSES or his or her designee at the applicant's expense where the applicant is determined by the Commissioner of DHSES or his or her designee to be non-responsible. In such event, the Commissioner of DHSES or his or her designee may complete the contractual requirements in any manner he or she may deem advisable and pursue legal or equitable remedies for breach. Applicants shall at all times during the Contract term remain responsible. The applicant agrees, if requested by the Commissioner of DHSES, or his or her designee, to present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity.

F. Satisfactory Progress

Satisfactory progress toward implementation includes but is not limited to; executing contracts and submitting payment requests in a timely fashion, retaining consultants, completing plans, designs, reports, or other tasks identified in the work program within the time allocated for their completion. DHSES may recapture awarded funds if satisfactory progress is not being made on the implementation of a grant project.

G. General Specifications

By submitting the application, the applicant attests that:

1. Applicant has express authority to submit on behalf of the applicant's agency.
2. Submission of an application indicates the applicant's acceptance of all conditions and terms contained in this RFA, including Appendices A-1 and C, and all other terms and conditions of the award contract.
3. The application and any resulting grant, if awarded, must adhere to, and be in full compliance with any, resulting contract(s) and relevant federal and states policies and regulations or be subject to termination.
4. Any not-for-profit subrecipients are required to be prequalified, prior to contract execution, by the State of New York upon application submission through the New York State Grants Gateway (<https://grantsgateway.ny.gov>)
5. If your organization is not currently doing business with NYS, you will need to submit a Substitute W-9 form to obtain a NYS Vendor ID. The form is available on the Office of the State Comptroller website at: <http://www.osc.state.ny.us/state-agencies/forms>.
6. Contract Changes - Contracts with applicants/subrecipients may be executed, terminated, renewed, increased, reduced, extended, amended, or renegotiated at the discretion of the Commissioner of DHSES, in light of applicants/subrecipients performance, changes in project conditions, or otherwise.
7. Records – Applicants/subrecipients must keep books, ledgers, receipts, work records, consultant agreements and inventory records pertinent to the project; and in a manner consistent with DHSES contractual provisions and mandated guidelines.
8. Liability - Nothing in the contract between DHSES and the applicant shall impose liability on the State of New York or DHSES for injury incurred during the performance of approved activities or caused by use of equipment purchased with grant funds.
9. Reports - A provider agency shall submit to the DHSES reports in a format and time schedule specified in the grant contract, which shall include a description of the program efforts undertaken during the report period and the current status of the project.
10. Tax Law Section 5-a Certification – In accordance with section 5–a of the Tax Law, subrecipients will be required, prior to the approval of any contract awarded as a result of this RFA, to certify that it and its affiliates, subcontractors, and subcontractors' affiliates have registered with the New York State Tax Department for the purpose of collection and remittance of sales and use taxes. In order to trigger this certification requirement, a subrecipient or its affiliates, subcontractor, or subcontractors' affiliates must have made more than \$300,000 in sales of tangible personal property or taxable services to location within New York State and the contract must be valued in excess of \$15,000. Certification will take the form of a completed Tax Form ST-220 (1/05).
11. Standard Contract Provisions - Grant contracts executed as a result of this RFA process will be subject to the standard clauses for New York State Contracts as referenced herein and as located at:
https://online.ogs.ny.gov/purchase/biddocument/23128i_AppendixA.pdf

12. Compliance with Procurement Requirements - The applicant shall certify to DHSES that all applicable federal and contractual procurement procedures were followed and complied with for all procurements.

H. Special Conditions

New York State Emergency Management Certification and Training Program

1. Participation in, and successful completion of, the New York State Emergency Management Certification and Training Program (EMC Training Program) is a mandatory requirement under this Contract and a condition of funding. The EMC Training Program will be made available to, and required for, DHSES-specified county and city government officials in order to ensure a consistent emergency management preparedness and response strategy across the State. Attendee substitutions, except as expressly approved by DHSES, shall not be permitted or deemed to be in compliance with this requirement.
2. To fulfill the EMC Training Program requirement of the Contract and in order to be eligible for funding under this Contract, applicants must arrange for DHSES-specified applicant employees to receive and acknowledge receipt of EMC Training no later than 180 days after execution of this Contract. Copies of the training certificates for each required participant must be submitted to DHSES upon execution of the Contract, or, in the event that training is scheduled, but not yet complete, the applicant will be required to submit a signed statement indicating the scheduled future dates of attendance, and no later than thirty (30) days after the training is complete, forward such training certificates to DHSES. Continued compliance with the EMC Training Program also requires an annual refresher training of one day per 365 day-cycle from the date of initial training for previously trained individuals if such person remains employed by the applicant and fulfilling the same functions as he or she fulfilled during the initial training. Should a new employee be designated to serve in the DHSES-specified positions, then he or she must come into compliance with the EMC Training Program requirements not later than 180 days after taking office.
3. Applicants must commit to active participation in a DHSES Annual Capabilities Assessment as a condition of funding. Active participation includes making reasonable staff, records, information, and time resources available to DHSES to perform the Annual Capabilities Assessment and meet the objectives and goals of the program. Applicants must be aware that the process of conducting a DHSES Annual Risk Assessment is an ongoing process and requires a continued commitment on the part of the applicant to ensure that it is effective.
4. All applicants funded through this program agree to provide DHSES, upon request at any time during the life of the grant contract, such cooperation and information deemed necessary by DHSES to ascertain: (1) the nature and extent of any threats or

hazards that may pose a risk to the recipients or subrecipients; and (2) the status of any corresponding recipients or subrecipients plans, capabilities, or other resources for preventing, protecting against, mitigating, responding to, and recovering from such threats or hazards.

5. Additionally, pursuant to Article 26 of the NYS Executive law, DHSES is authorized to undertake periodic drills and simulations designed to assess and prepare responses to terrorist acts or threats and other natural and man-made disasters. Funded applicants agree to attend and participate in any DHSES-sponsored conferences, training, workshops or meetings (excluding those identified by DHSES as voluntary) that may be conducted, by and at the request of DHSES, during the life of the grant contract.
6. Failure to comply with any of the requirements, as listed above, may result in sanctions up to and including the immediate suspension and/or revocation of the grant award.

XI. Questions

Questions regarding the FY2020 Critical Infrastructure Grant Program should be directed to the following e-mail address Grant.Info@dhses.ny.gov. To the degree possible, each inquiry should cite the RFA section and paragraph to which it refers. Written questions will be accepted until **12:00 noon on April 28, 2022**.

Updates and frequently asked questions will be posted on the NYS Division of Homeland Security and Emergency Services (DHSES) website (*Please check the website frequently for updates*): <https://www.dhses.ny.gov/targeted-grants>.

All questions regarding the E-Grants System should be directed to DHSES via e-mail (Grant.Info@dhses.ny.gov) or telephone (866-837-9133). No technical assistance will be available after **5:00 p.m. on May 5, 2022**.

Exhibit A: Allowable Costs Matrix

Reminder: Allowable costs for the FY2020 Critical Infrastructure Grant Program are more restrictive than the more general State Homeland Security Program (SHSP) because of the specialized nature of this targeted grant program. Accordingly, please refer only to “Exhibit A” of this Request for Applications (RFA) for details on allowable costs.

Allowable Costs

Equipment Categories
CBRNE Operational Search & Rescue Equipment ³
Interoperable Communications Equipment must be P-25 compliant
Detection Equipment
Power
CBRNE Reference Materials
Terrorism Incident Prevention Equipment
Physical Security Enhancement Equipment
Inspection & Screening Systems
CBRNE Logistical Support Equipment
Intervention Equipment
Other Authorized Equipment
Training Costs
Training workshops & conferences
Travel
Supplies
Other Items
Exercise Related Costs
Design, Develop, Conduct & Evaluate an Exercise
Exercise planning workshop
Implementation of HSEEP
Travel
Supplies
Other Items

³ Certain equipment (not all) within this category require DHS/FEMA approval pursuant to Information Bulletin 426.

Unallowable Costs

Training Costs
Overtime & backfill for emergency preparedness & response personnel attending FEMA-sponsored & approved training classes & technical assistance programs
Overtime & backfill expenses for part-time & volunteer emergency response personnel participating in FEMA training
Part-time staff or contractors/consultants (not full-time)
Tuition for Higher Education
Training Props
Exercise Related Costs
Part-time staff or contractors/consultants (not full-time)
Overtime & backfill costs, including expenses for part-time & volunteer emergency response personnel participating in FEMA exercises
Equipment Categories
Personal Protective Equipment
Explosive Device Mitigation & Remediation Equipment
Decontamination Equipment
Medical
CBNRE Incident Response Vehicles
CBRNE Response Watercraft (Requires FEMA approval)
CBRNE Aviation Equipment
Management and Administrative (M&A) Costs
Hiring of full or part-time staff or contractors/consultants to assist with the management of the respective grant program, application requirements, compliance with reporting & data collection requirements
Development of operating plans for information collection & processing necessary to respond to FEMA data calls
Overtime and backfill costs
Travel
Meeting related expenses
Authorized office equipment
Recurring expenses such as those associated with cell phones & faxes during the period of performance of the grant program
Leasing or renting of space for newly hired personnel during the period of performance of the grant program
Construction Related Costs
Construction Costs

Exhibit B: Risk Instructions and Template Assessment and Capability Evaluation

Reminder: The Risk Assessment submitted for the participating site must contain the information outlined in this exhibit including a risk assessment and capability assessment (note: separate tabs for each) in the template. **Assessments that do not contain the outlined information contained herein will not be evaluated.**

The application will be scored based upon review of information developed on potential threats, vulnerabilities, and consequences. Please refer to the 2013 National Infrastructure Protection at: <https://www.dhs.gov/national-infrastructure-protection-plan> (pages 15-20) for additional information on risk assessments.

Risk Assessment Methodology

This assessment should be based on the risk management framework methodology and influenced by the nature and magnitude of the threat, the vulnerabilities that relate to that threat, and the consequences that could result from that threat. It should also include personal observations, analysis of documents, interviews, and/or photographic documentation. **For each area below, measurable statistics MUST be included:**

THREAT: For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the **likelihood of an attack being attempted** by an adversary or, for other hazards, an estimated likelihood that a hazard will manifest itself, that has or indicates the potential to harm life, information, operations, the environment, and or/property. Threat assessment judgments are based upon available intelligence (law enforcement and open source information). The facility should be viewed in terms of whether the nature of public contact required in or resulting from the conduct of business is adversarial, or whether there is a history of adversarial acts committed at the facility, against facility tenants, or against the tenant agencies elsewhere.

VULNERABILITY: For the purpose of calculating risk of an intentional hazard, the common measure of vulnerability is the **likelihood that an attempted attack is successful**. Focus is on physical features or operational attributes that renders an entity open to exploitation or is susceptible to a given hazard.

CONSEQUENCE: For the purpose of calculating risk, the consequence assessment is the effect of an event, incident, or occurrence; **reflects the level, duration, and nature of loss resulting from the incident**. Consequences are divided into four main categories: public health and safety (i.e. loss of life, illness); economic (direct and indirect); psychological; and governance/mission impacts.

FY2020 Critical Infrastructure Grant Program Risk Assessment

Government Owned Critical Infrastructure/ Mass Gathering/ Special Event Site Details

Type of Government Owned Site (Critical Infrastructure or Mass Gathering/Special Event):	Please Select Type of Site from Dropdown Menu
Name of Government Owned Site Selected:	
Physical Address of Selected Site:	
Application Point of Contact:	
Assessment Completed By:	
Completion Date of Assessment:	

Mission

<p>What is the general purpose of the Government Owned Critical Infrastructure or Mass Gathering/Special Event Site? Provide a brief description of the mission of the selected site.</p>	
<p>Based off the mission of the selected Government Owned Critical Infrastructure or Mass Gathering/Special Event Site, how does the site contribute or affect the primary functions of the community?</p>	
<p>Based off the mission of the selected Government Owned Critical Infrastructure or Mass Gathering/Special Event Site, how does the site contribute to or affect the primary functions of the County?</p>	
<p>Based off the mission of the selected Government Owned Critical Infrastructure or Mass Gathering/Special Event Site, how does the site contribute to or affect the primary functions of the State?</p>	

Threat

1) From the list provided below, select all threats deemed relevant to your facility based on the THREAT component of your risk assessment. Then in the "Narrative" section, please describe why you chose that threat and how it could affect your location and/or the larger community. See the Directions tab for possible factors to consider. Scoring for this section is worth a maximum of 10 points and is based on the completeness and quality of the narrative provided, not the quantity of threat(s) selected.

Threat (Manmade or Natural)	Narrative (Explain your selection here or in an attachment)
<input type="checkbox"/> Biological Agent Release	
<input type="checkbox"/> Active Shooter	
<input type="checkbox"/> Improvised Explosive Device (Man Portable or Vehicle Born IED)	
<input type="checkbox"/> Improvised Nuclear Device (IND)	
<input type="checkbox"/> Radiological Dispersal Device (RDD)	
<input type="checkbox"/> Food Contamination	
<input type="checkbox"/> HazMat Release	
<input type="checkbox"/> Radiological Release (Fixed-Site)	
<input type="checkbox"/> Vehicle-ramming Attack	
<input type="checkbox"/> Attack on Critical Infrastructure/Critical Infrastructure Failure	
<input type="checkbox"/> Extreme weather event (e.g. severe winter storm; flooding; high winds; etc.)	
<input type="checkbox"/> Population surges/crowd surges	
<input type="checkbox"/> Major Fire	
<input type="checkbox"/> Other (Explain in narrative portion)	

Vulnerability

2) Please report the findings of the VULNERABILITY component of your risk assessment. Scoring for this section is worth a maximum of 10 points and is based on the completeness and overall quality of the narrative provided (2a-2c).

<p><i>2a) Identify and describe specific vulnerabilities that exist given the selected threats (from the above Threats section).</i></p>	
<p><i>2b) Describe all protective measures in place and how they reduce the vulnerabilities identified in 2a.</i></p>	
<p><i>2c) Are there written plans such as Standard Operating Procedures (SOP), in place that address the vulnerabilities identified in 2a? If yes, please describe.</i></p>	

Consequence

3) Please report the findings of the CONSEQUENCE component of your risk assessment. Scoring for this section is worth a maximum of 10 points and is based on the completeness and overall quality of the narrative provided (3a-3d).

<p><i>3a) Given the selected threat(s) and vulnerabilities, what are the estimated number of fatalities, injuries, and illness, if applicable?</i></p>	
<p><i>3b) What is the estimated economic loss in dollars, if applicable?</i></p>	
<p><i>3c) Please describe psychological impacts, if applicable.</i></p>	
<p><i>3d) Is there a continuity of operations plan or could other similar assets perform the key functions of the selected site? If yes, please briefly describe.</i></p>	

FY2020 Critical Infrastructure Grant Program Capability Evaluation

Capability Evaluation

This section addresses the capabilities of the partnering agencies. Applicants should answer the questions below in a narrative format for all partnering agencies. Scoring for this section is worth a maximum of 20 points and is based on the completeness and overall quality of the narrative provided.

Questions: Identify all partnering agencies including name, address, and contact information. In the Narrative section, indicate 1) any combined planning or training with partnering agencies with respect to the selected site; 2) the estimated response times to the selected site by the partner agencies; 3) the equipment that partnering agencies already own that facilitate protection/response capabilities at the site; 4) the equipment that partnering agencies do NOT have that hinder prevention/response capabilities at the site; and 5) how the overall capability of partnering agencies will be enhanced by the requested goods/services.

Name, Address, and Contact information for 1st Partner Agency:

Name, Address, and Contact information for 2nd Partner

Narrative (Provide here or in an attachment)

Exhibit C: Examples of Government Owned Critical Infrastructure, Mass Gathering and Special Event Sites

In order to best support the purpose, goals, and objectives of the FY2020 CIGP, applicants should obtain a clear understanding of what government owned critical infrastructure and mass gathering/special event sites can be.

For the purposes of this grant application, government owned critical infrastructure and mass gathering/special event sites can be any asset owned or leased by a government entity where events can occur and draw crowds. Some of these assets can be open to the public for business, commercial transactions, or recreation. Others may not be open to the public and contain highly sensitive materials and equipment.

These assets may not only be physical structures. Applicants should consider the automation elements associated with the operation and protection of government owned critical infrastructure.

Examples include, but are not limited to:

- Seat of government or critical government facilities
- Water treatment facilities
- Government communications infrastructure systems
- Critical emergency services facilities
- Transportation (airports, roadways, maritime)
- Government public health facilities
- Government owned (or leased) mass gathering/special event sites
 - Including, but not limited to, parks, sporting venues, performance arts venues, festivals, government owned fairgrounds, and other reoccurring event sites.



Exhibit D: Best Practices for Preparing an Effective Grant Application

What to do when you have received the Request for Applications (RFA):

- It is important to start early in preparing your application, highlighting deadlines and/or tasks that must be completed as part of the application process.
- Review all plans, strategies, policies, and documents related to the grant you are applying for to ensure you can appropriately address the goals and objectives pertaining to the nature of the grant opportunity.

What to do when you are completing the application:

- Ensure that the proposed budget is realistic, reasonable, and articulate how your budget will address the objectives of the grant opportunity.
- Review and evaluate the scoring criteria. Pay close attention to the sections that are weighted the most first, as they have a greater impact on your overall score.
- If your grant application requires you to reference goals and/or objectives, make sure the goals and objectives you cite are measurable. Goals should reflect the long-term and global impact of a program or project. Meanwhile, objectives should be specific and measurable building blocks designed to meet your goals.
- Create an evaluation plan that demonstrates how you will assess your proposed projects for effectiveness and/or meeting the objectives of the grant opportunity, even if such a plan is not required.
- Address steps that will be taken to institutionalize, sustain, or enhance the capabilities or proposed project being developed after grant funding has been exhausted.

What to do prior to submitting your application:

- Make sure that you have completed all the required sections of the application. Applicants are strongly recommended to share their completed applications with a colleague to ensure that the application is clearly written and addresses all the objectives of the grant opportunity.



Homeland Security and Emergency Services

2020 Critical Infrastructure Grant Program (CIGP)

Frequently Asked Questions (FAQs)

*(New and/or Updated FAQ's are Highlighted in Red;
Please Check the DHSES Website Frequently for Updates)*

I. Due Date and Application Instructions

- 1. Question: What is the application due date for the FY2020 Critical Infrastructure Grant Program?**

Answer: Applications are due to NYS Division of Homeland Security and Emergency Services – Grants Program Administration (DHSES-GPA) by **5:00 p.m. on May 5, 2022**. Applications submitted past this date will be disqualified. No extensions will be given.

