NEW YORK STATE | 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

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 consultants[1] 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** AEL link: https://www.fema.gov/authorized-equipment-list |
| 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=ypiA0BfIcc1qJooca1q%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.