- 2. Question: How do I submit my application for the FY2020 Critical Infrastructure Grant Program?**

Answer: Applications must be submitted via DHSES Grants Program Administration's E-Grants system. If you are not registered to use the E-Grants system, your agency will need to register and be assigned a username and password. Please refer to: <https://www.dhSES.ny.gov/targeted-grants> or detailed instructions.

- 3. Question: What must be submitted to consider the application complete? Answer:**

Applications must be submitted via E-Grants and include the Risk Assessment and Capability Evaluation template as an attachment.

- 4. Question: Would your agency be able to provide me with a sample of a previous grant application? (i.e., Critical Infrastructure Sites, Mass Gathering/Special Events Sites)?**

Answer: We cannot provide specific language or sample applications during an open competitive process. Our advice is to read the RFA carefully and submit as complete an application as possible for the best chance of success.

II. Eligibility and Objectives

1. Question: Is a community college an eligible applicant?

Answer: No, only units of local government are eligible to apply.

2. Question: Can a unit of local government submit more than one application?

Answer: No, a unit of local government may submit only one application under the FY2020 CIGP. Multiple applications are unallowable, and only one application for either a government owned critical infrastructure or a government owned mass gathering/special event site will be accepted.

3. Question: Can school districts submit an application directly?

Answer: No, a unit of local government is the only eligible applicant under this Request for Applications (RFA). School districts may coordinate with a unit of local government as a critical infrastructure site.

4. Question: Are projects that were funded under a prior year's CIGP grant eligible under the FY2020 Critical Infrastructure Grant Program for funding for continued build-out or sustainment?

Answer: Yes, as long as it meets the eligibility requirements, DHSES encourages the completion and/or sustainment of projects previously funded under prior grant year's funding.

5. Question: Are cyber security projects eligible for funding under the FY2020 Critical Infrastructure Grant Program?

Answer: No, cyber security projects are not an eligible project funding type.

6. Question: Who is eligible to apply for the FY2020 Critical Infrastructure Grant Program?

Answer: Only units of local government located in New York City or one of the following targeted counties: Albany, Broome, Dutchess, Erie, Herkimer, Livingston, Madison, Monroe, Nassau, Niagara, Oneida, Onondaga, Ontario, Orange, Orleans, Oswego, Putnam, Rensselaer, Rockland, Saratoga, Schenectady, Schoharie, Suffolk, Tioga, Wayne, Westchester, and Yates.

7. Question: What is a unit of local government?

Answer: For the FY2020 Critical Infrastructure Grant Program, a unit of local government includes counties, cities, towns and/or villages.

8. Question: Can local first responders submit an application directly?

Answer: No, a unit of local government is the only eligible applicant under this Request for Applications (RFA). First responders must coordinate with the unit of local government on an application.

9. Question: What is a government owned critical infrastructure site?

Answer: Examples of government owned critical infrastructure sites include, but are not limited to, government office buildings (city/town halls), emergency services (emergency operations centers, 911 centers, police or fire stations), water systems (water treatment facilities, water distribution, wastewater treatments) or government owned stadiums.

10. Question: What is a government owned mass gathering/special event site?

Answer: A government owned mass gathering/special event site is government property, where events such as, but not limited to, major community festivals, races, concerts, or games are held. These events must be reoccurring (but not necessarily the same event) and located or held on government owned or leased property that has definable geographic boundaries. The event or location must pose special security concerns, such as population surges and other factors that require additional law enforcement or emergency resources.

11. Question: Are Fire Districts eligible to submit for the FY2020 Critical Infrastructure Grant Program?

Answer: No. Only a unit of local government, defined as county, city, town, or village, can submit an application under the FY2020 Critical Infrastructure Grant Program.

Fire Districts may participate in the FY2020 Critical Infrastructure Grant Program as a partnering agency, as the application must be coordinated with at least two (2) agencies with prevention and/or protection responsibilities at the selected critical infrastructure sites. The agencies must be law enforcement, fire departments, emergency management, or public works agencies.

12. Question: Are standalone EMS agencies eligible to apply under this grant program?

Answer: No. Only units of local government are eligible to apply for the FY2020 CIGP. These include counties, cities, towns or villages. In addition, the application must be coordinated with at least two agencies with prevention and/or protection responsibilities at the selected site or special event site. These agencies must be law enforcement, fire department, emergency management or public works agencies. EMS agencies do not fit this criterion.

13. Question: Is there eligibility for reimbursement through this grant for items that are purchased in advance of the grant award?

Answer: Expenses that occur prior to the start date of the grant period of performance cannot be reimbursed.

III. Partnering Agencies

1. Question: Whom does the application need to be coordinated with?

Answer: The application must be coordinated with at least two (2) agencies with prevention and/or protection responsibilities at the selected critical infrastructure sites. The agencies must be law enforcement, fire department, emergency management, or public works agencies.

IV. Allowable Costs

1. **Question: Are Mass Casualty Incident (MCI) trailers an allowable expense under the FY2020 Critical Infrastructure Grant Program?**

Answer: No, vehicles and trailers are not allowable costs under the FY2020 Critical Infrastructure Grant Program.

For a comprehensive listing of allowable and unallowable costs, see Exhibit A.

2. **Question: Re: Exhibit A – Allowable Cost Matrix. Is a portable surveillance system an allowable cost?**

Answer: Equipment must (a) be contained on the Authorized Equipment List (AEL); (b) marked for applicability to the State Homeland Security Program (SHSP); and (c) fall under one of the more restrictive allowable categories identified within this Request for Applications (see RFA Exhibit A) in order to be considered eligible under the Critical Infrastructure Grant Program. The AEL is presented in a number of sections and each item in the AEL is marked for applicability to appropriate grant programs, to get started, cross reference RFA Exhibit A with the appropriate section of the AEL (i.e., 03 – CBRNE Operational Search and Rescue Equipment, 13 – Terrorism Incident Prevention Equipment or 14 – Physical Security Enhancement Equipment). The AEL can be found at: <https://www.fema.gov/authorized-equipment-list>

3. **Question: Can an applicant submit for equipment that is not listed in the Authorized Equipment List? Would a submission that addresses target hardening from natural disasters and accidental hazards (fire) fit within the program?**

Answer: No. All equipment requested under the FY2020 Critical Infrastructure Grant Program must be listed on the Authorized Equipment List and only those categories in Exhibit A in the Request for Applications are allowable (see question #2 above). One of the main objectives of the grant program is to complete a capability assessment to identify equipment, training and/or exercise needs to prevent and protect against attacks at the critical infrastructure site. A project solely addressing natural hazards and accidental fires would not be allowable.

4. **Question: Is salary, overtime or backfill overtime an allowable cost to design, develop, conduct and evaluate training exercise(s)?**

Answer: As per the “Exhibit A: Allowable and Unallowable Cost Matrix”, organizational, management and administrative, construction, and personnel costs are not allowable under the FY2020 Critical Infrastructure Grant Program to include overtime and backfill costs associated with training and exercises.

5. Question: Are there any restrictions on training equipment & supplies?

Answer: Equipment under the FY2020 CIGP must (a) be contained on the Authorized Equipment List (AEL); (b) marked for applicability to the State Homeland Security Program (SHSP); and (c) fall under one of the more restrictive allowable categories identified within this Request for Applications (see RFA Exhibit A) in order to be considered eligible under the FY2020 Critical Infrastructure Grant Program. The Authorized Equipment List (AEL) can be found at: <https://www.fema.gov/authorized-equipment-list>. The AEL is organized in a number of sub-categories and each item on the AEL that is allowable is outlined in the RFA Exhibit A. You can cross reference RFA Exhibit A with the appropriate section of the AEL (i.e., 03 – CBRNE Operational Search and Rescue Equipment, 13 – Terrorism Incident Prevention Equipment or 14 – Physical Security Enhancement Equipment) to determine allowability.

v. Other

1. Question: Is the word “attacks” in the RFA specifically for malicious intent or does it also apply to natural disaster scenarios?

Answer: Attacks, under this program refer to an intentional attack or an attempt by an adversary.

2. Question: I cannot find the capability evaluation; can I use the one from previous fiscal years?

Answer: No, the Risk Assessment and Capability Evaluation document has been updated for the FY2020 Critical Infrastructure Grant Program. The Capability Evaluation questions may be found in Exhibit B of the RFA.

3. Question: I have additional questions that are not addressed in this Frequently Asked Questions (FAQs) document, who can I contact?

Answer: Questions should be directed in writing to the following email address: Grant.Info@dhses.ny.gov. This FAQs bulletin will be updated regularly based on questions that are submitted. Please check the DHSSES website (<http://www.dhses.ny.gov>) frequently for updates.



DANIEL P. MCCOY
COUNTY EXECUTIVE

DANIEL LYNCH
DEPUTY COUNTY EXECUTIVE

COUNTY OF ALBANY
DEPARTMENT OF MANAGEMENT AND BUDGET
DIVISION OF INFORMATION SERVICES
112 STATE STREET, ROOM 500
ALBANY, NEW YORK 12207
PHONE: (518) 447-7200 FAX: (518) 447-3000
www.albanycounty.com

M. DAVID REILLY
COMMISSIONER

PERRY J. BLANCHARD
CHIEF INFORMATION OFFICER

DATE: April 29, 2022

TO: Hon. Andrew Joyce, Chairman
Albany County County Legislature
112 State Street, Room 710
Albany, New York 12207

RE: RLA - Authorization to Apply for NYS Division of Homeland Security and
Emergency Services (DHSES) FY20 Cyber Security Grant Program

Dear Chairman Joyce,

The Division of Information Services is requesting permission to apply for the NYS Division of Homeland Security and Emergency Services' FY2020 Cyber Security Grant Program. Information Services is requesting to apply for grant funding to contract with a qualified vendor to provide managed cyber security services. The subscription will allow Albany County to develop a comprehensive cyber risk strategy, to include an incident response plan and a vulnerability assessment. NYS DHSES is accepting applications for projects up to \$50,000, and Albany County will be applying for the full \$50,000.00. There is no cost/County match associated with this grant application.

Should you have any questions, please don't hesitate to contact me. Thank you for your consideration of this matter.

Sincerely,

Perry J Blanchard
Chief Information Officer
Division of Information Services

cc: Hon. Dennis A. Feeney, Majority Leader
Hon. Frank A. Mauriello, Minority Leader
Rebekah Kennedy, Majority Counsel
Arnis Zilgme, Minority Counsel



County of Albany

Harold L. Joyce
Albany County Office
Building
112 State Street - Albany,
NY 12207

Legislation Text

File #: TMP-3286, **Version:** 1

REQUEST FOR LEGISLATIVE ACTION

Description (e.g., Contract Authorization for Information Services):

Authorization for the Division of Information Services to Apply for the NYS Division of Homeland Security and Emergency Services' (DHSES) FY2020 Cyber Security Grant Program

Date: 4/29/2022
 Submitted By: Perry Blanchard
 Department: Division of Information Services
 Title: Chief Information Officer
 Phone: 518-447-4962
 Department Rep.
 Attending Meeting: Perry Blanchard / Dave Reilly

Purpose of Request:

- Adopting of Local Law
- Amendment of Prior Legislation
- Approval/Adoption of Plan/Procedure
- Bond Approval
- Budget Amendment
- Contract Authorization
- Countywide Services
- Environmental Impact/SEQR
- Home Rule Request
- Property Conveyance
- Other: (state if not listed) Click or tap here to enter text.

CONCERNING BUDGET AMENDMENTS

Increase/decrease category (choose all that apply):

- Contractual
- Equipment
- Fringe
- Personnel

- Personnel Non-Individual
- Revenue

Increase Account/Line No.: Click or tap here to enter text.
Source of Funds: Click or tap here to enter text.
Title Change: Click or tap here to enter text.

CONCERNING CONTRACT AUTHORIZATIONS

Type of Contract:

- Change Order/Contract Amendment
- Purchase (Equipment/Supplies)
- Lease (Equipment/Supplies)
- Requirements
- Professional Services
- Education/Training
- Grant

New

Submission Date Deadline 5/5/2022

- Settlement of a Claim
- Release of Liability
- Other: (state if not listed) Click or tap here to enter text.

Contract Terms/Conditions:

Party (Name/address):

NYS Division of Homeland Security and Emergency Services
1220 Washington Avenue
State Office Campus, Building 7A
Albany, NY 12226

Additional Parties (Names/addresses):

Click or tap here to enter text.

Amount/Raise Schedule/Fee: \$50,000
Scope of Services: Grant to provide funding for managed Cyber Security Services and
Cyber Risk Plan Development

Bond Res. No.: Click or tap here to enter text.
Date of Adoption: Click or tap here to enter text.

CONCERNING ALL REQUESTS

Mandated Program/Service: Yes No
If Mandated Cite Authority: Click or tap here to enter text.

Is there a Fiscal Impact: Yes No
Anticipated in Current Budget: Yes No

County Budget Accounts:

Revenue Account and Line: Click or tap here to enter text.
Revenue Amount: Click or tap here to enter text.

Appropriation Account and Line: Click or tap here to enter text.
Appropriation Amount: Click or tap here to enter text.

Source of Funding - (Percentages)

Federal: 0
State: 100%
County: 0
Local: 0

Term

Term: (Start and end date) Start TBD - August 31, 2023
Length of Contract: TBD

Impact on Pending Litigation

If yes, explain: Yes No
Click or tap here to enter text.

Previous requests for Identical or Similar Action:

Resolution/Law Number: Reso 2021 - 41
Date of Adoption: 2/8/2021

Justification: (state briefly why legislative action is requested)

The Albany County Division of Information Services (DIS) is seeking legislative authorization to apply for the NYS Division of Homeland Security and Emergency Services' FY2020 Cyber Security Grant Program. The DIS is applying for grant funding to cover the costs of some cyber managed services and to develop a cyber-risk strategy (including a cyber-program, incident response plan and a vulnerability assessment). The grant application is due May 5, 2022. DIS is applying for \$50,000 (out of an allowable \$50,000) in funding to cover the costs associated with planning. There is no County match associated with this grant.



Homeland Security and Emergency Services

FY2020 Cyber Security Grant Program: Request for Applications (RFA)

Application Deadline: May 5, 2022 by 5:00 pm

In order to ensure adequate time to respond, substantive written questions regarding this Request for Applications will be accepted until 12:00 noon on April 28, 2022.

Technical Assistance for E-Grants will not be available after 5:00 pm on May 5, 2022.

Table of Contents

I. Introduction	3
II. Eligibility	4
III. FY2020 Cyber Security Grant Program Objectives	4
A. Provide Resources and Equipment.....	4
B. Risk and Vulnerability Assessment.....	5
C. Promote Training.....	7
D. Develop Plans and Policies.....	7
E. Utilization of Available Resources.....	8
IV. Authorized Program Expenditures	9
A. Permissible Costs	9
B. Costs Not Permissible	10
V. Application Format and Content	10
A. Format.....	10
B. Required Application Content.....	10
VI. Application Evaluation Criteria	12
A. Tier 1 Criteria.....	13
B. Tier 2 Criteria	13
VII. Checklist of Required Documents	14
VIII. Timeline	15
IX. Approval and Notification of Award	15
X. Administration of Grant Contracts	15
A. Issuing Agency.....	16
B. Filing an Application.....	16
C. Reservation of Rights	16
D. Term of the Contract	17
E. Payment and Reporting Requirements of Grant Awardees	18
F. Satisfactory Progress	23
G. General Specifications	24
H. Special Conditions.....	25
XI. Questions	26
Exhibit A: Allowable Costs Matrix	27
Exhibit B: MS-ISAC Membership	29
Exhibit C: Cyber Security Resources for Local Governments	30
Exhibit D: Best Practices for Preparing an Effective Grant Application	34

I. Introduction

The purpose of this Request for Applications (RFA) is to solicit applications for up to \$50,000 in federal FY2020 State Homeland Security Program (SHSP) funding made available by DHSES for eligible applicants to enhance and sustain their cyber security posture as well as ensure that their information systems are secure and protected from cyber incidents. There is a total of up to \$2,000,000 in funding that is made available under this grant program and funds will be awarded competitively based on the submission of completed and eligible applications.

NYS DHSES recognizes the impacts that cyber incidents pose to our government information systems and critical infrastructure, placing our security, economy, and public health and safety at risk. As New York State's dependencies on computer networks and information systems grow, so do threats of cyber incidents. Government entities at every level and of every size use cyber-based systems to some degree. All sectors of critical infrastructure, including transportation, energy, communications, emergency services, and water systems rely on Information Technology (IT)-based controls, thus placing them at risk of cyberattacks. Minimizing risk is key to maintaining the security of these systems. With the cyber security threat landscape expanding in size and complexity, all levels of government must ensure their cyber security measures are kept current and updated regularly, relative to emerging threats.

Through the state-wide County Emergency Preparedness Assessments (CEPA) process conducted every three years by NYS DHSES, the threat of a cyber incident recently scored as the highest risk of all human-made/adversarial threats assessed. Despite its high-risk level, cyber security capabilities across New York State counties scored low, pointing to a considerable need for cyber security enhancement. The CEPA data showed cyber security weaknesses across multiple categories, including policy/procedures, training, software and equipment.

In response, NYS DHSES has devoted funding through this grant opportunity to aid local jurisdictions in enhancing their ability to identify, protect, detect, respond to and recover from cyber incidents.

The primary objectives of this grant opportunity are as follows:

1. To provide New York State local jurisdictions with the resources and equipment necessary to prevent disruption of the confidentiality, integrity, and availability of their information systems.
2. To assess cyber security risks, identify vulnerabilities and determine capability gaps with the focus of allocating resources to address the most critical needs.
3. To ensure that local jurisdictions are equipped with the knowledge and resources necessary for providing cyber security awareness training to their staff in support of good cyber hygiene at the user level.
4. To develop actionable cyber security plans that focus on response and immediate remediation to a cyber incident.

5. To encourage the participation in established cyber security support networks and utilization of the vast amount of resources available to local governments.

This grant opportunity will ensure that critical homeland security funding addresses prioritized capability development goals and objectives, as recognized by State and local stakeholders in the 2017-2020 New York State Homeland Security Strategy, specifically, Goal 4: *Enhance Cyber Security Capabilities*.

II. Eligibility

All New York State counties as well as local units of government to include cities, towns, and/or villages are eligible to apply for this grant opportunity. Only one application per jurisdiction will be accepted for funding consideration. Please coordinate with your municipality regarding submitting an application.

- **Additional Eligibility Requirement:** Eligible applicants are further required to be an existing member or register as a new member of the Multi-State Information Sharing and Analysis Center (MS-ISAC). DHSES staff will collaborate with MS-ISAC administrators to verify eligibility of all applicants. An overview and registration information of the MS-ISAC can be found in ***Exhibit B: MS-ISAC Membership*** of this RFA.
- **Nationwide Cyber Security Review (NCSR) Requirement:** All applicants that receive funding through the FY2020 Cyber Security Grant Program will be required to participate in the Nationwide Cyber Security Review (NCSR) as a condition of receiving federal homeland security funding. Details on accessing and registering for the Nationwide Cyber Security Review (NCSR) can be found at: <https://www.cisecurity.org/ms-isac/services/ncsr/>. It is advised that you coordinate closely with your Information Security Officer (ISO) to determine if your jurisdiction has already completed this requirement – please note that you are only required to submit once for your specific jurisdiction.

III. FY2020 Cyber Security Grant Program Objectives

DHSES has identified the following objectives for the FY2020 Cyber Security Grant Program:

- A. To provide New York State local jurisdictions with the resources and equipment necessary to prevent disruption of the confidentiality, integrity, and availability of their information systems.**

The confidentiality, integrity and availability of information, or the CIA triad of cyber security, represent the fundamental aspects of data that are sought to be protected within an organization's network. "Confidentiality" refers to maintaining legally protected or private data, accessible only to parties intended by the organization. "Integrity" refers to maintaining accuracy and completeness of data. "Availability" refers to the data being stored, processed, and

communicated properly to ensure its accessibility within the organization. These concepts each represent how an organization's systems could be disrupted if subjected to a cyber incident. Information Technology systems, as they relate to cyber security, consist of physical equipment, such as endpoint devices, servers and other hardware components that provide protection, as well as programmatic resources, such as firewalls and anti-virus software. These systems must be kept up to date and operating properly to ensure critical information is protected and secure.

Cyberattacks are successful when vulnerabilities in these systems are exploited. The FY2020 Cyber Security Targeted Grant Program supports local jurisdictions in protecting their systems through the use of funding and ensuring these systems continue to operate effectively to minimize cyber security risk, thus limiting harmful consequences to the organization.

B. To assess cyber security risks, identify vulnerabilities and determine capability gaps with the focus of allocating resources to address the most critical needs.

Every jurisdiction carries at least some degree of risk. Vulnerabilities within organizations can present in a variety of areas. Two perspectives from which to assess cyber security are that of governance/policy, to include awareness training, in addition to that of physical systems, including equipment and software. Conducting a comprehensive risk assessment will help jurisdictions determine which specific areas within their organization may present a risk for exploitation by an adversary. The risk assessment process should be used to identify specific vulnerabilities and to assist with prioritizing the most critical needs.

Center for Internet Security (CIS) Controls – Introduction

The DHSES Cyber Security Grant Program was created to help entities develop their cyber security programs. The grant encourages entities to evaluate their cyber posture using the Center for Internet Security (CIS) Controls and apply for funding to remediate the gaps they identify.

The CIS Controls are a list of high-priority, highly effective defensive actions that provide a “must-do, do-first” starting point for every entity seeking to improve their cyber defense. By adopting these controls, organizations can prevent the majority of cyberattacks.

Details regarding the CIS Controls can be found at <https://learn.cisecurity.org/cis-controls-download>

CIS Controls – Focus on Implementation Group 1

DHSES has provided an abbreviated version of its controls assessment tool, which is based on AuditScripts' “Critical Security Controls Initial Assessment Tool”, as a part of the Cyber Security Grant Program. This version of the tool focuses on Implementation Group 1 safeguards, which are the aspects of the CIS Controls that are essential for a successful cybersecurity program and are achievable with limited cyber security expertise. Use of this tool will aid New York's State and local governments in assessing their current posture and identifying fundamental security gaps.

There are 57 safeguards in Implementation Group 1 of the CIS Controls, most of which can be easily implemented with no-cost or low-cost solutions. Some safeguards may require expenditures or assistance to implement. In these cases, the entity may wish to consider a consulting engagement to implement the capability or use of an outsourced or managed service. Please note that proper procurement guidelines must be followed in the event that consultants are engaged for these services.

Encouraged and Favored Projects

Applications seeking funding for projects related to Implementation Group 1 safeguards are encouraged and favored where such gaps are identified in the assessment questionnaire. Other high priority projects that fall outside of this scope will also be considered but should be accompanied by justification and/or supporting documentation (such as a risk assessment report).

Based on past NYS breach and incident data, the following are favored and recommended projects for entities that do not have related or sufficient protections in place.

Multi-Factor Authentication (MFA) – Many incidents and compromises occur as a result of phishing, credential theft, and single factor authentication solutions (including email, remote access). These risks can be mitigated by implementing multi-factor authentication.

Email Filtering - One of the most common vectors for malware and social engineering is phishing. While not an Implementation Group 1 safeguard, we recognize that, when coupled with effective end user awareness training and other organizational controls, email filtering can provide effective protection for an entity and its mail system.

End User Training – Security training for staff can help prevent many cyber related incidents. With regular trainings, users can gain the knowledge and initiative to avoid compromise and report suspicious activity, thus thwarting attempted cyberattacks. There are many free training solutions that exist as outlined in this RFA. If you are submitting for training, please explain why a free solution is not sufficient and the benefits of applying for/purchasing a paid solution.

Backup Solutions – As seen in many headlines, ransomware continues to be a leading threat. Ensuring proper backup solutions are in place and tested can help with recovery in the case of a ransomware or other infection. It is important to maintain offline, non-network addressable backups. Many entities have experienced infections that encrypted their entire network and backups.

To aid in the application process, this guidance and the Application Worksheet were developed in collaboration with DHSES's Cyber Incident Response Team (CIRT) and Cyber Support Element (CSE), both of which provide cyber security support for local governments, non-executive agencies and public authorities through outreach, information sharing and cyber incident response.

C. To ensure that local jurisdictions are equipped with the knowledge and resources necessary for providing cyber security awareness training to their staff in support of good cyber hygiene at the user level.

In addition to physical systems, an equally, if not more critical component to cyber security is ensuring that all users of information technology systems are following safe and secure practices. This can be accomplished through regularly administered trainings of cyber security best practices and establishing jurisdiction-wide policies to enforce these practices. For example, a common method of cyberattack known as “phishing” occurs when a malicious party sends a fraudulent email, often purporting to be from a trusted source. The email will contain a link or attachment which installs malicious software (malware). Lacking proper knowledge and awareness, a user could be deceived and open the link, thus creating an entry point for a cyberattack. In this all-too-common scenario, a single user’s error will place the entire organization’s network at risk. With such cyberattacks targeting users’ behavior, the importance of cyber security awareness training is paramount.

With this consideration in mind, a well-educated user is also an invaluable resource for cyber threat detection, given the prevalence of email-based cyber threats. With regular trainings, users can gain the knowledge and initiative to report suspicious activity appropriately, thus thwarting attempted cyberattacks. Additionally, with the cyber security threat landscape expanding in sophistication and complexity, regular and recurrent training opportunities can incorporate updated information of specific cyber threats for users’ awareness.

Applicants of the FY2020 Cyber Security Grant Program are strongly encouraged to develop new or enhance existing cyber security training programs within their agency, as well as other investments focused on the creation of robust cyber security policies and practices. Please note that a multitude of training resources are available for free, which applicants are highly encouraged to seek prior to requesting grant funds for such resources. Please refer to ***Exhibit C: Cyber Security Resources for Local Governments*** for more information on available free and low-cost trainings.

D. To develop actionable cyber security plans that focus on response and immediate remediation to a cyber incident.

In addition to utilizing grant funds to enhance protection and prevention of cyber threats, the FY2020 Cyber Security Grant Program further supports a focus towards response to a cyberattack, should one occur. DHSES recognizes that even jurisdictions with a robust cyber security posture still carry some degree of risk of a cyber incident. Having an effective response plan in place following such an event is critical in minimizing disruption of an organization’s systems. Funding through this program supports local jurisdictions’ preparedness efforts to include effective planning and executing regular cyber security exercises. With planning and exercises occurring at regular intervals, an organization can effectively measure their cyber security policies and defenses. This will provide an opportunity for the organization to address any vulnerabilities identified during the exercise. Consequently, the organization will be prepared for real world cyber threats and any potential disruption would be minimized.

E. To encourage the participation in established cyber security support networks and utilization of the vast amount of resources available to local governments.

Through the FY2020 Cyber Security Grant Program, applicants are encouraged to take advantage of the many resources, available from organizations at the State and federal level, as well as the private sector, including information sharing and support networks, assessment tools, best practice recommendations and incident response assistance. Many of these resources are available free of charge and provide government organizations with the ability to assess their current capabilities, identify where vulnerabilities exist, prioritize where to focus resources, and understand how to mitigate and plan for potential cyber incidents in the future. Several of these resources are outlined in *Exhibit C: Cyber Security Resources for Local Governments* of this RFA.

DHSES is committed to ensuring that local government organizations are supported in their preparedness efforts as they relate to cyber security, through not only this funding opportunity, but also working collaboratively with other State and federal partners in an effort to coordinate information-sharing, provide outreach opportunities and support New York State's local governments with their cyber security needs.

- **Multi-State Information Sharing and Analysis Center (MS-ISAC):** Applicants of the FY2020 Cyber Security Grant Program will be required to be an existing member or register as a new member of the MS-ISAC. The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments. They are a valued partner of New York State, and work closely with the New York State Intelligence Center (NYSIC) and other NYS agencies to support New York State's local governments. Direct membership in the MS-ISAC and access to all its resources and services are available at no cost to New York's local governments. More information is available at <https://www.cisecurity.org/ms-isac/>.
- **Domain Name System (DNS) Filtering Inquiry:** Eligible applicants are further required to provide information about any DNS filtering solution they have in place to block the resolution of malicious domain names by clients in their environments. The information is to be provided in the Cyber Security Grant Program Application Worksheet. While we are simply gathering information during the current grant application cycle, use of a comprehensive service of this type may become a requirement for application to the Cyber Security Grant Program in a future cycle. DNS filtering is available at no cost to MS-ISAC members via its Malicious Domain Blocking and Reporting (MDBR) service: <https://www.cisecurity.org/ms-isac/services/mdbr/>
- **New York State Board of Elections (SBOE) Managed Security Service and Intrusion Detection Service Programs:** SBOE has recently made these services available to counties for the benefit of the County Boards of Elections. When applying for grants, applicants should consider whether the services identified in the application would or could be covered by SBOE's Managed Security Services and Intrusion Detection

Services programs that are being offered at no cost to the Counties. For additional information on these programs please email: info@elections.ny.gov.

IV. Authorized Program Expenditures

A. Permissible Costs

Grant funding under the FY2020 Cyber Security Grant Program may be used for certain planning, equipment, training and exercise costs allowable under the State Homeland Security Program (SHSP). ***Applicants should refer to Exhibit A, "Allowable Costs Matrix" for detailed information on allowable costs.***

Examples of projects that are in line with the grant program include, but are not limited to, the following:

1. Planning:

- Costs associated with the development of plans to include the hiring of consultants¹ to identify potential vulnerabilities and develop risk mitigation plans

2. Equipment:

- Software packages including firewalls, anti-virus applications and malware protection;
- Network equipment including servers;
- Encryption software;
- Intrusion detection systems;
- Hardware components that will provide protection against cyber threats;
- Physical security measures including cameras and access control for protection of IT hardware and equipment

3. Training:

- Training initiatives, including overtime and backfill costs;
- Costs associated with the development and delivery of cyber awareness training to staff at the user level
- Training costs specific to IT/Cyber-focused personnel

4. Exercises:

- Costs associated with the design, development, execution, and evaluation of exercises (regionally or locally) to determine the viability of new or pre-existing capabilities.

Note: The sample list above is not fully inclusive. Please note that equipment purchases must be allowable per the Authorized Equipment List located at: (<https://www.fema.gov/grants/guidance-tools/authorized-equipment-list>).

¹ Under the Cyber Security Grant Program, as with all SHSP funding, there is a 50% cap on personnel costs. Personnel Costs include OT/Backfill for Training and Exercises and most consultant costs (unless the consultant is developing defined deliverables or installing equipment.)

B. Costs Not Permissible

Organizational, Management & Administration (M&A) costs, construction costs, and the hiring of full or part-time staff are not allowable under this grant program. Applicants should refer to Exhibit A of this RFA to obtain clear guidance on allowable costs.

V. Application Format and Content

A. Format: Grant applications **MUST** be submitted via the automated E-Grants System operated by DHSES by 5:00 pm on **May 5, 2022**. The system allows an agency to complete an application electronically and submit it online using a secure portal. If upon reading this RFA you are interested in completing a grant application, and you have not previously been registered to use the DHSES E-Grants system, your agency will need to register and be assigned a username and password. The Registration Request Form and a detailed tutorial on how to use the E-Grants system is available at: <https://www.dhSES.ny.gov/e-grants>.

B. Required Application Content: The following questions must be addressed in your FY2020 Cyber Security Grant Program application. You must answer these grant-specific questions in the **required** Application Worksheet for your application to be considered.

1. Applicant Details: Applicants must provide the identification of their organization to include the following:

- Organization name and address;
- Point of Contact name and contact info (POC should be IT/Cyber-focused Personnel)
- Number of personnel within the organization for which the grant funding will apply (all front-line users of IT/all users of the agency’s e-mail system);
- Organizational structure of Information Technology/Cyber Security dedicated staff within the organization;
- Summary of the organization’s current IT environment to include basic description of network equipment and approximate number of endpoint devices (computers, smartphones, tablets, etc.);
- Cyber Incident History within the Organization, if applicable (things to consider include the type of cyber incident that occurred, what data, if any, was compromised, what steps the organization took in response to the incident and how well the organization recovered from the incident);
- Perceived Cyber Threats to the Organization, based on current security posture and observed threat environment;
- Cyber Threat Intelligence Source(s) for the Organization, including MS-ISAC membership status; and
Mission of the Organization and the role its IT systems meet to fulfill the functions of government

2. DNS Filtering Service Information Request: Applicants shall identify any DNS filtering solution they have in place to block the resolution of malicious domain names by clients

in their environments. DNS filtering is available at no cost to MS-ISAC members via its Malicious Domain Blocking and Reporting (MDBR) service: <https://www.cisecurity.org/ms-isac/services/mdbr/>. Please indicate if your organization uses MS-ISAC's MDBR service, another DNS filtering service, or does not currently use DNS filtering. If using a DNS filtering service other than MS-ISAC's MDBR, please complete all questions on this form.

- 3. Implementation Group 1 CIS Control Assessment:** As outlined above, the FY2020 Cyber Security Grant Program has adopted the "Implementation Group 1 CIS Control Assessment Tool", which was derived from the Center for Internet Security's (CIS) Controls version 8. Applicants should familiarize themselves with this tool via the "ReadMe" sheet of the Application Worksheet. To use the tool, select responses from the drop-down menus for each safeguard under "Safeguard Implemented" on the sheets labeled by the National Institute for Standards and Technology (NIST) functions "Identify (ID)", "Protect (PR)", "Detect (DE)", "Respond (RS)", and "Recover (RE)". As responses are provided, the assessment tool will automatically generate scores for each NIST function, as well as other metrics on the "Dashboard" sheet. By periodically updating the responses in this assessment, your organization can measure its progress in closing implementation gaps associated with the CIS Controls.
- 4. Proposed FY2020 Budget:** Applicants must list each project within the budget in order of priority (Project #1 being most critical, etc.) based on the submission of the budget details in the "Budget" tab of E-Grants, as well as the Application Worksheet. For each project, applicants must select a project title, provide a project description and outline proposed expenditures within each of the allowable spending categories (*Federal Spending Category* and *NYS Budget Category*). There is no cap on the number of projects that may be submitted, but the total request for the FY2020 Cyber Security Grant Program funding cannot exceed **\$50,000**.

The total costs identified in the budget plans will be reviewed for reasonable and necessary expenses, and whether they align with the objectives of this grant. The review panel will also reference the "Capability Advancement" section of the Application Worksheet to ensure that projects requested in the "Budget" section address gaps identified from the embedded CIS Controls Assessment Tool or otherwise justified by the applicant.

- ***NOTE: Please ensure the budget amounts reflected in the Application Worksheet correspond to the amounts entered in your E-Grants Application. Inconsistencies in your application documents may lead to a reduction in your score.***

- 5. Capability Advancement:** Applicants must provide a brief description of their current cyber security capabilities and highlight how the proposed projects in their budget for this grant program will address identified capability gaps and improve their overall cyber security posture. Please indicate any combined coordination, planning or training with external agencies or organizations with respect to cyber security. Applicants shall indicate, as clearly as possible, how the overall capabilities of the organization will be enhanced by the requested goods/services outlined in their proposed budget plan.

Applicants will be prompted to select the applicable National Institute for Standards and Technology (NIST) Function (Identify, Protect, Detect, Respond, or Recover) and safeguard to be enhanced by each project. Applicants will also be prompted to identify and describe the following components for each of their requested budget items: current capabilities, current gaps, what attempts have previously been made to address those gaps and how their proposed projects will close those gaps.

- ***NOTE: Applications seeking funding for projects that fall outside the scope of Implementation Group 1 safeguards will be considered, however, strong justification for such projects must be made in your application.***
6. **Multi-Year Planning:** Applicants must provide a Multi-Year Plan that communicates how capabilities (including the maintenance of equipment) will be developed under this grant program and how those capabilities will be enhanced and/or sustained after the successful completion of the projects proposed in your application upon the conclusion of the performance period (August 31, 2023).
 7. **Overall Assessment of Application:** Under the FY2020 Cyber Security Targeted Grant Program, applicants will receive up to ten (10) points based on their “Overall Assessment of Application Score.” This score will be determined by the reviewers based on a complete assessment of the application. Reviewers will assess how well the application addresses the five primary objectives of the FY2020 Cyber Security Grant Program.
 8. **Grant Management Performance History:** Per the Code for Federal Regulations (CFR) 2 CFR Part 200, DHSES is required to assess the risk posed by sub-recipients of federal funding passed through DHSES. For previously funded applicants, DHSES will assess how well they have historically managed federal grant funds. This will include reporting compliance, successful award spend-down, and program objective compliance. Once a prospective applicant’s final overall average score is determined by the review panel, DHSES may subtract up to ten (10) points based on its “Grant Management Performance History” criteria.
 9. **Bonus Points Criteria:** Due to the highly competitive nature of this program and to maximize the impacts of funding across the State, bonus points will be awarded to applicants who have not been previously funded under the Cyber Security Grant Program. All previously unfunded applicants will be awarded five (5) bonus points which will be added to their overall application score.

VI. Application Evaluation Criteria

The following multi-tiered criteria will be used by a committee selected by DHSES to evaluate each application and to determine the best applications for recommendation to the Commissioner to receive grant awards. All grant awards are approved by the Commissioner of DHSES.

A. Tier 1 Criteria

Tier 1 criteria are rated either “yes” or “no” and serve as a baseline by DHSES to determine if applicants are eligible and have appropriately submitted all the required application materials prior to review by the multi-agency review committee. If any of the answers are “no”, the application will be immediately disqualified without further review and will not be considered for an award.

1. Was the application submitted on time?
2. Was the application submitted via E-Grants?
3. Is the application complete, including the **required** Application Worksheet? (the Application Worksheet must be attached in E-Grants by the submission due date)
4. Did the application meet the eligibility requirements (from a county or local unit of government, and a registered member of the MS-ISAC)?

B. Tier 2 Criteria

Applications meeting the Tier 1 review set forth above will be reviewed and evaluated competitively using the criteria specified below. Scores per criterion will be totaled to establish a ranked list of eligible applications for consideration for awards. At the sole discretion of DHSES, applicants may be disqualified due to untimely submission of any requested supporting documentation.

Overall Assessment of Application: Under the FY2020 Cyber Security Targeted Grant Program, applicants will receive up to ten (10) points based on their “Overall Assessment of Application Score.” This score will be determined by the reviewers based on a complete assessment of the application. Reviewers will assess how well the application addresses the five primary objectives of the FY2020 Cyber Security Grant Program.

Bonus Points Criteria: Due to the highly competitive nature of this program and to maximize the impacts of funding across the State, bonus points will be awarded to applicants who have not been previously funded under the Cyber Security Grant Program. All previously unfunded applicants will be awarded five (5) bonus points which will be added to their overall application score.

Grant Management Performance History: Per the new Code for Federal Regulations (CFR) 2 CFR Part 200, DHSES is required to assess the risk posed by sub-recipients of federal funding passed through DHSES. For previously funded applicants, DHSES will assess how well they have historically managed federal grant funds. This will include reporting compliance, successful award spend-down, and program objective compliance. Once a prospective applicant’s final overall average score is determined by the review panel, DHSES may subtract up to ten (10) points based on its “Grant Management Performance History” criteria.

Tier 2 Evaluation Criteria	Point Score Range
CIS Controls Assessment Tool	0-20 points
Proposed Budget	0-30 points
Capability Advancement	0-30 points
Multi-Year Plan	0-10 points
Overall Application	0-10 points
Sub-Total	100 Points Maximum
Bonus Points: Previously Unfunded Applicants	5 points
Grant Management Performance History	0-10 points (Subtracted off the top of final average score)
Total	105 Points Maximum

Applications receiving the highest score based upon panel review will be selected for recommendation to the Commissioner for award. The total scores will be averaged and ranked in order from highest to lowest. The State reserves the right, for the purpose of ensuring the completeness and comparability of proposals, to analyze submissions and make adjustments or normalize submissions in the proposals, including applicants' technical assumptions, and underlying calculations and assumptions used to support the computation of costs, or to apply such other methods, as it deems necessary to make comparisons. In the event of a tie score where one or more applicants may not be fully funded, the applicant with the highest score in the Overall Application section will be ranked higher. Proposed budgets will be reviewed, and items deemed inappropriate, unallowable, or inconsistent with project or program activities will be eliminated. Budgets that include inappropriate and/or unallowable proposed expenditures will receive a reduced score. Grants in the amount of the budgets, as adjusted, will be made to the highest-ranking applicants until funds are insufficient to fund the next ranking application in full. The State reserves the right, at its discretion, to make amendments and/or alter funding levels of one or more applicants based on any new information discovered that would have originally affected the scoring or to not award funding to any application with a final average score of 60 or less.

VII. Checklist of Required Documents

- Applications must be submitted to DHSES via E-Grants with the required attachment uploaded.
- FY2020 Cyber Security Grant Program Application Worksheet must be submitted as an attachment in E-Grants.

VIII. Timeline

DHSES must receive completed grant applications by **5:00 p.m. on May 5, 2022**. Applications received after the due date and time will not be considered. Applications must be submitted via the DHSES E-Grants System. Please note that E-Grants technical assistance will only be available during business hours, including on the date the application is due. Furthermore, all written questions must be submitted to DHSES by **12:00 noon on April 28, 2022** to ensure that a timely response is provided to the applicant.

Grant applicants can expect to be notified of award decisions sometime in June / July of 2022.

IX. Approval and Notification of Award

The Commissioner of DHSES will provide oversight of the grant review process. The Commissioner will announce the final grant award decisions based on the review panel's rating of applications and recommendations. DHSES will notify all applicants in writing as to final grant award determinations. Nothing herein requires or prohibits DHSES to approve grant funding for any one applicant, certain applicants, all applicants or no applicants. Any disbursement of an award is contingent upon entering into a contract with DHSES, as explained in further detail below.

Pursuant to Section 163(9)(c) of the State Finance Law, any unsuccessful Bidder may submit a written request for a debriefing regarding the reasons that the Bid submitted by the Bidder was not selected for award. Requests for a debriefing must be made within 15 calendar days of notification by DHSES that the Bid submitted by the Bidder was not selected for award. An unsuccessful Bidder's written request for a debriefing shall be submitted to DHSES Director of Grants Program Administration. The debriefing shall be scheduled within 10 business days of receipt of the written request by DHSES or as soon as practicable under the circumstances.

Due to the competitive nature of this grant application proposed changes to the scope of the program may not be approved post-award.

X. Administration of Grant Contracts

DHSES will negotiate and develop a grant contract with the applicant based on the contents of the submitted application and intent of the grant program as outlined in this RFA. The grant contract is subject to approval by the NYS Office of the Attorney General and the Office of the State Comptroller before grant funding may actually be disbursed to reimburse project expenses.

The period of performance for contracts supported by the Cyber Security Grant Program funds will be determined once awards have been approved but cannot extend beyond **August 31, 2023**. Although the contract format may vary, the contract will include such standard terms and conditions included in DHSES grant contracts available for review on the DHSES website: <https://www.dhSES.ny.gov/grant-reporting-forms>.

Applicants agree to adhere to all applicable state and federal regulations.

A. Issuing Agency

This RFA is issued by DHSES, which is responsible for the requirements specified herein and for the evaluation of all applications.

B. Filing an Application

Grant applications must be submitted via the automated DHSES E-Grants System. The system allows an agency to complete an application electronically and submit it over the Internet using a secure portal. If, upon reading this RFA, you are interested in completing a grant application and you have not previously been registered to use the DHSES E-Grants system, your agency will need to register and be assigned a username and password. The Registration Request Form can be found at the following Internet address: <https://www.dhSES.ny.gov/e-grants>.

A detailed tutorial on how to use the E-Grants system can also be found at the following Internet address: <https://www.dhSES.ny.gov/targeted-grants>. It will guide you in a step-by-step process through the E-Grants application submission.

C. Reservation of Rights

The issuance of this RFA and the submission of a response or the acceptance of such response by DHSES does not obligate DHSES in any manner. DHSES reserves the right to:

1. Reject any and all applications received in response to this RFA;
2. Withdraw the RFA at any time at DHSES' sole discretion;
3. Make an award under the RFA in whole or in part;
4. Disqualify any applicant whose conduct and/or application fails to conform to the requirements of the RFA;
5. Seek clarifications and revisions of the applications;
6. Use application information obtained through site visits, management interviews and the State's investigation of an applicant's qualifications, experience, ability or financial standing, and any material or information submitted by the applicant in response to DHSES' request for clarifying information in the course of evaluation and/or selection under the RFA;
7. Prior to the application opening, amend the RFA specifications to correct errors or oversights, or to supply additional information, as it becomes available;
8. Prior to the application opening, direct applicants to submit application modifications addressing subsequent RFA amendments;
9. Change any of the scheduled dates;
10. Eliminate any non-mandatory, non-material specifications that cannot be complied with by all the prospective applicants;
11. Waive any requirements that are not material;
12. Negotiate with successful applicants within the scope of the RFA in the best interests of the State;
13. Conduct contract negotiations with the next responsible applicant, should DHSES be unsuccessful in negotiating with the selected applicant;
14. Utilize any and all ideas submitted in the applications received;

15. Unless otherwise specified in the RFA, every offer is firm and not revocable for a period of 60 days from the application opening; and,
16. Communicate with any applicant at any time during the application process to clarify responses and /or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of an applicant's proposal and/or to determine an applicant's compliance with the requirements of this RFA.
17. Award grants based on geographic or regional considerations to serve the best interests of the State.
18. Terminate, renew, amend or renegotiate contracts with applicants at the discretion of DHSES.
19. Periodically monitor the applicant's performance in all areas mentioned above, in addition to the activities in the contract.
20. Revoke funds awarded to an applicant, or enforce any available sanction against any applicant, who materially alters the activities or is in material noncompliance under the grant award, or who does not implement an approved project within 60 days of the final contract approval.
21. Consider all applications and documentation submitted as State agency records subject to the New York State Freedom of Information Law (Public Officers Law, Article 6). Any portion of the application that an applicant believes constitutes proprietary or critical infrastructure information entitled to confidential handling, as an exception to the Freedom of Information Law, must be clearly and specifically designated in the application.
22. Applicants funded through this program agree to provide DHSES, upon request at any time during the life of the grant contract, such cooperation and information deemed necessary by DHSES to ascertain: (1) the nature and extent of any threats or hazards that may pose a risk to the applicant; and (2) the status of any corresponding applicant or applicant plans, capabilities, or other resources for preventing, protecting against, mitigating, responding to, and recovering from such threats or hazards.
23. Require applicants to attend and participate in any DHSES-sponsored conferences, training, workshops or meetings (excluding those identified by DHSES as voluntary) that may be conducted, by and at the request of DHSES, during the life of the grant contract.
24. In its sole discretion, reserves the sole discretion to increase or decrease the total funding available for this program at any time, resulting in more or fewer applications funded under this RFA.

DHSES may exercise the foregoing rights at any time without notice and without liability to any responding applicant or any other party for its expenses incurred in preparation of responses hereto or otherwise. All costs associated with responding to this RFA will be at the sole cost and expense of the applicant.

D. Term of the Contract

Any resulting contract or agreement for more than \$50,000 from this RFA will be effective only upon approval by both the NYS Office of the Attorney General and State Comptroller. Any resulting contract for \$50,000 and under from this RFA will be effective upon signature of both parties. For grants valued at \$10,000 or less, a Purchase Order invoking a "Letter of Agreement" between DHSES and the successful applicant will be issued.

E. Payment and Reporting Requirements of Grant Awardees

1. Standard Cost Reimbursement Contract

Each successful applicant must enter into a standard cost reimbursement contract with DHSES. Such contract will include this Request for Applications, the successful applicant's proposal, any attachments or exhibits and the standard clauses required by the NYS Attorney General for all State contracts (available upon request). The contract will be subject to approval by the Attorney General and State Comptroller. Although the contract format may vary, the contract will include such clauses, information, and rights and responsibilities as can be found on the DHSES website, including:

APPENDIX A-1 -	Agency Specific Clauses or a Letter of Agreement (Depending upon Funding Amount)
APPENDIX B -	Budget
APPENDIX C -	Payment and Reporting Schedule
APPENDIX D -	Workplan/Special Conditions

For purposes of this RFA, these terms and conditions are incorporated by reference and the applicant must agree to the inclusion of all of these terms and conditions in any resulting grant contracts as part of the application submission. Copies of the standard terms and conditions included in DHSES grant contracts are available for review on the DHSES website at <https://www.dhSES.ny.gov/grant-reporting-forms>. Payments will be made subject to proper documentation and compliance with reimbursement procedures and all other contractual requirements.

2. Compliance with State and Federal Laws and Regulations, Including Procurement and Audit Requirements

2 CFR Part 200

Applicants (also referred to herein as "Subrecipients") are responsible to become familiar with and comply with all state and federal laws and regulations applicable to these funds. Applicants are required to consult with the DHSES standard contract language (referenced above) for more information on specific requirements. Additionally, applicants must comply with all the requirements in 2 CFR Part 200 (Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards). Applicants are required to understand and adhere to all federal requirements. You may access 2 CFR Part 200 at: <https://www.ecfr.gov/cgi-bin/text-idx?SID=1c9afe07b881b32365c2f4ce1db64860&mc=true&node=pt2.1.200&rgn=div5>

Procurements

Additionally, applicants must follow and comply with all procurement procedures under General Municipal Law 5A and 2 CFR Part 200, Subpart D (see 2 CFR §§200.317-.327), and/or any other state or federal regulations applicable to these funds and will be subject to monitoring by DHSES to ensure compliance.

Single Audit

Applicants that expend \$750,000 or more from all Federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the requirements of U.S. Government Accountability Office's (GAO) Government Auditing Standards, located at <http://www.gao.gov>, and the requirements of Subpart F of 2 CFR Part 200 located at: <http://www.ecfr.gov/cgi-bin/text-idx?node=sp2.1.200.f>.

Environmental and Historic Preservation (EHP) Compliance: As a federal agency, DHS/FEMA is required to consider the effects of its actions on the environment and/or historic properties to ensure that all activities and programs funded by DHS/FEMA, including grant-funded projects, comply with Federal EHP regulations, laws and Executive Orders, as applicable. Sub-recipients proposing projects that have the potential to impact the environment, including but not limited to the modification or renovation of existing buildings, structures and facilities, or new construction including replacement of facilities, must participate in the DHS/FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with supporting documentation so that DHS/FEMA may determine whether the proposed project has the potential to impact environmental resources and/or historic properties. In some cases, DHS/FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. The EHP review process must be completed before funds are released to carry out the proposed project; otherwise DHS/FEMA may not be able to fund the project due to noncompliance with EHP laws, executive order, regulations, and policies.

Conflict of Interest

Pursuant to 2 CFR §200.112, in order to eliminate and reduce the impact of conflicts of interest in the sub-award process, applicants must follow their own policies and procedures regarding the elimination or reduction of conflicts of interest when making sub-awards. Applicants are also required to follow any applicable state, local, or Tribal statutes or regulations governing conflicts of interest in the making of sub-awards.

The applicant must disclose to the respective Contract Representative, in writing, any real or potential conflict of interest as defined by the Federal, state, local, or Tribal statutes or regulations or their own existing policies, which may arise during the administration of the Federal award within five days of learning of the conflict of interest. Similarly, applicants must disclose any real or potential conflict of interest to the pass-through entity (State) as required by the applicant's conflict of interest policies, or any applicable state, local, or Tribal statutes or regulations.

Conflicts of interest may arise during the process of DHS/FEMA making a Federal award in situations where an employee, officer, or agent, any members of his or her immediate family, his or her partner has a close personal relationship, a business relationship, or a professional relationship, with an applicant, sub-applicant, recipient, subrecipient, or DHS/FEMA employees.

Additionally, applicants must disclose, in writing to the Federal Awarding Agency or to the pass-through entity (State) all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures can result in any of the remedies described in § 200.339. Remedies for noncompliance, including suspension or debarment. (See also 2 CFR part 180 and 31 U.S.C. 3321).

Contracting with Small and Minority Firms, Women's Business Enterprise and Labor Surplus Area Firms

Pursuant to New York State Executive Law Article 15-A, the New York State Division of Homeland Security and Emergency Services recognizes its obligation under the law to promote opportunities for maximum feasible participation of certified minority-and women-owned business enterprises and the employment of minority group members and women in the performance of New York State Division of Homeland Security and Emergency Services contracts. Minority and women-owned business enterprises can be readily identified on the directory of certified businesses at: <https://ny.newnycontracts.com/>.

All qualified applicants shall be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

Consistent with 2 CFR §200.321, non-Federal contracting entities must take all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible.

Affirmative steps must include:

1. Placing qualified small and minority businesses and women's business enterprises on solicitation lists;
2. Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
3. Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
4. Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises;
5. Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce; and
6. Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs (1) through (5) of this section.

For purposes of this solicitation, applicants and subcontractors are hereby notified the State of New York has set an overall goal of **30% for MWBE participation** or more, **15% for Minority-Owned Business Enterprises** ("MBE") participation and **15% for Women-Owned Business Enterprises** ("WBE") participation, based on the current availability of qualified MBEs and WBEs for your project needs.

An applicant on any contract resulting from this procurement ("Contract") must incorporate the affirmative steps above into its grant management policies and procedures.

Further, pursuant to Article 15 of the Executive Law (the "Human Rights Law"), all other State and Federal statutory and constitutional non-discrimination provisions, the applicant and subrecipients

will not discriminate against any employee or applicant for employment because of race, creed (religion), color, sex, national origin, sexual orientation, military status, age, disability, predisposing genetic characteristic, marital status or domestic violence victim status, and shall also follow the requirements of Human Rights Law with regard to non-discrimination on the basis of prior criminal conviction and prior arrest.

Sexual Harassment Prevention

By submitting this application, Applicants are certifying that Applicant has a policy addressing sexual harassment prevention and that applicant provides sexual harassment training to all its employees on an annual basis that meets the Department of Labor's model policy and training standards. If Applicant cannot make the certification, the Applicant may provide an explanatory statement with its bids detailing the reasons why the certification cannot be made.

Use of Service-Disabled Veteran-Owned Business Enterprises in Contract Performance

Article 17-B of the Executive Law enacted in 2014 acknowledges that Service-Disabled Veteran-Owned Businesses (SDVOBs) strongly contribute to the economics of the State and the nation. As defenders of our nation and in recognition of their economic activity in doing business in New York State, bidders/proposers for this contract for commodities, services or technology are strongly encouraged and expected to consider SDVOBs in the fulfillment of the requirements of the contract. Such partnering may be as subcontractors, suppliers, protégés or other supporting roles. SDVOBs can be readily identified on the directory of certified businesses at <https://online.ogs.ny.gov/SDVOB/search>

Bidders/proposers need to be aware that all authorized users of this contract will be strongly encouraged to the maximum extent practical and consistent with legal requirements of applicable federal laws and regulations including 2 CFR Part 200, State Finance Law, General Municipal Law and the Executive Law to use responsible and responsive SDVOBs in purchasing and utilizing commodities, services and technology that are of equal quality and functionality to those that may be obtained from non-SDVOBs. Furthermore, bidders/proposers are reminded that they must continue to utilize small, minority and women-owned businesses consistent with current State Law. Utilizing SDVOBs in State contracts will help create more private sector jobs, rebuild New York State's infrastructure, and maximize economic activity to the mutual benefit of the contractor and its SDVOB partners. SDVOBs will promote the contractor's optimal performance under the contract, thereby fully benefiting the public sector programs that are supported by associated public procurements.

Public procurements can drive and improve the State's economic engine through promotion of the use of SDVOBs by its contractors. The State, therefore, expects bidders and proposers to provide maximum assistance to SDVOBs in their contract performance. The potential participation by all kinds of SDVOBs will deliver great value to the State and its taxpayers.

For purposes of this solicitation, applicants and subrecipients are hereby notified the State of New York has set an overall goal of 6% for SDVOB participation or more.

Contractor will report on actual participation by each SDVOB during the term of the contract to the contracting agency/authority according to policies and procedures set by the contracting agency/authority.

Worker's Compensation and Disability Benefits Insurance Coverage

By submitting this application, Applicants are certifying that Applicant has workers' compensation and disability coverage. If Applicant cannot make the certification, the Applicant may provide an exemption statement with its bids detailing the reasons why the certification cannot be made.

3. Iran Divestment Act

As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, a new provision has been added to the State Finance Law (SFL), § 165-a, effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b), the initial list is expected to be issued no later than 120 days after the Act's effective date, at which time it will be posted on the OGS website.

By submitting a proposal in response to this RFA, or by assuming the responsibility of a Contract awarded hereunder, the applicant (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, applicants are advised that once the list is posted on the OGS website, any applicant seeking to renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should DHSES receive information that a person is in violation of the above-referenced certification, DHSES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then DHSES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Contractor in default. DHSES reserves the right to reject any bid or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the prohibited entities list after contract award.

4. Vendor Responsibility

State Finance Law §163(9)(f) requires a State Agency to make a determination that an applicant is responsible prior to awarding that applicant a State contract which may be based on numerous factors, including, but not limited to the applicants: (1) financial and organizational capacity; (2) legal authority to do business in this State; (3) integrity of the owners, officers, principals, members, and contract managers; and (4) past performance of the applicant on prior government

contracts. Thereafter, applicants shall at all times during the Contract term remain responsible. The applicant agrees, if requested by the Commissioner of DHSES, or his or her designee, to present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity. DHSES requires that vendors file the required Vendor Responsibility Questionnaire online via the New York State VendRep System. To enroll in and use the New York State VendRep System, see the VendRep System, see the VendRep System Instructions available at:

http://www.osc.state.ny.us/vendrep/info_vrsystem.htm or go directly to the VendRep system online at <https://onlineservices.osc.state.ny.us/Enrollment/login?0> . Vendors must provide their New York State Vendor Identification Number when enrolling. To request assignment of a Vendor ID or for VendRep System assistance, contact the Office of the State Comptroller's Help Desk at 866-370-4672 or 518-408-4672 or by email at ITServiceDesk@osc.state.ny.us. Vendors opting to complete and submit a paper questionnaire can obtain the appropriate questionnaire from the VendRep website http://www.osc.state.ny.us/vendrep/forms_vendor.htm or may contact the Office of the State Comptroller's Help Desk for a copy of the paper form. Applicants will also be required to complete and submit a Vendor Responsibility Questionnaire prior to contracting.

a) Suspension of Work for Non-Responsibility:

The Commissioner of DHSES or his or her designee, in his or her sole discretion, reserves the right to suspend any or all activities under the Contract, at any time, when he or she discovers information that calls into question the responsibility of the applicant. In the event of such suspension, the applicant will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the Commissioner of DHSES or his or her designee issues a written notice authorizing the resumption of performance under the Contract.

b) Termination for Non-Responsibility:

Upon written notice to the applicant, and a reasonable opportunity to be heard by appropriate DHSES officials or staff, the Contract may be terminated by the Commissioner of DHSES or his or her designee at the applicant's expense where the applicant is determined by the Commissioner of DHSES or his or her designee to be non-responsible. In such event, the Commissioner of DHSES or his or her designee may complete the contractual requirements in any manner he or she may deem advisable and pursue legal or equitable remedies for breach. Applicants shall at all times during the Contract term remain responsible. The applicant agrees, if requested by the Commissioner of DHSES, or his or her designee, to present evidence of its continuing legal authority to do business in New York State, integrity, experience, ability, prior performance, and organizational and financial capacity.

F. Satisfactory Progress

Satisfactory progress toward implementation includes but is not limited to; executing contracts and submitting payment requests in a timely fashion, retaining consultants, completing plans, designs, reports, or other tasks identified in the work program within the time allocated for their

completion. DHSES may recapture awarded funds if satisfactory progress is not being made on the implementation of a grant project.

G. General Specifications

By submitting the application, the applicant attests that:

1. Applicant has express authority to submit on behalf of the applicant's agency.
2. Submission of an application indicates the applicant's acceptance of all conditions and terms contained in this RFA, including Appendices A-1 and C, and all other terms and conditions of the award contract.
3. The application and any resulting grant, if awarded, must adhere to, and be in full compliance with any, resulting contract(s) and relevant federal and states policies and regulations or be subject to termination.
4. Any not-for-profit subrecipients are required to be prequalified, prior to contract execution, by the State of New York upon application submission through the New York State Grants Gateway (<https://grantsgateway.ny.gov>)
5. If your organization is not currently doing business with NYS, you will need to submit a Substitute W-9 form to obtain a NYS Vendor ID. The form is available on the Office of the State Comptroller website at: <http://www.osc.state.ny.us/state-agencies/forms>.
6. Contract Changes - Contracts with applicants/subrecipients may be executed, terminated, renewed, increased, reduced, extended, amended, or renegotiated at the discretion of the Commissioner of DHSES, in light of applicants/subrecipients performance, changes in project conditions, or otherwise.
7. Records – Applicants/subrecipients must keep books, ledgers, receipts, work records, consultant agreements and inventory records pertinent to the project; and in a manner consistent with DHSES contractual provisions and mandated guidelines.
8. Liability - Nothing in the contract between DHSES and the applicant shall impose liability on the State of New York or DHSES for injury incurred during the performance of approved activities or caused by use of equipment purchased with grant funds.
9. Reports - A provider agency shall submit to the DHSES reports in a format and time schedule specified in the grant contract, which shall include a description of the program efforts undertaken during the report period and the current status of the project.
10. Tax Law Section 5-a Certification – In accordance with section 5–a of the Tax Law, sub-recipients will be required, prior to the approval of any contract awarded as a result of this RFA, to certify that it and its affiliates, subcontractors, and subcontractors' affiliates have registered with the New York State Tax Department for the purpose of collection and remittance of sales and use taxes. In order to trigger this certification requirement, a subrecipient or its affiliates, subcontractor, or subcontractors' affiliates must have made more than \$300,000 in sales of tangible personal property or taxable services to location within New York State and the contract must be valued in excess of \$15,000. Certification will take the form of a completed Tax Form ST-220 (1/05).
11. Standard Contract Provisions - Grant contracts executed as a result of this RFA process will be subject to the standard clauses for New York State Contracts as

referenced herein and as located at:

https://online.ogs.ny.gov/purchase/biddocument/23128i_AppendixA.pdf

12. Compliance with Procurement Requirements - The applicant shall certify to DHSES that all applicable federal and contractual procurement procedures were followed and complied with for all procurements.

H. Special Conditions

New York State Emergency Management Certification and Training Program

1. Participation in, and successful completion of, the New York State Emergency Management Certification and Training Program (EMC Training Program) is a mandatory requirement under this Contract and a condition of funding. The EMC Training Program will be made available to, and required for, DHSES-specified county and city government officials in order to ensure a consistent emergency management preparedness and response strategy across the State. Attendee substitutions, except as expressly approved by DHSES, shall not be permitted or deemed to be in compliance with this requirement.
2. To fulfill the EMC Training Program requirement of the Contract and in order to be eligible for funding under this Contract, applicants must arrange for DHSES-specified applicant employees to receive and acknowledge receipt of EMC Training no later than 180 days after execution of this Contract. Copies of the training certificates for each required participant must be submitted to DHSES upon execution of the Contract, or, in the event that training is scheduled, but not yet complete, the applicant will be required to submit a signed statement indicating the scheduled future dates of attendance, and no later than thirty (30) days after the training is complete, forward such training certificates to DHSES. Continued compliance with the EMC Training Program also requires an annual refresher training of one day per 365 day-cycle from the date of initial training for previously trained individuals if such person remains employed by the applicant and fulfilling the same functions as he or she fulfilled during the initial training. Should a new employee be designated to serve in the DHSES-specified positions, then he or she must come into compliance with the EMC Training Program requirements not later than 180 days after taking office.
3. Applicants must commit to active participation in a DHSES Annual Capabilities Assessment as a condition of funding. Active participation includes making reasonable staff, records, information, and time resources available to DHSES to perform the Annual Capabilities Assessment and meet the objectives and goals of the program. Applicants must be aware that the process of conducting a DHSES Annual Risk Assessment is an ongoing process and requires a continued commitment on the part of the applicant to ensure that it is effective.
4. All applicants funded through this program agree to provide DHSES, upon request at any time during the life of the grant contract, such cooperation and information deemed necessary by DHSES to ascertain: (1) the nature and extent of any threats or hazards that may pose a risk to the recipients or subrecipients; and (2) the status of any corresponding recipients or subrecipients plans, capabilities, or other resources for preventing, protecting against, mitigating, responding to, and recovering from such threats or hazards.

5. Additionally, pursuant to Article 26 of the NYS Executive law, DHSES is authorized to undertake periodic drills and simulations designed to assess and prepare responses to terrorist acts or threats and other natural and man-made disasters. Funded applicants agree to attend and participate in any DHSES-sponsored conferences, training, workshops or meetings (excluding those identified by DHSES as voluntary) that may be conducted, by and at the request of DHSES, during the life of the grant contract.
6. Failure to comply with any of the requirements, as listed above, may result in sanctions up to and including the immediate suspension and/or revocation of the grant award.

XI. Questions

Questions regarding the FY2020 Cyber Security Grant Program should be directed to the following e-mail address: Grant.Info@dhSES.ny.gov. To the degree possible, each inquiry should cite the RFA section and paragraph to which it refers. Written questions will be accepted until **12:00 noon on April 28, 2022.**

Updates and frequently asked questions will be posted on the NYS Division of Homeland Security and Emergency Services (DHSES) website: <https://www.dhSES.ny.gov/targeted-grants>. Please check the website frequently for updates.

All questions regarding the E-Grants System should be directed to DHSES via e-mail (Grant.Info@dhSES.ny.gov) or telephone (866-837-9133). No technical assistance will be available after **5:00 pm on May 5, 2022.**

Exhibit A: Allowable Costs Matrix

Reminder: Allowable costs for the FY2020 Cyber Security Grant Program are more restrictive than the more general State Homeland Security Program (SHSP) because of the specialized nature of this targeted grant program. Please note that Organizational, Management & Administrative (M&A) as well as Construction costs, and the hiring of Personnel are not allowable under the FY2020 Cyber Security Grant Program.

Personnel Cap: Under the FY2020 Cyber Security Grant Program, there is a 50% cap on personnel costs. Personnel Costs include OT/Backfill for Training and Exercises and most Consultant Costs (unless the consultant is developing defined deliverable or installing equipment).

Planning Costs
Public education & outreach
Develop and enhance plans and protocols
Develop and conduct assessments
Hiring of contractors/consultants to assist with planning activities
Conferences to facilitate planning activities
Materials required to conduct planning activities
Travel/per diem related to planning activities
Overtime, backfill and fringe costs
Equipment Categories <small>AEL link: https://www.fema.gov/authorized-equipment-list</small>
Biometric User Authentication Devices
Remote Authentication Systems
Encryption Software
Data Transmission Encryption Systems
Forensic Software (for purposes of analysis and investigation of cyber-related incidents)
Malware Protection Software
Firewalls (Personal and Network)
Intrusion Detection/Prevention System
Vulnerability Scanning Tools
Hardware, Computer, Integrated (hardware components that will protect against cyber security threats)
Other Items
Training Costs
Overtime & backfill for personnel attending FEMA-sponsored & approved training classes & technical assistance programs
Training workshops & conferences
Travel
Hiring of contractors/consultants
Supplies

Exercise Costs
Design, Develop, Conduct & Evaluate an Exercise
Exercise planning workshop
Hiring of contractors/consultants
Overtime & backfill costs, including expenses for personnel participating in FEMA exercises
Implementation of HSEEP
Travel
Supplies

Unallowable Costs

Management and Administrative (M&A) Costs
Hiring of full or part-time staff or contractors/consultants to assist with the management of the respective grant program, application requirements, compliance with reporting & data collection requirements
Development of operating plans for information collection & processing necessary to respond to FEMA data calls
Overtime and backfill costs
Travel
Meeting related expenses
Authorized office equipment
Recurring expenses such as those associated with cell phones & faxes during the period of performance of the grant program
Leasing or renting of space for newly hired personnel during the period of performance of the grant program
Organizational Categories
Overtime for information, investigative, & intelligence sharing activities
Hiring of new staff positions/contractors/consultants for participation in information/intelligence analysis & sharing groups or fusion center activities
Construction Costs
All Construction Costs

Exhibit B: MS-ISAC Membership (Requirement for Grant Applicants)

Overview: The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a program area of the Center for Internet Security and is funded by the U.S. Department of Homeland Security. The MS-ISAC has been designated as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments. Through its state-of-the-art 24/7 Security Operations Center, the MS-ISAC serves as a central resource for situational awareness and incident response for these SLTT governments.

There is no cost to become a member of the MS-ISAC. The only requirement to enroll as a member organization is completion of online registration at the following link:

<https://learn.cisecurity.org/ms-isac-registration>

MS-ISAC Member Benefits:

- **24/7 Security Operations Center (SOC)**
- **Incident response assistance**
- **Cybersecurity exercises**
- **Cybersecurity advisories & daily tips**
- **Cyber event notifications**
- **Awareness/education materials**
- **Vulnerability assessment services**
- **Secure portals for communication & document sharing**
- **Member initiatives & collaborative resources**
- **Malicious Code Analysis Platform (MCAP)**
- **Monthly newsletters, webinars & threat briefings**
- **Alert status map**
- **Cyber threat information & analytical products**
- **Free CIS SecureSuite membership**
- **Discounts on training and other products through the CIS CyberMarket**
- **Nationwide Cyber Security Review (NCSR)**
- **Vulnerability Management Program (VMP)**

Exhibit C: Cyber Security Resources for Local Governments

DHSES Cyber Incident Response Team (CIRT)

Cyber Security Incident Response

- Remote and on-site response options available
- “In the moment,” incident-specific recommendations on containment, eradication, and recovery
- Real time cyber-threat intelligence sharing
- Post-incident recommendations to help your entity achieve a more proactive cyber security program

Digital Forensics

- Analysis of your incident’s indicators of compromise to assist with timely identification of root cause and effective remediation planning
- Analysis of incident-relevant logs and system images via our secure portal – or DHSES CIRT will come to you
- Benefit from DHSES CIRT’s expertise and industry-standard toolset without the overhead of managing “in-house”
- Available in support of active incident response or as proactive analysis

Cybersecurity Risk Assessment Services

- Customized to fit your needs, DHSES CIRT will assess the technical and governance aspects of your cyber-program:
 - Edge Assessment – An objective assessment of your cyber-perimeter from the perspective of a potential attacker, this offering enumerates your public-facing systems and publicly available information, highlighting potential weaknesses that could be exploited externally to gain internal system access
 - Internal Vulnerability Assessment – Focused within your network perimeter, this offering identifies opportunities to limit the impact of an internal compromise, whether it originated externally or due to a scenario involving insider threat
 - Security Program Posture Assessment – A guided assessment of your organization’s cybersecurity maturity, assessed against the CIS controls, in key areas shown to reduce the risks associated with cyber-incidents
- Upon completion of your assessment, you will receive a comprehensive report with prioritized remediation recommendations on the design and implementation of solutions that balance risk mitigation with cost

Phishing Testing and Awareness Services

- DHSES CIRT will work with Information Technology (IT) and executive leadership to schedule a phishing campaign that simulates a targeted attack. Upon completion, you will receive a report detailing how many of your users recognized the phishing emails and reacted to them
- Several DHSES CIRT recommended training modules are available for all end users regardless of performance during the Phishing Assessment
- Following completion of the phishing exercise and follow-on training, DHSES CIRT provides a report that can be used to jump start your cyber security awareness training and reduce your risk

Cyber Security Incident Response Tabletop Exercises – A DHSES CIRT team will walk your organization’s leadership through a mock cyber security incident, which will help identify gaps in your incident response plan and prepare your team in case of a real cyber-incident.

Please contact the DHSES CIRT at (844) OCT-CIRT to report a cybersecurity incident or contact us at cirt@dhSES.ny.gov for more information on proactive services. You can also find more information on the CIRT's offerings on its website, <https://www.dhSES.ny.gov/cyber-incident-response-team>.

Nationwide Cyber Security Review (NCSR)

The NCSR is a voluntary self-assessment survey designed to evaluate an organization's cyber security management practices. Available annually, the NCSR generates customized reports to help participants understand their cyber security maturity. Recommendations for cyber improvements and summary reports gauging security measures against peers, using anonymized data, are also included. More information is available at <https://msisac.cisecurity.org/resources/ncsr/>. Please contact NCSR@cisecurity.org or (518) 880-0736 to sign up for the NCSR.

NYS Intelligence Center (NYSIC)

Cyber Analysis Unit (CAU) – The NYSIC-CAU provides a variety of strategic, tactical, and technical intelligence in the form of intelligence bulletins or email and phone notifications. In order to receive these products and resources please contact the CAU at (518) 786-2191 or CAU@nysic.ny.gov.

NYS Office of Information Technology Services (ITS)

Local Government Cyber Security Toolkit – Features practical information, risk assessment tools and guidance to help local government minimize cyber risk and increase cyber security awareness, available at (its.ny.gov/ciso/local-government – TOOLKIT tab). Components of the toolkit include:

Asset Inventory Guidance & Templates – to help identify critical information assets for risk assessment.

Critical Security Controls Assessment Framework & User Guide – to assist with evaluating, prioritizing and tracking the 20 security measures that reduce the risk of the most pervasive and dangerous cyber-threats.

Application Risk Assessment Tool – helps to identify and evaluate application system risk and prioritize remediation efforts in a standardized manner.

Secure System Development Life Cycle (SSDLC) Resources - defines security requirements and tasks that must be considered and addressed within every system, project or application that are created or updated to address a business need.

New York State Information and Cyber Security Awareness Training - designed to improve employees' cyber security awareness and to strengthen overall cyber security readiness.

New York State Cyber Security Policies, Standards and Guidelines - Provides a menu of ITS security policies that local governments can scale and replicate for their cyber security programs.

Registration for Multi-State Information Sharing and Analysis (MS-ISAC) membership - to allow access to associated cyber resources and services.

Non-Technical Cyber Security Guides – helpful for increasing the information security awareness level of those local government staff in non-technical positions (such as elected officials and administrators, available at (its.ny.gov/ciso/local-government – click on the REPORTS tab).

Awareness, Training, and Events – Provides training videos, best practices, links to free/discounted training opportunities (e.g., FedVTE, Cybrary) and other offerings and is available at <http://its.ny.gov/awarenesstrainingevents> and at its.ny.gov/ciso/local-government – click on the AWARENESS, TRAINING & EVENTS tabs.

Vulnerability Scanning – Web Application Scanning (WAS) is used to identify known security vulnerabilities in web applications and web sites, such as cross-site scripting, SQL injection, command execution, directory traversal and insecure server configuration. For more information please contact the CISO Vulnerability Management Team at CISO.vm@its.ny.gov.

Incident Response- when an incident occurs, the NYS Cyber Command Center (CyCom) Cyber Incident Response Team (CIRT) assists in assessing scope, magnitude and source of intrusions. The CIRT can perform forensics, log analysis, and malware reverse-engineering. In addition, the CIRT will recommend steps to remediate the problem and mitigate future attacks. Contact at cycom@its.ny.gov or (518) 242-5045.

NYS Office of General Services (OGS)

IT Umbrella, System Integration, Project Consulting, Manufacturing, Distribute – This group of contracts includes three different umbrella contracts that municipalities can use to procure cyber security technology and services from accredited contractors and is available at https://ogs.ny.gov/purchase/snt/lists/gp_73600.asp. For other IT contracting questions please contact OGS Procurement Services at (518) 474-6717 or customer.services@ogs.ny.gov.

U.S. Department of Homeland Security (DHS)

DHS Cyber Hygiene (CyHy) Program – Provides an assessment encompassing continuous configuration error and vulnerability scanning of public, internet-facing information systems. A report is provided to participants on a recurring basis which includes remediation and mitigation recommendations to address identified vulnerabilities. This service is free. Contact SLTTCyber@hq.dhs.gov to request these services.

Risk and Vulnerability Assessments (RVA) – Provides a broader suite of cyber security services than the CyHy Program, including penetration testing, social engineering, wireless discovery and identification, database scanning, and operating system scanning. This is recommended for larger organizations. This service is free, and a report is provided to participants annually. Contact SLTTCyber@hq.dhs.gov to request these services.

DHS Cyber Resilience Review (CRR) – The CRR is a non-technical assessment to evaluate an organization’s operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals and is available at <https://www.us-cert.gov/ccubedvp/assessments>.

DHS Cyber Infrastructure Survey Tool (C-IST) – The C-IST is a facilitated assessment of cyber security controls related to critical IT services. The C-IST is intended to assist government and private sector

participants in surveying cyber protection in 5 domains. More information is available at https://cdn.fedweb.org/fed-91/268/CIST_Fact_Sheet_2015.pdf.

DHS External Dependencies Management (EDM) Assessment – The EDM Assessment is a non-technical facilitated assessment to help stakeholders assess and manage risks arising from external dependencies, specifically dependencies on the information and communication technology service supply chain. More information is available at <http://static1.1.sqspcdn.com/static/f/869587/26055675/1426700102660/EDM+Fact+Sheet+2014.pdf?token=ypiA0Bflcc1qJooa1q%2BCrxdRXw%3D>.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Assessments – ICS-CERT performs cyber assessments to safeguard the nation’s critical infrastructure. These assessments are available at <https://ics-cert.us-cert.gov/Assessments>.

Federal Cyber Incident Unified Message – This message provides useful points of contact in the federal government as well as detailed descriptions of when to report cyber incidents, what to report, how to report, and types of federal responses, and it is available at <https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf>.

Federal Ransomware Guidance – This guide has preventive and response advice for ransomware, and it is available at https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf.

Exhibit D: Best Practices for Preparing an Effective Grant Application

What to do when you have received the Request for Applications (RFA):

- It is important to start early in preparing your application, highlighting deadlines and/or tasks that must be completed as part of the application process.
- Review all plans, strategies, policies and documents related to the grant you are applying for to ensure you can appropriately address the goals and objectives pertaining to the nature of the grant opportunity.

What to do when you are completing the application:

- Ensure that the proposed budget is realistic, reasonable, and articulate how your budget will address the objectives of the grant opportunity.
- Review and evaluate the scoring criteria. Pay close attention to the sections that are weighted the most first as they have a greater impact on your overall score.
- If your grant application requires you to reference goals and/or objectives, make sure the goals and objectives you cite are measurable. Goals should reflect the long-term and global impact of a program or project. Meanwhile, objectives should be specific and measurable building blocks designed to meet your goals.
- Create an evaluation plan that demonstrates how you will assess your proposed projects for effectiveness and/or meeting the objectives of the grant opportunity, even if such a plan is not required.
- Address steps that will be taken to institutionalize, sustain, or enhance the capabilities or proposed project being developed after grant funding has been exhausted.

What to do prior to submitting your application:

- Make sure that you have completed all the required sections of the application. Applicants are strongly recommended to share their completed applications with a colleague to ensure that the application is clearly written and addresses all the objectives of the grant opportunity.

Service Description for Unit 42 Public Sector Expertise on Demand Subscription

Palo Alto Networks' Unit 42 Public Sector Expertise on Demand Subscription ("EOD Subscription") is available to federal government (where applicable), state and local government, and education (both K-12 and higher education) entities ("Customer(s)"). This Service Description outlines the EOD Services available to an EOD Subscription Customer. This EOD Subscription shall be subject to the terms and conditions in the [End User Agreement](#) and [Unit 42 Public Sector Expertise on Demand Subscription Addendum](#).

1. Description of Services Available for Use

In purchasing the EOD Subscription, Customer will receive on-demand access to the Services set forth in the attached Appendix A (Unit 42 Public Sector Expertise on Demand Subscription Services List), subject to fixed annual maximum number of consulting hours.

2. Delivery of Service

Unit 42 consulting hours are delivered in fifteen (15) minute increments and may be used to obtain any of the EOD Services described in Appendix A, all of which are provided remotely in the United States unless otherwise agreed to in writing. If Customer requires more Unit 42 consulting hours than originally purchased, Customer may upgrade its subscription to a higher service tier as described in Section 5 of this Service Description. Upon Customer's request, Palo Alto Networks will provide Customer with an estimate of the Unit 42 consulting hours needed to perform the relevant EOD Services, BUT MAKES NO REPRESENTATION OR WARRANTY AND PROVIDES NO GUARANTEE THAT SUCH EOD SERVICES WILL BE ACCOMPLISHED WITHIN THE ESTIMATED TIME.

3. Palo Alto Networks' Responsibilities

There are no pre-set deliverables as part of the EOD Subscription. Depending on the EOD Services performed, Palo Alto Networks may provide the following:

- Verbal Status Updates: Unit 42 will provide verbal status updates for major findings or as requested. Verbal status updates will include findings to date, activities completed, plans for the next reporting period, issues requiring attention, and budgetary updates if requested.
- Executive Summary Report: At the request of the Customer, Unit 42 will generate a written summary report that details the analysis performed and subsequent findings.

4. Kickoff and Notification

Unit 42 will, with Customer's participation, conduct an initial kickoff to review Customer's primary focus and objectives under this Service Description. Customer and Unit 42 will identify key activities and work streams, with associated prioritization and Customer team members. Subsequent requests by Customer to obtain any of the EOD Services described in Appendix A shall be provided in writing by sending an email to the designated Unit 42 EOD email address, which will be provided to Customer at kickoff. Unit 42 will provide Customer

with periodic updates summarizing the number of EOD hours consumed and the number remaining in the Term.

5. Limitation on Total Annual Hours

In purchasing the EOD Subscription, Customer shall receive on-demand access to Services, up to an annual maximum number of consulting hours as set forth in the table below. In addition, Customer may purchase additional tiers of service hours for their EOD Subscription, as needed, by upgrading to a higher service tier at any time during the Term.

As reflected in the table below, a Service Level Agreement (“SLA”) for response times for Incident Response services is included for each subscription level. The SLA is for remote responses, does not apply to on-site services, and is not applicable to services other than Incident Response services as described in the Appendix.

Service Tier Level	Annual Maximum Consulting Hours	SKU	Incident Response SLA
Level 1	124 hours	PAN-CES-EOD-LVL1	24 hours remote
Level 2	274 hours	PAN-CES-EODLVL2	12 hours remote
Level 3	449 hours	PAN-CES-EOD-LVL3	8 hours remote
Level 4	500 hours	PAN-CES-EOD-LVL4	4 hours remote

6. Assumptions

In order for Palo Alto Networks to provide the EOD Services in Appendix A, Customer will provide written consent from the legal owner or other applicable legal authorization to Palo Alto Networks prior to commencement, if Customer is not the owner of the computer system provided for assessment(s); ensure that Palo Alto Networks personnel may access and use Customer’s and third-party licensors’ proprietary materials and data, as necessary, for Palo Alto Networks to perform the EOD Services; and, where installation and use of any software is required, Customer will provide approval for and facilitate the installation and maintenance thereof. Customer warrants and represents that it has the right and authority to grant such access and use to Palo Alto Networks and hereby grants Palo Alto Networks the rights to use and access such proprietary materials as needed for Palo Alto Networks to perform the EOD Services.

7. Term

The term of an EOD subscription is twelve (12) months (“Term”) and shall commence upon Palo Alto Networks’ receipt of a purchase order. Any unused Services or service hours will expire at the end of the Term and are non-transferable and non-refundable.

Appendix A:

Unit 42 Public Sector Expertise on Demand Subscription Services List

Services Type	Description
<p>Incident Response</p>	<ul style="list-style-type: none"> ● Incident Response <ul style="list-style-type: none"> ○ Investigate and recover from security incidents and data breaches: <ul style="list-style-type: none"> ■ Contain and eradicate the threat ■ Determine the initial point of access ■ Determine the extent of unauthorized activity ■ Determine what, if any, data was accessed or stolen ○ Malware analysis and reverse engineering ● Ransomware Investigation <ul style="list-style-type: none"> ○ Engage the threat actor on Customer's behalf ○ Seek proof that the attacker can decrypt the data ○ Refer Customer to service providers of payment services to acquire encryption keys for data recovery ○ Reverse engineer the attacker-provided decryption utility to ensure no malicious code exists ○ Provide tutorial to the Customer's team to demonstrate how to decrypt files ○ Provide remote troubleshooting support ● Business Email Compromise <ul style="list-style-type: none"> ○ Contain the incident and recommend additional safeguards; Investigate and determine root cause, window of compromise, attacker activity, and review data accessed to quantify sensitive information. ● Web Compromise <ul style="list-style-type: none"> ○ Contain threat and implement safeguards, analyze logs, review code, quantify exposure or loss of sensitive information, and recommend design hardening countermeasures. ● Cloud Breach Response <ul style="list-style-type: none"> ○ Identify initial attack vector and extent of unauthorized access and exfiltration, contain incident, identify scope of systems for remediation and recommend/implement additional safeguards and ongoing checks. ● PCI Investigation <ul style="list-style-type: none"> ○ Contain the incident and implement safeguards, navigate the PFI process, respond to alleged violations, identify the attack vector and window of compromise, quantify the number of exposed cards.

	<ul style="list-style-type: none"> ● Malware Analysis <ul style="list-style-type: none"> ○ Conduct analysis on samples using open source intel., sandboxing, reverse engineering, and deliver a detailed report focused on the behavior and functionality of the malware. ● Data Mining <ul style="list-style-type: none"> ○ Identify data at risk using industry standard tools to index, search for, and produce data for review and to identify PII and PHI affected after a data breach.
Digital Forensics	<ul style="list-style-type: none"> ● Digital Investigations, including matters related to insider threats, departed employees, and intellectual property theft. ● Perform forensic analysis of digital media, including desktop/laptop computers, servers, mobile phones/tablets, and/or log data to meet specific objectives, including identifying data access, movement, exfiltration and/or destruction. ● Hardware forensics to determine the functionality of a device, or extract data from IoT devices, new technologies, or attacker-made hardware ● Structured Data Investigations <ul style="list-style-type: none"> ○ Advise on the collection and lead the analysis of SQL and NoSQL database environments, including but not limited to the review of schemas, tables, procedures, and logs collected from impacted database systems, to assess threat actor activity and data exposure risk.
Testing & Assessment Services	<ul style="list-style-type: none"> ● Breach Readiness Review (BRR) <ul style="list-style-type: none"> ○ Targeted cybersecurity risk assessment focused on detective controls, people, processes, and technologies necessary to effectively respond to cyber threats. ○ Includes remediation recommendations, control enhancements, and a strategic roadmap to achieve a target state of breach readiness. ● Incident Response Program Development <ul style="list-style-type: none"> ○ Facilitate the development of an incident response program to assist in establishing or enhancing current incident response plan, policies, procedures, and playbooks. ● Penetration Tests - Purple and Red Team Exercises <ul style="list-style-type: none"> ○ Simulates a real-world cyber-attack to assess the strength of countermeasures and identify hidden security vulnerabilities.

	<ul style="list-style-type: none"> ○ Define a scope, rules of engagement, and establish goals, and then identify attack paths and exploit chains a threat actor would likely leverage to gain access to sensitive data or critical business applications.
	<ul style="list-style-type: none"> ● Vulnerability Assessment <ul style="list-style-type: none"> ○ Internal and/or external technical assessment designed to yield as many vulnerabilities as possible in environment, along with the severity and recommended remediation priority.
	<ul style="list-style-type: none"> ● Web Application Assessment <ul style="list-style-type: none"> ○ Evaluate web applications for vulnerabilities, including flaws in development, configuration, deployment, upgrade process, API integrations, maintenance or third-party add-ons.
	<ul style="list-style-type: none"> ● Cloud/SaaS Security Assessment <ul style="list-style-type: none"> ○ Perform a targeted assessment and deep dive review of the security configuration specific to critical business services, including Office365, Microsoft Azure, G Suite, or Google Cloud Platform. ○ Assess Customer's current configurations against multiple hardening standards and industry best practices. ○ Following the assessment, Palo Alto Networks can supervise the implementation of recommended enhancements in an advisory capacity.
	<ul style="list-style-type: none"> ● Tabletop Simulation <ul style="list-style-type: none"> ○ Simulate the response to a severe data security incident with key stakeholders. ○ We build customized scenarios based on Customer's industry-specific threats, and real world breaches the Palo Alto Networks team has responded to.
	<ul style="list-style-type: none"> ● Mobile Application Assessments <ul style="list-style-type: none"> ○ Test and improve the security of mobile applications. Enumerate the attack surface, looking for vulnerabilities, misconfigurations, or logic flaws that lead to likely paths of compromise and/or the exfiltration of data.
	<ul style="list-style-type: none"> ● Email Phishing Exercises <ul style="list-style-type: none"> ○ Test and improve Customer's employees' cybersecurity awareness and reduce susceptibility to phishing attacks.

	<ul style="list-style-type: none"> ● Compromise Assessment / Threat Hunting <ul style="list-style-type: none"> ○ Review Customer's networks and endpoint behaviors to determine whether there is evidence of unauthorized access or activity.
	<ul style="list-style-type: none"> ● Email Security Assessment <ul style="list-style-type: none"> ○ Conduct a comprehensive review of the security configuration of the Customer's email environment that includes the review of account management, email forwarding rules, inbox policies, authentication controls, etc.
Strategic Advisory Services	<ul style="list-style-type: none"> ● Virtual Chief Information Security Officer (vCISO) <ul style="list-style-type: none"> ○ A Palo Alto Networks vCISO assists with developing and implementing a cybersecurity strategy, identifying risk, and providing recommendations for risk reduction measures. ○ A vCISO can answer board of directors' or senior management's questions about benchmarks and security program's maturity, breach readiness, effectiveness, and adequacy, etc.
	<ul style="list-style-type: none"> ● Cyber Risk Strategy and Mitigation Roadmaps <ul style="list-style-type: none"> ○ Develop customized strategic plans that lay out a path, timeline, and budget to achieve an organization's cyber resilience goals.
	<ul style="list-style-type: none"> ● BoD Security Strategy Review <ul style="list-style-type: none"> ○ Assessment and review to identify cyber risk, create a current state profile, and build a clear security strategy to share with your executives and Board.
	<ul style="list-style-type: none"> ● Cyber Program, Policy & Standards Development Maturation <ul style="list-style-type: none"> ○ Develop or improve cybersecurity policies and standards. Taking into consideration industry-specific standards, customer objectives, and future goals.
	<ul style="list-style-type: none"> ● SOC Assessment <ul style="list-style-type: none"> ○ Design and advise on build of a next gen security operations center and/or infosec program based on best practices.
	<ul style="list-style-type: none"> ● Discrete Cyber Project Implementation <ul style="list-style-type: none"> ○ Expert assistance with the architecture, overseeing implementation, and tuning of a critical cybersecurity project.

	<ul style="list-style-type: none"> ○ Strategic and tactical services, e.g., advise on hardening critical business applications, enterprise email, and next-gen detective controls.
	<ul style="list-style-type: none"> ● Post breach strategic recovery and remediation advisory services <ul style="list-style-type: none"> ○ Strategic remediation guidance and prioritization to avoid further spread of any persistence related to Incident. ○ Assessment of state of security controls, systems, managed services providers, team design and procedures intended to identify and prevent the specific Incident. ○ Based on assessment, develop and deliver a strategic remediation plan including, short, medium and long-term prioritized objectives to address security weaknesses exposed by a specific incident and reduce risk of any ongoing or recurrence of an incident.
Governance, Risk, & Compliance Services	<ul style="list-style-type: none"> ● CIS V8 Assessment <ul style="list-style-type: none"> ○ CIS V8 Report & Tailored Recommendations. ○ 12 – 24 Month Implementation Roadmap,
	<ul style="list-style-type: none"> ● NIST Cybersecurity Framework (NIST CSF) Assessment <ul style="list-style-type: none"> ○ NIST CSF Findings Workbook. ○ Thematic Findings Executive Report. ○ 12 – 24 Month Implementation Roadmap.
	<ul style="list-style-type: none"> ● Regulated and Contract-based Cybersecurity Assessments (e.g. CCPA, NYDFS, HIPAA, FINRA, PCI DSS, C2M2, GDPR) <ul style="list-style-type: none"> ○ Perform an assessment mapping to the control requirements of contractual, state, and/or regulatory frameworks. ○ Assess control requirements, find and remediate gaps, and demonstrate compliance.
	<ul style="list-style-type: none"> ● M&A Cyber Due Diligence Reviews <ul style="list-style-type: none"> ○ Targeted assessment in connection with pending merger/acquisition activity. Focused and tactical, this assessment is designed to provide transparency to deal participants. ○ Identify potential red flags, highlight hidden cybersecurity risks, and obtain an independent assessment of overall information security program maturity.

	<ul style="list-style-type: none">● Third Party Vendor Cybersecurity Risk Assessment<ul style="list-style-type: none">○ Evaluation of third-party vendor-based cybersecurity risk.○ Evaluate and improve information security-related contract requirements.○ Develop and/or enhance security operations related to third party vendor compliance with security requirements.
	<ul style="list-style-type: none">● Cybersecurity Training and Awareness<ul style="list-style-type: none">○ Remote or on-site training modules for groups ranging from 5 to 5,000+.○ Development of employee cyber training programs.

Squadra Solutions
 Squadra Solutions, LLC
 1750 Tysons Boulevard
 Suite #1532
 McLean VA 22102
 United States

Quote 2022-QO-2014



CUSTOMER: County of Albany, NY
 Perry Blanchard
Perry.blanchard@albanycounty.com

SALES REP: Jeff Cohen
jcohen@squadrasolutions.com

Tax ID# 81-0712443
 DUNS# 080090995
 Cage: 7JDW1
 GSA: GS-35F-0511T
 NYS Contract: PM 21270

QUOTE EXPIRES 04/24/2022	DATE 03/25/2022	TOTAL \$50,250.00
------------------------------------	---------------------------	-----------------------------

QUOTE OWNER: Perry Blanchard

TITLE: Palo Alto

MEMO: Palo Alto Code 42 LVL2

ACTIVITY	QTY	LIST PRICE	CUSTOMER UNIT PRICE	CUSTOMER EXTENDED
Maintenance/Support				
PAN-CES-EOD-LVL2 Unit 42 Public Sector Expertise on Demand Subscription, Level 2, with 12 hours remote response time	134	\$375.00	\$375.00	\$50,250.00

Payment Terms: Net 30
 NYS OGS Contract and Appendix A terms apply

Hardware/Software	0.00
Support/Maintenance	50,250.00
Professional Services	0.00
Other Services	0.00

TOTAL **\$50,250.00**

THANK YOU.

Accepted By: _____

Accepted Date: _____

RESOLUTION NO. 41

AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES REGARDING THE FY2019 CYBER SECURITY GRANT FOR THE ALBANY COUNTY DIVISION OF INFORMATION SERVICES

Introduced: 2/8/21

By Public Safety Committee:

WHEREAS, The County Executive has requested authorization to submit a grant application to the New York State Division of Homeland Security and Emergency Services regarding the FY2019 Cyber Security Grant for the Albany County Division of Information Services in an amount not to exceed \$43,673, and

WHEREAS, The County Executive indicated that, if granted, funding will be allocated to the purchase of enhanced cyber security software and support for Albany County which is necessary due to increased remote working, now, therefore be it

RESOLVED, By the Albany County Legislature that the County Executive is authorized to submit a grant application to the New York State Division of Homeland Security and Emergency Services regarding the FY2019 Cyber Security Grant in the amount not to exceed \$43,673 for the purchase of enhanced cyber security software and support, and, be it further

RESOLVED, That the County Attorney is authorized to approve said application as to form and content, and, be it further

RESOLVED, That the Clerk of the County Legislature is directed to forward certified copies of this resolution to the appropriate County Officials.



ALBANY COUNTY SHERIFF'S OFFICE
 County Court House Albany, New York 12207 (518) 487-5400
WWW.ALBANYCOUNTYSHERIFF.COM



MICHAEL S. MONTELEONE
 EXECUTIVE UNDERSHERIFF

CRAIG D. APPLE, SR.
 SHERIFF

WILLIAM M. RICE
 UNDERSHERIFF

SHAWN P. NOONAN
 CHIEF DEPUTY

LEON A. BORMANN
 CHIEF DEPUTY

May 4, 2022

Honorable Andrew C. Joyce
 Legislative Clerk's Office
 112 State Street, Room 710
 Albany, New York 12207

Dear Mr. Joyce:

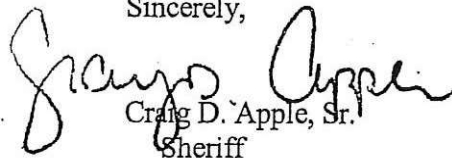
The attached correspondence is forwarded for presentation to the members of the Albany County Legislature.

Legislative approval is being requested authorizing the following personnel changes and we have attached a budget amendment.

Eliminate	Salary
Correction Officer	\$52,000.00
Clerk 1	27,952.00
Add	
Senior Investigator	\$39,976.00
Senior Investigator	39,976.00

Should there be any questions, please do not hesitate to contact me.

Sincerely,


 Craig D. Apple, Sr.
 Sheriff

- cc: Hon. Daniel McCoy, County Executive
 Hon. William Clay, Public Safety Chairman
 Hon. Wanda Willingham, Audit & Finance Committee
 Brandon Russell, Esq., Majority Counsel
 Arnis Zilgme, Esq., Minority Counsel
 Christian Barnes, Minority Conference

REQUEST FOR LEGISLATIVE ACTION

FOR COUNSEL USE ONLY	
DATE:	_____
RECEIVED:	_____
RECEIVED BY:	_____
METHOD:	HAND _____
	COURIER _____
	MAIL _____

DATE: MAY 4, 2022

DEPARTMENT: ALBANY COUNTY SHERIFF'S DEPT

CONTACT PERSON: SHERIFF CRAIG D APPLE SR

TELEPHONE: 518-447-5440

DEPT. REPRESENTATIVE ATTENDING SHERIFF CRAIG D APPLE SR

COMMITTEE MEETING:

PURPOSE OF REQUEST:

- ADOPTION OF LOCAL LAW _____
- AMENDMENT OF PRIOR LEGISLATION _____
- APPROVAL/ADOPTION OF PLAN/PROCEDURE _____
- BOND APPROVAL _____
- BUDGET AMENDMENT(SEE BELOW) X
- CONTRACT AUTHORIZATION (SEE BELOW) _____
- ENVIRONMENTAL IMPACT _____
- HOME RULE REQUEST _____
- PROPERTY CONVEYANCE _____
- OTHER:(STATE BRIEFLY IF NOT LISTED ABOVE) X

THE SHERIFF'S OFFICE IS REQUESTING THE FOLLOWING PERSONNEL ADJUSTMENT IN DEPT. 3150

THIS MOVE WILL BE BUDGET NEUTRAL IN OUR 2022 BUDGET

SEE ATTACHED SPREADSHEETS

CONCERNING BUDGET AMENDMENTS

STATE THE FOLLOWING

INCREASE ACCOUNT/LINE NO. SEE ATTACHED

SOURCE OF FUNDS: _____

TITLE CHANGE: _____

CONCERNING CONTRACT AUTHORIZATION,

STATE THE FOLLOWING:

TYPE OF CONTRACT

- CHANGE ORDER/CONTRACT AMENDMENT _____
- PURCHASE (EQUIPMENT/ SUPPLIES) _____
- LEASE (EQUIPMENT/SUPPLIES) _____
- REQUIREMENTS _____
- PROFESSIONAL SERVICES _____
- EDUCATIONAL/TRAINING _____
- GRANT: NEW _____
- RENEWAL _____
- SUBMISSION DEADLINE DATE _____

SETTLEMENT OF A CLAIM _____

RELEASE OF LIABILITY _____

OTHER: (STATE BRIEFLY) _____

CONCERNING CONTRACT AUTHORIZATION (CONT'D)

STATE THE FOLLOWING:

CONTRACT TERMS/CONDITIONS: _____ PARTY (NAME/ADDRESS):

AMOUNT/RATE SCHEDULE/FEE:

TERM: _____

SCOPE OF SERVICES: _____

CONTRACT FUNDING:

ANTICIPATED IN CURRENT BUDGET: YES _____ NO _____
FUNDING SOURCE: _____
COUNTY BUDGET ACCOUNTS: _____
REVENUE: _____
APPROPRIATION: _____
BOND (RES. NO. & DATE OF ADOPTION) _____

CONCERNING ALL REQUESTS:

MANDATED PROGRAM/SERVICE: YES _____ NO X
IF MANDATED CITE: AUTHORITY _____
ANTICIPATED IN CURRENT ADOPTED BUDGET: YES _____ NO X
IF YES, INDICATE REVENUE APPROPRIATION ACCOUNTS: _____

FISCAL IMPACT - FUNDING: _____ (DOLLARS OR PERCENTAGES)

FEDERAL _____
STATE _____
COUNTY _____ 100%
TERM/LENGTH OF FUNDING _____

PREVIOUS REQUESTS FOR IDENTICAL OR SIMILAR ACTION:

RESOLUTION/LAW NUMBER: _____
DATE OF ADOPTION: _____

JUSTIFICATION: _____ (STATE BRIEFLY WHY LEGISLATIVE ACTION IS REQUESTED)

PER SPREAD SHEET

THIS WILL BE BUDGET NEUTRAL IN OUR 2022

BACK-UP MATERIAL SUBMITTED _____ (I.E. APPLICATION/APPROVAL NOTICES FROM FUNDING SOURCE,
BID TABULATION SHEET, CIVIL SERVICE APPROVAL NOTICE, PROGRAM ANNOUNCEMENT, CONTRACTS
AND/OR ANY MATERIALS WHICH EXPLAIN OR SUPPORT THE REQUEST FOR LEGISLATIVE ACTION.)

SUBMITTED BY: CRAIG D APPLE SR
TITLE: SHERIFF

2022 BUDGET AMENDMENT (3150)									
RESOLUTION NO. BTGH	ACCOUNT NO.	RESOLUTION DESCRIPTION	INCREASE	DECREASE	ANNUAL SALARY	POSITION CONTROL NUMBER			
		APPROPRIATIONS							
A 3150	1 4131	SHERIFF'S SENIOR INVESTIGATOR	39,976.00		79,952.00	NEED TO CREATE POSITION			
A 3150	1 4131	SHERIFF'S SENIOR INVESTIGATOR	39,976.00		79,952.00	NEED TO CREATE POSITION			
		TOTAL APPROPRIATIONS	79,952.00		159,904.00				
		APPROPRIATIONS							
		RESOLUTION DESCRIPTION							
A 3150	1 4115	CORRECTIONS OFFICER		52,000.00	65,697.00	390205 ELIMINATE POSITION			
A 3150	1 6202	CLERK 1		27,952.00	42,036.00	390398 ELIMINATE POSITION			
		GRAND TOTALS	0.00	79,952.00	107,733.00				

NOTE: THE ANNUAL SALARIES HAVE BEEN PROTECTED FOR 26 WEEKS



ALBANY COUNTY SHERIFF'S OFFICE

County Court House Albany, New York 12207 (518) 487-5400
WWW.ALBANYCOUNTYSHERIFF.COM



MICHAEL S. MONTELEONE
EXECUTIVE UNDERSHERIFF

CRAIG D. APPLE, SR.
SHERIFF

WILLIAM M. RICE
UNDERSHERIFF

SHAWN P. NOONAN
CHIEF DEPUTY

LEON A. BORMANN
CHIEF DEPUTY

May 3, 2022

Honorable Andrew Joyce
Legislative Clerk's Office
112 State Street, Room 710
Albany, New York 12207

Dear Mr. Joyce:

The attached correspondence is forwarded for presentation to the Albany County Legislature.

Legislative approval is required in order to allow Albany County to apply for and accept the awarded amount from the NYS, Division of Homeland Security & Emergency services, 2022 Statewide Interoperable Communications Grant – Targeted Program.

The grant application for the Albany County Sheriff's Office is a maximum of \$6,000,000.00, with no match. These grant funds, if awarded, will be utilized for the implementation of regional connectivity via radio system core, connecting Albany, Schenectady and Rensselaer Counties. Schenectady and Rensselaer Counties will also be seeking like funds as their part of the project.

The performance period for the 2022 SICG-Targeted Program is four (4) years from the execution of the contract.

There are no matching funds required.

Should there be any questions, do not hesitate to call.

Sincerely,

Craig D. Apple, Sr.
Sheriff

Att.

Cc: Hon. Daniel P. McCoy, County Executive
Hon. William Clay, Public Safety Chairman
Hon. Wanda Willingham, Audit & Finance
Brandon Russell, Esq., Majority Counsel
Arnis Zilgme, Esq., Minority Counsel
Christian Barnes, Minority Counsel

REQUEST FOR LEGISLATIVE ACTION

FOR COUNSEL USE ONLY	
DATE:	_____
RECEIVED:	_____
RECEIVED BY:	_____
METHOD:	<u>HAND</u> _____
	<u>COURIER</u> _____
	<u>MAIL</u> _____

DATE : MAY 3, 2022

DEPARTMENT: ALBANY COUNTY SHERIFF'S DEPT

CONTACT PERSON: CRAIG D APPLE SR
TELEPHONE: 487-5440

DEPT. REPRESENTATIVE ATTENDING COMMITTEE MEETING: SHERIFF CRAIG D APPLE SR

PURPOSE OF REQUEST:

- ADOPTION OF LOCAL LAW _____
- AMENDMENT OF PRIOR LEGISLATION _____
- APPROVAL/ADOPTION OF PLAN/PROCEDURE _____
- BOND APPROVAL _____
- BUDGET AMENDMENT(SEE BELOW) _____
- CONTRACT AUTHORIZATION (SEE BELOW) _____
- ENVIRONMENTAL IMPACT _____
- HOME RULE REQUEST _____
- PROPERTY CONVEYANCE _____
- OTHER:(STATE BRIEFLY IF NOT LISTED ABOVE) X

TO APPLY AND ACCEPT THE AWARDED AMOUNT FOR THE 2022 STATEWIDE INTEROPERABLE COMMUNICATIONS GRANT - TARGETD PROGRAM, FROM NYS DIVISION OF HOMELAND SECURITY. THIS GRANT COULD BE WORTH UP TO \$6,000,000

CONCERNING BUDGET AMENDMENTS

STATE THE FOLLOWING

INCREASE ACCOUNT/LINE NO. _____
SOURCE OF FUNDS: _____
TITLE CHANGE: _____

CONCERNING CONTRACT AUTHORIZATION, _____

STATE THE FOLLOWING:

TYPE OF CONTRACT

- CHANGE ORDER/CONTRACT AMENDMENT _____
- PURCHASE (EQUIPMENT/ SUPPLIES) _____
- LEASE (EQUIPMENT/SUPPLIES) _____
- REQUIREMENTS _____
- PROFESSIONAL SERVICES _____
- EDUCATIONAL/TRAINING _____

GRANT: NEW X
RENEWAL _____
SUBMISSION DEADLINE DATE 5/11/2022

SETTLEMENT OF A CLAIM _____
RELEASE OF LIABILITY _____
OTHER: (STATE BRIEFLY) _____

CONCERNING CONTRACT AUTHORIZATION (CONT'D)

STATE THE FOLLOWING:

CONTRACT TERMS/CONDITIONS: _____ **PARTY (NAME/ADDRESS):**
JEROME HAUER, COMMISSIONER
DIVISION OF HOMELAND SECURITY & EMERGENCY SERVICES
1220 WASHINGTON AVENUE, BLDG 7A, SUITE 710, ALBANY 12242
AMOUNT/RATE SCHEDULE/FEE:
UP TO \$ 6,000,000 (WITH NO MATCH)
TERM: 4 YEARS FROM THE EXECUTION OF THE CONTRACT
SCOPE OF SERVICES:
THESE GRANT FUNDS WILL BE USED FOR THE IMPLEMENTATION OF
REGIONAL CONNECTIVITY VIA RADIO SYSTEM CORE TO OTHER COUNTIES

CONTRACT FUNDING:
ANTICIPATED IN CURRENT BUDGET: YES _____ NO X
FUNDING SOURCE: NYS DEPT. OF HOMELAND SECURITY
COUNTY BUDGET ACCOUNTS:
REVENUE: _____
APPROPRIATION: _____
BOND(RES. NO. & DATE OF ADOPTION) _____

CONCERNING ALL REQUESTS:
MANDATED PROGRAM/SERVICE: _____ YES _____ NO X
IF MANDATED CITE: AUTHORITY _____
ANTICIPATED IN CURRENT ADOPTED BUDGET: YES _____ NO X
IF YES, INDICATE REVENUE APPROPRIATION ACCOUNTS: _____

FISCAL IMPACT - FUNDING: _____ (DOLLARS OR PERCENTAGES)
FEDERAL _____
STATE 100%
COUNTY _____
TERM/LENGTH OF FUNDING _____

PREVIOUS REQUESTS FOR IDENTICAL OR SIMILAR ACTION:
RESOLUTION/LAW NUMBER: _____
DATE OF ADOPTION: _____

JUSTIFICATION: (STATE BRIEFLY WHY LEGISLATIVE ACTION IS REQUESTED)
THIS GRANT WILL BE UTILIZED TO HELP WITH REGIONAL CONNECTIVITY TO
SURROUNDING COUNTIES VIA RADIO SYSTEM CORE.
THERE IS NO MATCH WITH THIS GRANT

BACK-UP MATERIAL SUBMITTED _____ (I.E. APPLICATION/APPROVAL NOTICES FROM FUNDING SOURCE,
BID TABULATION SHEET, CIVIL SERVICE APPROVAL NOTICE, PROGRAM ANNOUNCEMENT, CONTRACTS
AND/OR ANY MATERIALS WHICH EXPLAIN OR SUPPORT THE REQUEST FOR LEGISLATIVE ACTION.)

SUBMITTED BY: CRAIG D APPLE SR
TITLE: SHERIFF

Miller, Doug

From: Info, Grant (DHSES) <Grant.Info@dhses.ny.gov>
Sent: Wednesday, April 6, 2022 1:50 PM
To: Info, Grant (DHSES)
Subject: FY2022 Statewide Interoperable Communications Targeted Grant Program – Request for Applications Released

**NYS Division of Homeland Security and Emergency Services
Office of Interoperable and Emergency Communications
Announces the
2022 Statewide Interoperable Communications Targeted Grant
Program
(2022 SICG-Targeted)**

The NYS Division of Homeland Security and Emergency Services, Office of Interoperable and Emergency Communications, is pleased to announce the Statewide Interoperable Communications Targeted Grant program. Funding for the 2022 SICG-Targeted Program is distributed by an analysis of data related to the implementation of National Interoperability Channels in New York. The SICG-Targeted Program focuses on closing gaps in National Interoperability channels implementation and enhancing regional connectivity, ensuring that county communication systems are capable to support multijurisdictional response. The SICG-Targeted Program provides a way forward for providing a safer environment for public safety personnel, integration with other emergent technologies, and the ability to establish technology and performance standards.

Purpose: The overall objective of the SICG-Targeted Program is to close gaps in the interoperability infrastructure, regional communications deficiencies, and implementation of National Interoperability channels.

Eligible Applicants: County governments, requesting funding for the benefit of the county as a single entity. Additional eligibility criteria are listed in the 2022 SICG-Targeted Request for Applications.

Source of Funds: This grant program is supported by the Statewide Public Safety Communications Account.

Total Funding Available for 2022 SICG-Targeted: \$62,427,798

Schedule of Events:

- **Submission of Written Questions** April 27, 2022
- **Request for Applications Updates (if any)** May 3, 2022
- **Applications Due** May 11, 2022 by 5:00 P.M.

All Documents for this RFA may be found on the OIEC Grants Home
Page: <https://www.dhses.ny.gov/statewide-interoperable-communications-grant-targeted-sicg>

Frequently Asked Questions concerning the RFA are also located on the OIEC Grants Home Page: <https://www.dhSES.ny.gov/statewide-interoperable-communications-grant-targeted-sicg> under "FAQ" tab.

Contact Information:

- Grant Administrator
Office of Interoperable and Emergency Communications
NYS Division of Homeland Security and Emergency Services
1220 Washington Avenue, Building 7A, Suite 710
Albany, NY 12242

E-mail: Grant.Info@dhSES.ny.gov



ALBANY COUNTY SHERIFF'S OFFICE

County Court House Albany, New York 12207 (518) 487-5400
WWW.ALBANYCOUNTYSHERIFF.COM



MICHAEL S. MONTELEONE
EXECUTIVE UNDERSHERIFF

CRAIG D. APPLE, SR.
SHERIFF

WILLIAM M. RICE
UNDERSHERIFF

SHAWN P. NOONAN
CHIEF DEPUTY

LEON A. BORMANN
CHIEF DEPUTY

May 4, 2022

Honorable Andrew Joyce
Legislative Clerk's Office
112 State Street, Room 710
Albany, New York 12207

Dear Mr. Joyce:

The attached correspondence is forwarded for presentation to the Albany County Legislature.

Legislative approval is required in order to allow Albany County Sheriff's Office to apply for and accept \$40,000.00 in grant funding from the Research Foundation for Mental Hygiene.

The term of this contract will be April 4, 2022 through December 31, 2022.

As a law enforcement agency, we recognize the need to address the stressful challenges that uniformed officer's face on a daily basis and the impact these challenges have on the officer's mental health and well-being. By utilizing these funds, we will invest in the wellness and resiliency of our staff while offering them education and support.

Should there be any questions, do not hesitate to call.

Sincerely,

Craig D. Apple, Sr.
Sheriff

Att.

Cc: Hon. Daniel P. McCoy, County Executive
Hon. William Clay, Public Safety Chairman
Hon. Wanda Willingham, Audit & Finance
Brandon Russell, Esq., Majority Counsel
Arnis Zilgme, Esq., Minority Counsel
Christian Barnes, Minority Counsel

REQUEST FOR LEGISLATIVE ACTION

FOR COUNSEL USE ONLY	
DATE:	_____
RECEIVED:	_____
RECEIVED BY:	_____
METHOD:	<u>HAND</u> _____
	<u>COURIER</u> _____
	<u>MAIL</u> _____

DATE: MAY 4, 2022

DEPARTMENT: ALBANY COUNTY SHERIFF'S DEPT

CONTACT PERSON: CRAIG D APPLE SR

TELEPHONE: 487-5440

DEPT. REPRESENTATIVE ATTENDING

COMMITTEE MEETING:

SHERIFF CRAIG D APPLE SR

PURPOSE OF REQUEST:

- ADOPTION OF LOCAL LAW _____
- AMENDMENT OF PRIOR LEGISLATION _____
- APPROVAL/ADOPTION OF PLAN/PROCEDURE _____
- BOND APPROVAL _____
- BUDGET AMENDMENT(SEE BELOW) _____
- CONTRACT AUTHORIZATION (SEE BELOW) _____
- ENVIRONMENTAL IMPACT _____
- HOME RULE REQUEST _____
- PROPERTY CONVEYANCE _____
- OTHER:(STATE BRIEFLY,IF NOT LISTED ABOVE) X

TO APPLY AND ACCEPT A GRANT FOR \$40,000 FROM THE RESEARCH FOUNDATION FOR MENTAL HYGIENE

CONCERNING BUDGET AMENDMENTS

STATE THE FOLLOWING

INCREASE ACCOUNT/LINE NO. _____

SOURCE OF FUNDS: _____

TITLE CHANGE: _____

CONCERNING CONTRACT AUTHORIZATION, STATE THE FOLLOWING:

TYPE OF CONTRACT

- CHANGE ORDER/CONTRACT AMENDMENT _____
- PURCHASE (EQUIPMENT/ SUPPLIES) _____
- LEASE (EQUIPMENT/SUPPLIES) _____
- REQUIREMENTS _____
- PROFESSIONAL SERVICES _____
- EDUCATIONAL/TRAINING _____
- GRANT: NEW X
- RENEWAL _____
- SUBMISSION DEADLINE DATE _____

SETTLEMENT OF A CLAIM _____

RELEASE OF LIABILITY _____

OTHER: (STATE BRIEFLY) _____

CONCERNING CONTRACT AUTHORIZATION (CONT'D)

STATE THE FOLLOWING:

CONTRACT TERMS/CONDITIONS: _____ **PARTY (NAME/ADDRESS):** _____

RESEARCH FOUNDATION FOR MENTAL HYGIENE

150 BROADWAY

MENANDS, NY 12204

AMOUNT/RATE SCHEDULE/FEE:

\$40,000 (WITH NO MATCH)

TERM: _____ **4/4/2022 THRU 12/31/2022**

SCOPE OF SERVICES: _____

THESE FUNDS WILL BE USED TO OFFER EDUCATION AND SUPPORT TO

OUR STAFF IN THE AREA OF MENTAL HEALTH WELL-BEING

CONTRACT FUNDING:

ANTICIPATED IN CURRENT BUDGET: YES _____ NO X

FUNDING SOURCE: **RESEARCH FOUNDATION FOR MENTAL HYGIENE**

COUNTY BUDGET ACCOUNTS:

REVENUE: _____

APPROPRIATION: _____

BOND(RES. NO. & DATE OF ADOPTION) _____

CONCERNING ALL REQUESTS:

MANDATED PROGRAM/SERVICE: YES _____ NO X

IF MANDATED CITE: AUTHORITY _____

ANTICIPATED IN CURRENT ADOPTED BUDGET: YES _____ NO X

IF YES, INDICATE REVENUE APPROPRIATION ACCOUNTS: _____

FISCAL IMPACT - FUNDING: _____ **(DOLLARS OR PERCENTAGES)**

FEDERAL _____

STATE 100%

COUNTY _____

TERM/LENGTH OF FUNDING _____

PREVIOUS REQUESTS FOR IDENTICAL OR SIMILAR ACTION:

RESOLUTION/LAW NUMBER: _____

DATE OF ADOPTION: _____

JUSTIFICATION: _____ **(STATE BRIEFLY WHY LEGISLATIVE ACTION IS REQUESTED)**

THIS WILL BE UTILIZED TO OFFER OUR UNIFORMED OFFICERS EDUCATION AND

SUPPORT IN THE AREA OF MENTAL HEALTH WELL-BEING AS THEY COPE WITH STRESSFUL

SITUATIONS ON A DAILY BASIS.

BACK-UP MATERIAL SUBMITTED _____ **(I.E. APPLICATION/APPROVAL NOTICES FROM FUNDING SOURCE, BID TABULATION SHEET, CIVIL SERVICE APPROVAL NOTICE, PROGRAM ANNOUNCEMENT, CONTRACTS AND/OR ANY MATERIALS WHICH EXPLAIN OR SUPPORT THE REQUEST FOR LEGISLATIVE ACTION.)**

SUBMITTED BY: **CRAIG D. APPLE SR**

TITLE: **SHERIFF**

For RFMH Use Only:	
<input checked="" type="checkbox"/> New P.O. # <u>156952</u>	<input type="checkbox"/> Change P.O. # _____
Total to be encumbered: <u>\$40,000</u>	
Category Breakdown:	
Consulting: \$ <u>40,000</u>	_____
Travel: \$ <u>n/a</u>	_____
Project Org: <u>550 OMH</u>	_____
P/T/A: <u>1017636/10/26808</u>	_____
Period of Performance <u>04/04/2022</u> to <u>12/31/2022</u>	
Jay Carruthers	

**Independent Contractor/Consulting Agreement
Resulting from New York State Contracts**

**RESEARCH FOUNDATION FOR MENTAL HYGIENE, INC.
AND
INDEPENDENT CONTRACTOR**

MADE by and between the RESEARCH FOUNDATION FOR MENTAL HYGIENE, INC., a nonprofit corporation organized and existing under the laws of the State of New York, with its principal offices located at Riverview Center, 150 Broadway, Suite 301, Menands, New York 12204, hereinafter referred to as the "FOUNDATION," and Albany County Sheriff's Office, having a place of business at 16 Eagle Street, Room 79 Albany, NY 12207, EIN/DUNS (if applicable): _____ hereinafter referred to as "INDEPENDENT CONTRACTOR."

WITNESSETH:

WHEREAS, the FOUNDATION has been awarded a certain grant from the State of New York, specifically New York State Office of Mental Health ("Sponsor") to carry out a project entitled "CARES UP CY22"; Sponsor ID Number: C020687 (hereinafter the "PROJECT"); and

WHEREAS, the FOUNDATION desires the INDEPENDENT CONTRACTOR to perform certain services for the FOUNDATION in connection with the PROJECT; and

WHEREAS, INDEPENDENT CONTRACTOR has represented to the FOUNDATION that INDEPENDENT CONTRACTOR is competent, willing and able to perform such services for the FOUNDATION.

NOW, THEREFORE in consideration of the premises and the mutual covenants and agreements contained herein it is mutually agreed by and between the respective parties as follows:

1. Scope of Work

INDEPENDENT CONTRACTOR agrees to perform, as an independent Contractor, and not as an agent or employee of the FOUNDATION, all of the services set forth in Exhibit A

appended hereto and made a part hereof to the satisfaction of the FOUNDATION's Principal Investigator, Jay Carruthers.

2. **Compensation**

In full and complete consideration of INDEPENDENT CONTRACTOR's performance hereunder, the FOUNDATION agrees to compensate INDEPENDENT CONTRACTOR \$ 40,000 Dollars. The payments should be in accordance with Exhibit B.

3. **Term and Termination**

Unless sooner terminated as provided herein, this Agreement shall continue in full force and effect from 04/04/2022 through 12/31/2022. A final invoice must be submitted within sixty (60) days of the end of this Agreement. It is understood and agreed that the FOUNDATION may terminate this Agreement upon written notice by registered mail addressed to INDEPENDENT CONTRACTOR at the address indicated herein, or such other address as INDEPENDENT CONTRACTOR may designate in writing, whenever the FOUNDATION determines, in its discretion, that such termination would be in the best interests of the FOUNDATION. FOUNDATION may terminate this Agreement immediately if the Grant between Sponsor and FOUNDATION is terminated.

Upon notice of termination, INDEPENDENT CONTRACTOR shall immediately terminate work in progress and turn over to FOUNDATION all products, work in progress, reports and other data and information accumulated during the performance of services under this Agreement.

4. **Rights in Work Product**

INDEPENDENT CONTRACTOR agrees that material produced by INDEPENDENT CONTRACTOR hereunder shall be considered "work for hire" which shall be owned by FOUNDATION. INDEPENDENT CONTRACTOR agrees that INDEPENDENT CONTRACTOR shall not claim or assert any proprietary interest in any of the data or materials required to be produced or delivered by INDEPENDENT CONTRACTOR in the performance of INDEPENDENT CONTRACTOR'S obligation hereunder, and hereby assigns all rights, title and interest in said data and materials to FOUNDATION. INDEPENDENT CONTRACTOR warrants any material produced by INDEPENDENT CONTRACTOR hereunder shall be original except for such portion from copyrighted works as may be included with the permission of the copyright owners thereof and are marked with appropriate copyright notices, that it shall contain no libelous or unlawful statements or materials, and will not infringe upon any copyright, trademark, patent, statutory or other proprietary rights of others, and that INDEPENDENT CONTRACTOR will hold harmless the FOUNDATION from any costs, expenses and damages resulting from any breach of this warranty. INDEPENDENT CONTRACTOR further agrees not to publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to this Agreement without the prior written consent of the FOUNDATION. Notwithstanding the foregoing, INDEPENDENT CONTRACTOR will retain ownership of intellectual property included in deliverables to the extent that said intellectual property has been independently developed by INDEPENDENT

CONTRACTOR without Research Foundation financial support. With respect to such INDEPENDENT CONTRACTOR owned intellectual property, INDEPENDENT CONTRACTOR hereby grants to Research Foundation and Sponsor a royalty-free, nonexclusive license to use such intellectual property for purposes consistent with the Research Foundation's obligations under the grant or contract which funds this project.

5. **Assignment**

It is understood and agreed that the services to be rendered by INDEPENDENT CONTRACTOR are unique and that INDEPENDENT CONTRACTOR shall not assign, transfer, contract or otherwise dispose of INDEPENDENT CONTRACTOR's rights or duties hereunder, in whole or in part, to any other person, firm or corporation.

6. **Status of Parties**

The nature of the relationship which the INDEPENDENT CONTRACTOR shall have to the FOUNDATION pursuant to this Agreement shall be that of an independent contractor. In connection with its status as an independent contractor, INDEPENDENT CONTRACTOR hereby warrants that it is in compliance with all tax filing and similar requirements imposed on independent contractors, and acknowledges that it is solely responsible for paying income taxes, FICA taxes, and other taxes and assessments which arise from receipt of consulting payments under this Agreement. This Agreement shall not be construed to contain any authority either express or implied, enabling the INDEPENDENT CONTRACTOR to incur any expense or perform any act on behalf of the FOUNDATION.

7. **Entire Agreement**

This Agreement represents the entire Agreement and understanding of the parties hereto and no prior writings, conversations or representations of any nature shall be deemed to vary the provisions hereof. This Agreement may not be amended or extended in any way except by a writing duly executed by both parties hereto.

8. **Compliance with Laws and Regulations: General Obligations**

a) In the performance of the work authorized pursuant to this agreement, INDEPENDENT CONTRACTOR agrees to comply with all applicable laws and regulations, as well as policies of the Sponsor applicable to INDEPENDENT CONTRACTOR's performance hereunder, and the express terms of FOUNDATION's agreement with the Sponsor, which shall be deemed to be inserted herein, and this agreement shall be read and enforced between the parties as though all such provisions were included verbatim herein.

b) The INDEPENDENT CONTRACTOR certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency:

c) The INDEPENDENT CONTRACTOR agrees to comply with Department of Health and Human Services Regulation, 45 CFR 46, regarding confidential data and research involving human subjects.

d) The INDEPENDENT CONTRACTOR agrees to make any and all data and work products relating to the services set for in Exhibit A reasonably available for inspection and copying.

e) The INDEPENDENT CONTRACTOR agrees not to use the names of FOUNDATION, FOUNDATION Principal Investigator or New York State Office of Mental Health for any purpose without prior written approval of FOUNDATION.

9. Confidentiality

a) All of the information disclosed by the FOUNDATION and FOUNDATION's Principal Investigator to INDEPENDENT CONTRACTOR, including the any data provided by the FOUNDATION to the INDEPENDENT CONTRACTOR to be used by INDEPENDENT CONTRACTOR in the performance of the services outlined in Exhibit A, shall be considered "Confidential Information". INDEPENDENT CONTRACTOR agrees to hold in confidence all Confidential Information and agrees that it will not use any information for any purpose other than set forth in this Agreement. INDEPENDENT CONTRACTOR will take all reasonable steps to ensure its security. INDEPENDENT CONTRACTOR may disclose Confidential Information to its own employees assisting in the services under this Agreement, provided that such employees shall have agreed to be bound by the terms of this Agreement or have entered into an agreement of similar scope and obligations to protect the Confidential Information. All Confidential Information must be returned within thirty (30) days after FOUNDATION makes a written request for its return or at the conclusion of this Agreement. The INDEPENDENT CONTRACTOR shall not disclose the Confidential Information to any third party without prior written permission

b) This obligation of confidentiality does not extend to Confidential Information which:

- 1) was known to the INDEPENDENT CONTRACTOR as evidenced by written documentation;
- 2) was or becomes a matter of public information or publicly available through no fault of the INDEPENDENT CONTRACTOR as evidenced by written documentation;
- 3) is acquired from a third party entitled to disclose information to the INDEPENDENT CONTRACTOR as evidenced by written documentation; or
- 4) is developed independently by INDEPENDENT CONTRACTOR

c) Except as required by law, regulation, court order, or with prior written permission, the INDEPENDENT CONTRACTOR will not disclose Confidential Information for a period of five (5) years from the end of this Agreement.

d) INDEPENDENT CONTRACTOR shall comply with all applicable laws regarding the confidentiality of subjects' medical records and protected health information.

e) INDEPENDENT CONTRACTOR shall not use or disclose protected health information other than as permitted or required by this Agreement or as required by law.

f) In the event that identifiable health information is disclosed to the INDEPENDENT CONTRACTOR that is not provided for in this Agreement, the INDEPENDENT CONTRACTOR shall notify the FOUNDATION of such disclosure, shall hold in confidence all such information and shall destroy such information upon the request of the FOUNDATION.

10. Indemnification

INDEPENDENT CONTRACTOR will indemnify, defend and hold harmless FOUNDATION, the New York State Office of Mental Health, and their respective trustees, directors, officers, agents and employees (collectively "Indemnitees"), against all suits, claims, demands or prosecutions, (hereinafter "Claim") that may be brought or instituted, and all judgments, damages, liabilities, court costs and expenses (including attorney's fees) arising out of INDEPENDENT CONTRACTOR's negligent acts or omissions relating to its performance hereunder or its willful misconduct.

11. Insurance Requirements

INDEPENDENT CONTRACTOR shall not commence work under this Agreement until it has obtained, at its own expense, all the insurance required under this Agreement, and within the Scope of Work as provided for in Exhibit A, and such insurance has been approved by FOUNDATION.

a) Workers' Compensation and Employers' Liability Insurance as required by law.

b) Commercial General Liability Insurance with a combined personal injury, bodily injury (including death) and property damage limit of at least \$1,000,000 for each occurrence and \$3,000,000 in the aggregate.

c) Professional Liability Insurance, including Medical Malpractice and Clinician's Liability: if INDEPENDENT CONTRACTOR or any of its employees are providing professional services under this Agreement, Professional Liability in an amount not less than \$1,000,000 for each wrongful act and \$3,000,000 in the aggregate.

12. Modifications

This agreement may be changed, amended, modified or extended only by a writing duly executed by the respective parties hereto.

13. Governing Law

Regardless of the place of physical execution or performance this agreement shall be construed according to the laws of the State of New York without regard to its conflict of laws provision, and shall be deemed to have been executed in the State of New York.

14. Order of Precedence

In the event of any inconsistency between clauses 1-13 of this Agreement, and the attached Exhibit A and B, the inconsistency should be resolved by giving precedence to clauses 1-13.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement the day and year first above written.

Research Foundation for
Mental Hygiene, Inc.

Independent Contractor

By _____
Robert Burke

By _____

Date _____

Date _____

Attach: CV
W9